



Delft University of Technology

Shortcuts towards fiber-based quantum networks

Avis, G.

DOI

[10.4233/uuid:d5548689-2e68-4960-ae7c-b475d82c7cd7](https://doi.org/10.4233/uuid:d5548689-2e68-4960-ae7c-b475d82c7cd7)

Publication date

2023

Document Version

Final published version

Citation (APA)

Avis, G. (2023). *Shortcuts towards fiber-based quantum networks*. <https://doi.org/10.4233/uuid:d5548689-2e68-4960-ae7c-b475d82c7cd7>

Important note

To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright

Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy

Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

Shortcuts Towards Fiber-Based Quantum Networks

Guus Avis



Shortcuts towards fiber-based quantum networks

Shortcuts towards fiber-based quantum networks

Proefschrift

ter verkrijging van de graad van doctor
aan de Technische Universiteit Delft,
op gezag van de Rector Magnificus prof. dr. ir. T.H.J.J. van der Hagen,
voorzitter van het College voor Promoties,
in het openbaar te verdedigen
op donderdag 15 juni 2023 om 10.00 uur

door

August Frederik Gerbrand AVIS

Master of Science in Physics and Climate Science,
Universiteit Utrecht, Nederland,
geboren te Bussum, Nederland.

Dit proefschrift is goedgekeurd door de promotoren.

Samenstelling promotiecommissie:

Rector Magnificus,
Prof. dr. S.D.C. Wehner,
Prof. dr. ir. R. Hanson,

voorzitter
Technische Universiteit Delft, promotor
Technische Universiteit Delft, promotor

Onafhankelijke leden:

Prof. dr. T.E. Northup,
Prof. dr. B.M. Terhal,
Prof. dr. L. DiCarlo,
dr. H. Ollivier,
dr. M. Veldhorst,

University of Innsbruck, Austria
Technische Universiteit Delft
Technische Universiteit Delft
INRIA, France
Technische Universiteit Delft, reservelid



QUANTUM
INTERNET
ALLIANCE



Printed: on recycled paper by Ridderprint | www.ridderprint.nl

Cover: created by Eva Peet and Guus Avis using Midjourney

Copyright ©2023 by A.F.G. Avis

ISBN 978-94-6483-200-6

An electronic version of this dissertation is available at
<http://repository.tudelft.nl/>.

Contents

Summary	xi
Samenvatting	xiii
1 Introduction	1
2 Preliminaries	7
2.1 Basic operations of quantum repeaters	7
2.1.1 Bell states	7
2.1.2 Entanglement swapping	8
2.1.3 Heralded entanglement generation.	8
2.2 Types of quantum repeaters	9
2.2.1 Long-lived quantum memory	10
2.2.2 Multiplexing	10
2.2.3 Other types of repeaters	11
2.3 Quantifying repeater performance	12
2.3.1 Rate and fidelity	12
2.3.2 Secret-key rate	12
2.3.3 Blind quantum computing	13
3 Requirements for a processing-node quantum repeater on a real-world fiber grid	21
3.1 Results	22
3.1.1 Quantum-Network Path	24
3.1.2 Blind Quantum Computation.	28
3.1.3 Minimal Hardware Requirements.	29
3.1.4 Absolute Minimal Requirements.. . . .	30
3.2 Discussion	32
3.2.1 Hardware Requirements in Simplified Settings.. . . .	32
3.2.2 Entanglement Without a Repeater.	33
3.2.3 Outlook.	35
3.3 Methods	35
3.3.1 Conditions on Network Path to Enable VBQC.	35
3.3.2 Average Teleportation Fidelity.	35
3.3.3 Hardware Improvement for VBQC as an Optimization Problem. . .	36
3.3.4 Optimization Parameters.	37
3.3.5 Evaluating Hardware Quality.	39
3.3.6 Framework for Simulating Quantum Repeaters.	39
3.3.7 Finding Minimal Hardware Improvements.. . . .	40
3.3.8 Finding Absolute Minimal Hardware Requirements.	40

3.4	Data availability	41
3.5	Code availability	41
3.6	Setup.	41
3.6.1	Fiber network and node placement.	41
3.6.2	Repeater protocol	42
3.6.3	Quantum-computing server	44
3.6.4	Processing nodes.	44
3.6.5	Color centers.	45
3.6.6	Trapped ions	48
3.6.7	Abstract nodes	51
3.6.8	Entanglement generation.	57
3.7	Target metric.	57
3.7.1	Teleportation fidelity.	58
3.7.2	Requirements from VBQC	59
3.7.3	Proving Theorem 3.1	60
3.7.4	Proving Theorem 3.2	65
3.7.5	Remote state preparation.	66
3.8	Double-click model.	74
3.8.1	Model assumptions.	74
3.8.2	POVMs.	76
3.8.3	Results without coincidence window.	78
3.8.4	Results with coincidence window	80
3.9	Effect of detection and coincidence time windows	81
3.10	Single-click model	95
3.10.1	Model assumptions.	95
3.10.2	Results	96
3.11	Optimization method.	98
3.11.1	Termination criteria for genetic algorithms.	98
3.11.2	Cost function.	99
3.11.3	Probabilities of no-imperfection	100
3.11.4	Optimizing over tunable parameters	102
3.12	Simulation performance	103
3.13	Framework for simulating quantum repeaters	105
3.13.1	Services	106
3.13.2	SWAP-ASAP protocol	107
3.13.3	Configuring quantum networks	108
3.14	Extra optimization results	109
3.14.1	To move or not to move	109
3.14.2	Architecture comparison	111
3.14.3	Connecting Delft and Eindhoven without a repeater	111
3.14.4	Hardware requirements for repeaters with single and double-click entanglement generation.	112
3.14.5	Hardware improvement costs	113

4	Asymmetric node placement in fiber-based quantum networks	125
4.1	Asymmetry in midpoint placement.	126
4.1.1	Cycle time	128
4.1.2	Imbalanced losses	128
4.1.3	Photon indistinguishability.	131
4.2	Asymmetry in repeater chains	137
4.2.1	SWAP-ASAP repeaters with parallel entanglement generation . . .	137
4.2.2	Research questions.	138
4.2.3	Quantifying repeater performance	139
4.2.4	Quantifying chain asymmetry	139
4.2.5	Model for Repeater Chain	141
4.2.6	Numerical results	141
4.2.7	Reflection on numerical results.	142
4.3	Conclusion.	146
4.4	Code availability	146
4.5	Single-click and double-click expressions.	146
4.5.1	Double click	147
4.5.2	Single click.	148
4.6	Calculating photon indistinguishability	149
4.6.1	Gaussian	149
4.6.2	Lorentzian	150
5	Requirements for upgrading trusted nodes to a repeater chain over 900 km of optical fiber	159
5.1	Introduction	159
5.1.1	Setup.	160
5.1.2	Applications	163
5.1.3	Minimal hardware requirements	163
5.1.4	State-of-the-art parameters.	164
5.1.5	Determining minimal hardware requirements	165
5.2	Impact of number of repeaters on hardware requirements	165
5.2.1	Absolute minimal number of multiplexing modes	166
5.2.2	Minimal hardware requirements for quantum-key distribution. . .	167
5.2.3	Secret-key rate: quantum-bit error rate and entanglement generation rate	169
5.3	Impact of target on hardware requirements	170
5.3.1	Requirements for different secret-key-rate targets	171
5.3.2	Requirements for secret-key and blind-quantum-computing success rates.	172
5.4	Conclusion.	173
5.5	Data availability	174
5.6	Code availability	174
5.7	Baseline parameters	174
5.8	Repeater placement chosen by optimization method	175
5.9	Optimization method.	177
5.9.1	No-imperfection probabilities	177
5.9.2	Local optimization	178

5.9.3	Performing the optimization	179
5.10	BQC test protocol	179
6	Designing Quantum Networks Using Preexisting Infrastructure	185
6.1	Results	188
6.1.1	Path-Based Formulation	191
6.1.2	Link-Based Formulation	192
6.2	Discussion	194
6.2.1	Example on a Real Network	194
6.2.2	Effect of Network-Requirement Parameters	195
6.2.3	Computation Times	199
6.2.4	Extensions	200
6.2.5	Limitations	202
6.3	Methods	205
6.3.1	Explanation of the Path-Based Formulation	205
6.3.2	Toy-Model Calculation of N_{\max} and L_{\max} from R_{\min} and F_{\min} . . .	206
6.3.3	Proof of Equivalence	207
6.3.4	Generating Random Networks	208
6.3.5	Scaling of the Formulations	208
6.4	Toy-Model Calculation of Rate and Fidelity	211
6.5	Proof of Equivalence	212
6.5.1	Formulations	213
6.5.2	From the Path-Based Formulation to the Link-Based Formulation .	215
6.5.3	From the Link-Based Formulation to the Path-Based Formulation .	220
7	Analysis of multipartite entanglement distribution using a central quantum-network node	229
7.1	Introduction	229
7.1.1	Summary of results.	231
7.1.2	Comparison of analytical results to prior work	231
7.1.3	Different central nodes	232
7.1.4	Outline.	234
7.2	Setup, Protocol and Model	235
7.3	Analytical Results	238
7.3.1	Rate	238
7.3.2	Fidelity.	240
7.4	Comparison	244
7.5	Physical Implementation	252
7.5.1	Trapped Ions	253
7.5.2	Nitrogen-Vacancy Centers	253
7.6	Conclusion.	257
7.7	Data Availability	259
7.8	Code Availability.	260
7.9	Verification of Analytical Expressions for Rate and Fidelity.	260
7.10	Deriving the Density Matrix Created by Protocol 7.1	262
7.11	Coefficients of Fidelity Function	264

7.12	Expected Values for Memory Decoherence	267
7.12.1	Indices	267
7.12.2	Probability Building Blocks.	268
7.12.3	Probability Distribution of Links	270
7.12.4	Expected Value.	272
7.12.5	Recursive Relation	276
7.12.6	Counting Orders	278
7.12.7	Calculating G	281
7.12.8	Lower Bound.	281
7.13	Expected Value of Distribution Time	283
7.13.1	Exact Recursion Relation.	284
7.13.2	Upper Bound.	285
7.13.3	Leading Order	285
Acknowledgments		295
Curriculum Vitæ		299
List of Publications		301

Summary

The future quantum internet promises to create shared quantum entanglement between any two points on Earth, enabling applications such as provably-secure communication and connecting quantum computers. A popular method for distributing entanglement is by sending entangled photons through optical fiber. However, the probability of successful transmission decreases exponentially with the fiber length. This makes it challenging to realize large fiber-based quantum networks that create shared entanglement, let alone the construction of a quantum internet. Quantum repeaters have been proposed as a solution to mitigate losses by acting as intermediary nodes that divide long optical fibers into smaller segments. The required technology, however, is still under development. In this thesis we aim to expedite the realization of fiber-based quantum networks by identifying shortcuts towards that end.

One way in which we look for shortcuts is by identifying the technological advances that are required to build such networks. To achieve this we translate performance demands on the network to requirements on individual components, such as quantum repeaters. This way we are not only able to indicate how much development current-day technology still requires before functional quantum networks can be built, but also what specific set of improvements could be applied to state-of-the-art hardware to get there as soon as possible.

A specific promising shortcut that we investigate in this thesis is the construction of quantum networks using existing fiber infrastructure. As deploying optical fiber is costly, an economical method for building quantum networks would be to incorporate fiber that has already been placed in the field. Existing infrastructure however imposes restrictions on quantum networks, in particular on the possible locations where quantum hardware could be installed. An important question to answer is then how severe the effects of these restrictions are. We address this question by investigating the performance degradation caused by displacing nodes from their optimal location, and the increase in required technological advances when restrictions are taken into account. Additionally, we provide tools for choosing where to deploy quantum repeaters when subject to placement restrictions.

Finally, we also address the fact that quantum networks may need to provide entanglement to more than just two parties. When a network has many end nodes that require bipartite entanglement between different pairs of them, it is important that it is designed such that every end node is sufficiently connected to every other end node. We provide conditions to judge whether this is the case and a method to ensure the conditions are met. Alternatively end nodes could require multipartite entangled states shared by more than two of them, in which case specialized nodes may need to be included in the network. We investigate what such a node could look like and perform a thorough performance analysis.

Samenvatting

Het toekomstige kwantuminternet belooft kwantumverstrengeling tussen welke twee locaties op aarde dan ook te kunnen creëren en zo toepassingen, zoals communicatie waarvan de veiligheid bewezen is en het verbinden van kwantumcomputers, mogelijk te maken. Een populaire manier om kwantumverstrengeling te verspreiden is door verstrengelde fotonen door glasvezelkabels te versturen. Echter, de kans dat een foton succesvol wordt ontvangen neemt exponentieel af met de lengte van de kabel. Dit maakt het moeilijk om grote glasvezelkwantumnetwerken te realiseren, laat staan een kwantuminternet. Kwantumversterkers zouden op verschillende punten langs de kabel kunnen worden geïnstalleerd om zo de snelheid waarmee verstrengeling wordt verspreid te vergroten, maar de benodigde technologie is nog in ontwikkeling. Met dit proefschrift hopen we de aanvang van glasvezelkwantumnetwerken te bespoedigen door afsnijroutes daartoe te identificeren.

Één manier waarop wij afsnijroutes zoeken is door te bepalen welke technologische vooruitgang er nodig is om zulke netwerken mogelijk te maken. Hiertoe vertalen wij vereisten aan de prestaties van het netwerk naar benodigdheden aan individuele componenten, zoals kwantumversterkers. Op deze manier kunnen wij niet alleen aangeven hoeveel ontwikkeling hedendaagse technologie nog nodig heeft voordat er functionele kwantumnetwerken gebouwd kunnen worden, maar ook welke specifieke verbeteringen dat het snelste mogelijk zouden maken.

Een veelbelovende afsnijroute die wij in dit proefschrift in het bijzonder onderzoeken is het bouwen van kwantumnetwerken door middel van reeds bestaande glasvezelinfrastructuur. Het uitrollen van glasvezel is duur, en aangezien er al veel zulke kabels in de grond liggen is een zuinigere manier om kwantumnetwerken te bouwen het gebruik daarvan. Bestaande infrastructuur beperkt echter wel hoe kwantumnetwerken eruit kunnen zien, in het bijzonder waar kwantumapparatuur precies geïnstalleerd kan worden. Een belangrijke vraag is dan ook hoe ernstig de effecten van deze beperkingen zijn. We adresseren deze vraag door te onderzoeken hoezeer prestaties worden verslechterd wanneer kwantumapparatuur enige afstand van de meest ideale locatie verwijderd is, en door te bestuderen hoezeer deze beperkingen de vereiste technologische vooruitgang vergroten. Verder bieden wij ook hulpmiddelen aan om te bepalen waar kwantumversterkers in dat geval het beste geplaatst kunnen worden.

Als laatste adresseren wij ook het feit dat kwantumnetwerken mogelijk verstrengeling moeten bieden aan meer dan twee deelnemers. Wanneer een netwerk veel deelnemers heeft die, in verschillende paren van twee, verstrengeling willen delen, is het belangrijk dat het netwerk zo is ontworpen dat alle deelnemers goed genoeg verbonden zijn met elkaar. We formuleren vereisten om te bepalen of dit het geval is en presenteren een methode om aan deze vereisten te voldoen. Het zou echter ook kunnen zijn dat meer dan twee deelnemers samen één verstrengelde kwantumtoestand willen delen, in welk geval wellicht gespecialiseerde kwantumapparatuur in het netwerk opgenomen moet worden.

We onderzoeken hoe die apparatuur er uit zou kunnen zien en bestuderen in detail hoe goed die zou presteren.

1

Introduction

The theory of quantum mechanics has been developed since the early twentieth century to describe physics at small length scales, arguably starting with the seminal work by Max Planck on black-body radiation in 1900 [1]. According to quantum mechanics, two or more systems can be entangled [2], in which case they share a single quantum state and cannot be accurately described independently from one another. As first discovered by John Stewart Bell in 1964 [3], the statistics predicted by quantum mechanics when performing certain measurements on entangled systems display a level of correlation that would be hard to reproduce in a world governed by classical physics. In fact, these correlations are incompatible with any theory in which local measurement outcomes only depend on local (possibly hidden) variables, given that a number of basic assumptions hold [4], such as statistical independence between the settings of measurement devices and the systems they measure [5]. It has been experimentally verified that the correlations predicted by quantum mechanics are not just theoretical but also hold in nature, for example in an experiment conducted in Delft in 2015 (a “loophole-free Bell test”) [6].

Besides the important implications entanglement has for fundamental physics, more recently interest has arisen in the engineering of entangled quantum states to be used as a practical resource. For instance, if two parties have access to entangled states, the application Quantum Key Distribution (QKD) enables them to create a provably-secure secret key [7–9], which can be used, e.g., for the encryption of messages that only the owners of that key can decrypt. Other applications that make use of quantum entanglement include connecting remote telescopes to take higher-resolution pictures [10] and improved clock synchronization [11]. Another practical application of the properties of quantum mechanics is the construction of quantum computers, which manipulate quantum states in order to, in theory, perform some calculations more efficiently than possible on a classical computer [12–16]. Shared entanglement enables the exchange of quantum information between quantum computers through quantum teleportation [17]. Other applications of entanglement shared between quantum computers include distributed quantum computing [18, 19], allowing the computers to perform computations in a distributed fashion, and blind quantum computing [20, 21], allowing a client to perform quantum computations on a server without the server learning the nature of those computations.

In order to perform applications that require entanglement, first one needs to create entangled states shared between the relevant parties. Quantum networks are networks

able to distribute remote entanglement, their construction envisioned to ultimately lead to a quantum internet that enables the creation of shared entanglement between any two points on Earth [22, 23]. However, at the time of writing, a quantum internet is far from realized, with the first quantum network connecting three nodes having only recently been demonstrated [24]. While the manipulation and control of quantum systems is in general by no means an easy task, quantum networks are particularly challenging to construct due to the transmission losses encountered when exchanging entangled particles between nodes of the network [25–28]. In this thesis, we focus on quantum networks in which entanglement is generated between nodes by sending entangled photons through optical fiber. Although optical fibers have been highly optimized after years of optical telecommunication (even leading to a Nobel prize being awarded to Charles K. Kao in 2009 [29]), the probability that a photon is successfully transmitted through a fiber still falls exponentially with the length of that fiber [30, 31]. With typical losses in single-mode optical fiber being of the order of 0.2 dB/km [31], the photon survival probability is about one in a hundred over hundred kilometers of optical fiber, but quickly declines to approximately only one in ten billion over five hundred kilometers. Direct transmission of photons over fiber is therefore not well suited for the construction of large-scale quantum networks, let alone a global quantum internet.

When a classical signal is sent through optical fiber, the same exponential losses are encountered. These can be mitigated using optical amplifiers, but that strategy does not work in the quantum case due to the no-cloning theorem [28], according to which it is impossible to duplicate an arbitrary quantum state [32–34]. Still it is possible to increase entangling rates by installing intermediate nodes that separate a longer stretch of optical fiber into shorter segments [35]. While entanglement may be generated only slowly over the full fiber distance, it can be created much more efficiently on each of the shorter segments. Just splitting fiber into segments, however, is not enough. The intermediate nodes need to be able to provide certain functionality that enables leveraging the higher efficiency on the shorter segments such that end-to-end entanglement is produced faster than what would be achievable over the full fiber length all at once. Devices that provide such functionality are called quantum repeaters [22, 26–28], and a quantum network can consist of both end nodes that require shared entanglement as a service, and repeaters that facilitate that service [23]. There are a number of different operational principles on which a quantum repeater can be based (as discussed in Chapter 2), but although impressive progress is being made and proof-of-principle experiments have been recently performed [36, 37], practical quantum repeaters that can be usefully deployed are still technologically out of reach.

In this thesis, we aim to contribute to the swift deployment of quantum repeaters, and to the real-world construction of fiber-based quantum networks. To this end, we analyze the requirements imposed on such networks and identify paths towards their realization. As such, we aim to find shortcuts towards the realization of fiber-based quantum networks, as suggested by the title of this thesis. Below we list the particular research questions that we address and indicate what part of this thesis addresses the question in what way.

What are the minimal requirements on quantum hardware to build a functional quantum-repeater network?

It is clear that experimental progress is needed in order to build useful quantum networks. However, it is not always obvious how much progress is needed. Even more importantly,

there are many ways in which quantum hardware could be improved, and it would be useful to know which should have the highest priority. For instance, is it more important to improve a device's emission probability or its error rates when manipulating quantum states? An answer to this question could help realize a more efficient allocation of research projects and resources, such that quantum networks can come into fruition as soon as possible. Within this thesis, this particular question is addressed most in depth in Chapter 3. In that chapter we consider a concrete single-repeater quantum network and specific types of quantum hardware, and investigate what the “smallest” admissible amount of improvement over the state-of-the-art is such that the network performance meets a set of demands (namely, a minimal rate and fidelity of entanglement distribution). The question is also addressed in Chapter 5, where we additionally investigate the effect of the number of repeaters in the network and the focus is less on the hardware specifics and more on how the different demands that could be imposed on the network as a whole affect the requirements on individual repeaters.

How large is the effect of constraints imposed by existing fiber infrastructure on hardware requirements and network performance, if a quantum network is constructed using that infrastructure?

Classical telecommunication networks utilize optical fiber, and as such fiber infrastructure is already widespread. Using this existing infrastructure to build quantum networks, rather than deploying new infrastructure, would be a very economical method for the construction of fiber-based quantum networks and can be thought of as a shortcut towards their realization. However, incorporating existing infrastructure imposes a number of constraints on the quantum network. Not only is fiber only available along specific paths, also the locations where the fiber emerges from the ground and quantum hardware could be installed are predetermined. In both Chapters 3 and 5 we optimize over the constrained placement of network nodes, and in Chapter 3 we also explicitly investigate how much larger the requirements imposed on quantum hardware are on a real fiber grid compared to a more idealized fiber grid. One of the consequences of infrastructure constraints is that the nodes of the quantum network may not always be evenly spaced, meaning that different fiber segments having different lengths. In Chapter 4 we investigate in depth to what extent such an uneven spacing would deteriorate the performance of specific types of quantum networks. Finally, in Chapter 6, we address the question of where in an existing fiber grid one should install quantum repeaters and where not, in case one aims to minimize the total number of repeaters in the network while ensuring a number of demands on the network performance are met.

How can a set of multiple end nodes in a quantum network be served optimally?

While in Chapters 3, 4 and 5 we mostly focus on quantum networks that have only two end nodes, a general network could have many end nodes that require shared entanglement. In Chapter 6 we focus on the distribution of bipartite entanglement, i.e., entanglement between two quantum systems, between different pairs of end nodes in a network. More specifically, we consider how quantum repeaters can be allocated across a network such that any set of two end nodes can obtain shared entanglement with some guaranteed quality of service. In Chapter 7, on the other hand, we consider the case when the end nodes want to share multipartite entanglement, i.e., entanglement shared between more than two quantum systems. We investigate how nodes dedicated to the creation of multipartite

entanglement (somewhat akin to quantum repeaters) could be operated and perform a thorough performance analysis. This is a step towards determining optimal strategies for the distribution of multipartite entanglement in future quantum networks in the presence of hardware imperfections.

References

- [1] D. P. G. -. Deutsche Physikalische Gesellschaft (1899-1945), *Verhandlungen der Deutschen physikalischen Gesellschaft* (Friedr. Vieweg & Sohn, 1900).
- [2] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, *Quantum entanglement*, Rev. Mod. Phys. **81**, 865 (2009).
- [3] J. S. Bell, *On the Einstein Podolsky Rosen paradox*, Physics Physique Fizika **1**, 195 (1964).
- [4] W. Myrvold, M. Genovese, and A. Shimony, *Bell's Theorem*, in *The Stanford Encyclopedia of Philosophy*, edited by E. N. Zalta (Metaphysics Research Lab, Stanford University, 2021) fall 2021 ed.
- [5] J. R. Hance and S. Hossenfelder, *Bell's theorem allows local theories of quantum mechanics*, Nat. Phys. **18**, 1382 (2022).
- [6] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, *Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres*, Nature **526**, 682 (2015).
- [7] C. H. Bennett, G. Brassard, and N. D. Mermin, *Quantum cryptography without Bell's theorem*, Phys. Rev. Lett. **68**, 557 (1992).
- [8] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, Theoretical Computer Science Theoretical Aspects of Quantum Cryptography – Celebrating 30 Years of BB84, **560**, 7 (2014).
- [9] A. K. Ekert, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett. **67**, 661 (1991).
- [10] D. Gottesman, T. Jennewein, and S. Croke, *Longer-Baseline Telescopes Using Quantum Repeater*, Phys. Rev. Lett. **109**, 070503 (2012).
- [11] P. Kómár, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sørensen, J. Ye, and M. D. Lukin, *A quantum network of clocks*, Nature Physics **10**, 582 (2014).
- [12] R. P. Feynman, *Simulating physics with computers*, Int J Theor Phys **21**, 467 (1982).
- [13] D. Gottesman, *Opportunities and Challenges in Fault-Tolerant Quantum Computation*, (2022), arXiv:2210.15844 .
- [14] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien, *Quantum computers*, Nature **464**, 45 (2010).

- [15] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, tenth ed. (Cambridge University Press, USA, 2011).
- [16] R. Rietsche, C. Dremel, S. Bosch, L. Steinacker, M. Meckel, and J.-M. Leimeister, *Quantum computing*, Electron Markets **32**, 2525 (2022).
- [17] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, Phys. Rev. Lett. **70**, 1895 (1993).
- [18] J. I. Cirac, A. K. Ekert, S. F. Huelga, and C. Macchiavello, *Distributed quantum computation over noisy channels*, Phys. Rev. A **59**, 4249 (1999).
- [19] L. K. Grover, *Quantum Telecomputation*, (1997), arXiv:9704012 .
- [20] A. Broadbent, J. Fitzsimons, and E. Kashefi, *Universal blind quantum computation*, 2009 50th Annual IEEE Symposium on Foundations of Computer Science , 517 (2009), 0807.4154 .
- [21] D. Leichtle, L. Music, E. Kashefi, and H. Ollivier, *Verifying BQP Computations on Noisy Devices with Minimal Overhead*, PRX Quantum **2**, 040302 (2021).
- [22] H. J. Kimble, *The Quantum Internet*, Nature **453**, 1023 (2008), 0806.4195 .
- [23] S. Wehner, D. Elkouss, and R. Hanson, *Quantum internet: A vision for the road ahead*, Science **362**, eaam9288 (2018).
- [24] M. Pompili, S. L. N. Hermans, S. Baier, H. K. C. Beukers, P. C. Humphreys, R. N. Schouten, R. F. L. Vermeulen, M. J. Tiggelman, L. dos Santos Martins, B. Dirkse, S. Wehner, and R. Hanson, *Realization of a multinode quantum network of remote solid-state qubits*, Science **372**, 259 (2021).
- [25] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, *Fundamental Limits of Repeaterless Quantum Communications*, Nat Commun **8**, 15043 (2017).
- [26] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication*, Phys. Rev. Lett. **81**, 5932 (1998).
- [27] K. Azuma, S. E. Economou, D. Elkouss, P. Hilaire, L. Jiang, H.-K. Lo, and I. Tzitrin, *Quantum repeaters: From quantum networks to the quantum internet*, (2022), arXiv:2212.10820 .
- [28] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, *Inside Quantum Repeaters*, IEEE Journal of Selected Topics in Quantum Electronics **21**, 78 (2015).
- [29] *The Nobel Prize in Physics 2009*, <https://www.nobelprize.org/prizes/physics/2009/kao/facts/> (2009).
- [30] F. Mitschke, *Fiber Optics: Physics and Technology* (Heidelberg ; New York, 2010).
- [31] *G.652 : Characteristics of a single-mode optical fibre and cable*, <https://www.itu.int/rec/T-REC-G.652> (2013).

- [32] D. Dieks, *Communication by EPR devices*, Physics Letters A **92**, 271 (1982).
- [33] J. L. Park, *The concept of transition in quantum mechanics*, Found Phys **1**, 23 (1970).
- [34] W. K. Wootters and W. H. Zurek, *A single quantum cannot be cloned*, Nature **299**, 802 (1982).
- [35] S. Pirandola, *End-to-end capacities of a quantum communication network*, Commun Phys **2**, 1 (2019).
- [36] M. K. Bhaskar, R. Riedinger, B. Machielse, D. S. Levonian, C. T. Nguyen, E. N. Knall, H. Park, D. Englund, M. Lončar, D. D. Sukachev, and M. D. Lukin, *Experimental demonstration of memory-enhanced quantum communication*, Nature **580**, 60 (2020).
- [37] S. Langenfeld, P. Thomas, O. Morin, and G. Rempe, *Quantum Repeater Node Demonstrating Unconditionally Secure Key Distribution*, Phys. Rev. Lett. **126**, 230506 (2021).

2

Preliminaries

In this chapter we briefly discuss some of the key concepts required to understand this thesis. Particularly, we discuss the types of quantum repeaters that we consider and some of the metrics employed to quantify the performance level of a quantum network.

2.1 Basic operations of quantum repeaters

All the quantum repeaters we study in this thesis share two basic operational principles. These are heralded entanglement generation [1–4], which is used to create entangled states between neighboring nodes in the network, and entanglement swapping [2, 5, 6], which is used to transform entangled states between neighbors into entangled states between non-neighboring nodes. Let us for simplicity focus on a quantum-repeater chain, that is, a one-dimensional quantum network with two end nodes at the far ends and quantum-repeater nodes as intermediary nodes. Entanglement between the end nodes can then be generated by first performing heralded entanglement generation between all neighbors, and then performing entanglement swapping at all repeaters. Before looking at specific types of quantum repeaters, we will first explain entanglement swapping and heralded entanglement generation in more detail.

2.1.1 Bell states

A quantum bit (qubit) is a two-level system that can be in the state $|0\rangle$, $|1\rangle$, or a superposition of the two of the form

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (2.1)$$

with complex numbers α and β such that the state is normalized (i.e., $|\alpha|^2 = |\beta|^2 = 1$) [7, 8]. Then, when there are two qubits, their state can be any normalized superposition of $|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$ and $|1\rangle \otimes |1\rangle$. Now let us define the Bell states [7–9],

$$|\phi_{ij}\rangle = (X^i Z^j \otimes \mathbb{1}) \frac{1}{\sqrt{2}} (|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle). \quad (2.2)$$

Here, i and j can take the values 0 and 1, X and Z are the Pauli X and Z operators respectively defined as $X = |0\rangle\langle 1| + |1\rangle\langle 0|$ and $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$, and $\mathbb{1}$ is the identity operator $\mathbb{1} = |0\rangle\langle 0| + |1\rangle\langle 1|$. These four states form an orthonormal basis, known as the Bell basis, for

two qubits. That is, any two-qubit state can be written as a normalized superposition of the Bell states instead of the states $|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$ and $|1\rangle \otimes |1\rangle$ [7–9]. These Bell states are entangled, by which it is meant that they cannot be written as a product of two single-qubit states,

$$|\phi_{ij}\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle. \quad (2.3)$$

In fact, the Bell states are maximally entangled (meaning that when one qubit is lost there is no information left about the remaining qubit), and every two-qubit maximally entangled state is equivalent to a Bell state up to single-qubit unitary operations [10]. The goal of the chains of quantum repeaters considered in this thesis is to distribute such a maximally entangled state between the chain's end nodes, as fast and with as few errors as possible. Heralded entanglement generation, discussed in more detail below, is a method for creating Bell states shared between qubits at neighboring nodes.

2.1.2 Entanglement swapping

Now, we define a Bell-State Measurement (BSM) as a two-qubit measurement with measurement operators that are projectors onto the Bell basis (see, e.g., Ref. [8] for a review on measurements in quantum mechanics). Then, if qubits 1 and 2 are in the state $|\phi_{ij}\rangle_{1,2}$ and the qubits 3 and 4 are in the state $|\phi_{kl}\rangle_{3,4}$, a BSM on qubits 2 and 3 with outcome $|\phi_{mn}\rangle$ creates the following state shared by qubits 1 and 4:

$$\frac{(|\phi_{mn}\rangle\langle\phi_{mn}|)_{2,3} |\phi_{ij}\rangle_{1,2} |\phi_{kl}\rangle_{3,4}}{||\phi_{mn}\rangle\langle\phi_{mn}|)_{2,3} |\phi_{ij}\rangle_{1,2} |\phi_{kl}\rangle_{3,4}|} = |\phi_{i \oplus k \oplus m, j \oplus l \oplus n}\rangle_{1,4} |\phi_{mn}\rangle_{2,3}. \quad (2.4)$$

Here, \oplus denotes addition modulo two. Thus, the qubits 1 and 4 which before did not share any entanglement now share a Bell state. This method for creating entanglement between two possibly remote qubits is what we refer to here as entanglement swapping, a procedure discovered first in Ref. [5]. In the context of quantum repeaters, entanglement swapping is when a BSM is performed on two local qubits that are entangled with qubits at different nodes. If there is a Bell state shared between every pair of neighboring nodes in a quantum-repeater chain and every repeater performs entanglement swapping, the end nodes will end up sharing entanglement. Entanglement swapping has been experimentally realized in various physical systems [11–16].

2.1.3 Heralded entanglement generation

In this thesis, we consider a class of protocols for distributing entanglement between neighbors that we refer to as heralded entanglement generation [1, 2]. By this, we mean a protocol that works as follows. Two nodes that want to share entanglement perform a sequence of attempts at entanglement generation. At the end of every attempt, both partaking nodes are notified whether the attempt was successful or not (success and failure are “heralded”). After a success, the nodes share an entangled (but possibly erroneous) state. After a failure, the nodes are left with nothing and must try again. In particular, in this thesis, we consider the so-called single-click protocol (proposed in Ref. [3], demonstrated experimentally in, e.g., Refs. [15, 17, 18]) and the double-click protocol (also sometimes referred to as the Barrett-Kok protocol after its inventors [4], experimentally realized in, e.g., Refs. [19–22]) for heralded entanglement generation. For other protocols see, e.g., Refs [1, 6].

In these protocols, two neighboring nodes both generate local entanglement between a matter qubit and a photon. The entangled photons are then transmitted through optical fiber to a midpoint station, where a BSM is performed on the photons. As explained above, this will result in the creation of an entangled state shared between the two matter qubits. Attempts can fail for several reasons, one of which is photon loss (e.g., due to attenuation losses in fiber). In both the single- and double-click scheme, the heralding station performs a BSM using linear optics (more specifically, using beam splitters and single-photon detectors). In that case, even if there is no loss in the system, there is a probability that the measurement does not project on an entangled state, resulting in heralded failure. In fact, it has been proven that it is impossible to exceed a success probability of 50% using only linear optics [23] (unless ancillary entangled photons are introduced [24], although even then the BSM remains probabilistic). For more detailed models for the single- and double-click protocols, see Chapter 3. We note that when building a quantum network using existing fiber infrastructure, this may restrict not only the placement of quantum repeaters but also of midpoint stations.

2.2 Types of quantum repeaters

Let two end nodes be separated by a fiber of total length L . Then the probability that a photon transmitted from one node to the other is not lost due to fiber attenuation is given by an exponential decay [25],

$$\eta(L) = e^{-\frac{L}{L_{\text{att}}}}, \quad (2.5)$$

where L_{att} is the attenuation length of the fiber (a typical value considered in quantum-repeater literature is $L_{\text{att}} \approx 22$ km) [2, 6]. For simplicity, let us assume that the success probability of heralded entanglement generation between the two nodes takes the form [6]

$$P_{\text{succ}}(L) = p_0 \eta(L), \quad (2.6)$$

where p_0 parametrizes all loss in the system not due to attenuation. This formula is approximately correct when heralded entanglement generation is implemented using the double-click protocol or the direct transmission of entangled photons (for the single-click protocol the scaling would be rather like $\sqrt{\eta}$, but this would not change the argument made below). Imagine now that we split the distance L between the end nodes into N equal segments by installing $N - 1$ repeaters along the fiber, and that all neighboring nodes simultaneously perform one attempt at entanglement generation after which all repeaters perform entanglement swapping. End-to-end entanglement will only be created in case each of the repeaters held two entangled qubits to perform the swap on, or equivalently, in case entanglement generation succeeded on each of the segments. The success probability is then

$$P_{\text{succ, chain}}(L, N) = P_{\text{succ}}(L/N)^N = p_0^N e^{-\frac{L}{L_0}} < P_{\text{succ}}(L). \quad (2.7)$$

Therefore, introducing repeaters actually reduced the success probability by including the non-attenuation losses p_0 multiple times. Apparently, just splitting a fiber into smaller segments is in itself not enough to realize faster entanglement distribution. The quantum repeaters need additional functionality before they can actually be used as repeaters. There are two such types of functionality in particular that we consider in this thesis. Namely, they are long-lived quantum memory and multiplexing. While quantum repeaters can

be built using only one of these types of functionality, they can also be combined (as we consider in Chapter 5).

2

2.2.1 Long-lived quantum memory

A long-lived quantum memory is a system that can preserve quantum states for extended periods of time. It can boost the rate at which entanglement is distributed between end nodes as follows [2, 6, 26]: Imagine, again, that heralded entanglement generation is performed on each of the segments of a repeater chain. Entanglement will be successfully distributed between some of the nodes but not between others. Now, instead of requiring all the repeaters to immediately perform entanglement swapping, repeaters can store their entangled qubits in quantum memory. Then, the segments over which entanglement generation was previously unsuccessful are used to reattempt entanglement generation. Successfully entangled qubits are again stored in memory, while repeaters that failed a second time will yet again perform a new attempt. This can be continued until all neighboring nodes share entanglement. At that point, entanglement swapping can be executed at the repeaters to create an end-to-end entangled state. By not requiring all segments to be successful at the same time, the average time required until the end nodes share entanglement can be decreased. However, it must be noted that real-life quantum memory is imperfect and extended storage periods can incur errors [13, 15, 27–29]. Therefore, states can often not be stored indefinitely but should be discarded after some time. The amount of time after which a state is discarded is referred to as the cutoff time [30–36]. The cutoff time can often be freely chosen, where having a short cutoff time lessens the probability of an error occurring, but at the cost of often having to discard states, thereby increasing the time required until end-to-end entanglement can be generated. For example, in Chapters 3 and 5 the cutoff time is optimized over to determine the minimal hardware requirements for meeting a set of network performance demands.

We note that enhancing entangling rates using long-lived quantum memory is a strategy not limited to quantum repeaters. For instance, in Chapter 7 we investigate network nodes dedicated to the distribution of multipartite entangled states shared between $N > 2$ end nodes. First heralded entanglement generation is executed between the dedicated node and each end node, after which a multipartite analogue of entanglement swapping is performed. If no memory is present at the central node, heralded entanglement generation must succeed with all N neighbours at the same time, resulting in a success probability that decreases exponentially with the number of end nodes. If the central node instead contains quantum memory, entanglement generation does not need to succeed everywhere at the same time, thereby reducing the time required to distribute the multipartite state.

2.2.2 Multiplexing

Another strategy for decreasing the time until end-to-end entanglement is distributed is multiplexing. When multiplexing is used, every time slot of heralded entanglement generation is used to perform multiple attempts. This can for instance be done by using different frequency modes [37–39] or temporal modes [40–43] of the photons employed. Then, two neighbors end up sharing entanglement after a single time slot if at least one attempt was successful. Even if they are forced to perform entanglement swapping straight away because of the lack of long-lived quantum memory, the end-to-end success probability will be increased by the presence of the repeaters. If there are n modes of multiplexing, the

success probability of heralded entanglement generation over one segment is equal to the probability that not all n modes fail, i.e.,

$$P_{\text{succ}, n \text{ modes}} = 1 - (1 - P_{\text{succ}})^n \approx nP_{\text{succ}}. \quad (2.8)$$

This approximation is valid when P_{succ} is small. Given enough repeaters and modes, the success probability can then theoretically be brought arbitrarily close to unity. However, it must be noted that even when using multiplexing one still requires short-lived quantum memories for heralded entanglement generation, as local entangled qubits need to be stored until success or failure of each mode is heralded by the midpoint station. Based on this information, repeater nodes need to decide which of the $2n$ local qubits should undergo entanglement swapping. While storage times will be only relatively short, one difficulty with implementing multiplexing is the need for multimode quantum memories [40, 42, 44–48] (see, e.g., Ref. [39] for a thorough analysis).

2.2.3 Other types of repeaters

We would like to stress that the types of repeaters considered in this thesis and explained above by no means represent the most general class of repeater protocols. For instance, the repeaters we consider don't incorporate techniques for combatting errors that may occur during heralded entanglement generation or entanglement swapping. If the probability of such errors is high, the end-to-end entanglement delivered by a repeater chain may not be useful anymore (see Section 2.3 for a discussion about how the severity of errors in entangled states can be quantified). Two possible techniques for combatting errors are entanglement distillation and the use of quantum-error-corrected logical qubits. Entanglement distillation (also known as entanglement purification) is a technique to transform a number of noisy entangled states into a smaller number of less noisy states [49–52]. Combining distillation with the use of quantum memory (and possibly multiplexing) results in a so-called first-generation quantum-repeater protocol [2, 6, 53], an example of which is the first proposal for a quantum-repeater protocol, named the BDCZ protocol after its inventors [26]. When instead quantum error correction [54–56] is used, entanglement is not created between individual physical qubits but instead between logical qubits that each exist of multiple physical qubits according to some encoding scheme [57–60]. Redundancy in the encoding of logical qubits can lead to resilience against errors. When such a scheme is used, entanglement swapping must be performed between two logical qubits instead of between two physical qubits. When quantum memory (and possibly multiplexing) is combined with quantum error correction this is sometimes referred to as a second-generation quantum-repeater protocol [2, 6, 53]. A downside to both techniques for combatting errors is that they require more capabilities of quantum repeaters, such as the generation and storage of multiple entangled pairs with each neighboring node and a more thorough manipulation of those stored states. This may make them less suitable for near-future quantum networks (see, for example, Refs. [61, 62] for studies that investigate whether distillation helps for hardware quality close to the current state-of-the-art), and this motivates why they are mostly absent in this thesis.

A final type of quantum repeater that we mention here is the one-way quantum repeater (also known as a third-generation quantum repeater) [2, 6, 53, 63–66]. These types of quantum repeaters employ quantum-error-correcting codes to protect against losses and do away with the need for two-way communication between nodes, thereby poten-

tially enabling repetition rates that are much higher than for schemes based on heralded entanglement generation. A downside however is that by the no-cloning theorem it is impossible to effectively protect against losses if they exceed 50%, meaning that repeaters need to be spaced closely together (50% attenuation loss corresponds to approximately 15 km of fiber at $L_{\text{att}} = 22$ km) [6]. For more information about different types of quantum repeater see, e.g., Refs. [2, 6].

2.3 Quantifying repeater performance

In order to quantify how well a repeater chain performs, we need performance metrics for entanglement distribution. Repeaters have been presented here primarily as a method for speeding up entanglement generation over large distances. However, just looking at how quickly entanglement is created is not enough. It is also important to consider the probability that there are errors in the delivered entangled state. For example, end nodes may think they share a Bell state $|\phi_{00}\rangle$, but if there has been a Pauli-X error on a qubit it may instead be the Bell state $|\phi_{10}\rangle$. Such errors can be accounted for using the density-matrix formalism [7–9]. When a system is in the quantum state $|\psi_i\rangle$ with probability p_i (such that $\sum_i p_i = 1$), a density matrix

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \quad (2.9)$$

is assigned to that system. When there are multiple nonzero p_i 's, the system is said to be in a mixed state. Conversely, when there is only one nonzero p_i , the state is said to be pure.

2.3.1 Rate and fidelity

Probably the simplest way of quantifying the performance of entanglement generation is using the rate and fidelity. The (entangling) rate R is simply the number of end-to-end entangled states that can be produced on average per time unit and is often reported in entanglement-generation experiments [15, 17, 21, 22, 67–69]. To be more precise, let T be the average time that the end nodes have to wait between the creation of one end-to-end entangled state and the next, then the rate is given by [70]

$$R = \frac{1}{T}. \quad (2.10)$$

On the other hand, the fidelity is a metric for how erroneous delivered states are. If the target state of entanglement generation is $|\phi\rangle$ but in reality the delivered state is represented by the density matrix ρ , the fidelity is defined by [71]

$$F = \langle\phi|\rho|\phi\rangle. \quad (2.11)$$

2.3.2 Secret-key rate

A downside to rate and fidelity is that they are two numbers for quantifying the performance level of one process. If one repeater chain produces entanglement at a rate of 1 Hz and a fidelity of 0.8 and another chain at a rate of 10 Hz and a fidelity of 0.6, which is better? One way of solving this issue is by looking at how good the system is at supporting

actual applications that require entanglement. As one of the oldest and best known such applications, Quantum Key Distribution (QKD) [72–77] is a straightforward application to consider to this end. When performing entanglement-based QKD, two parties sharing an entangled state measure their qubits. If they measure in the same basis and the state they share is a pure, maximally-entangled state, the results are either expected to be perfectly correlated or anticorrelated (depending on the entangled state and the measurement basis). In that case, each such measurement directly produces one bit that can be used as a secret key. When there are errors present however, correlations are imperfect, as quantified by the Quantum Bit Error Rate (QBER) (it is the probability that measurement outcomes are not correctly correlated). These erroneous measurement results provide a raw key, from which a secret key can still be distilled using classical error correction as long as the QBER is not too large. We here define the secret fraction f to be the ratio between the lengths of the secret key and the raw key in the asymptotic limit, i.e., in the limit where the length of the raw key goes to infinity. It is a decreasing function of the QBER and hence a measure of how erroneous the entangled state is. The secret-key rate can then be defined as

$$\text{SKR} = Rf, \quad (2.12)$$

i.e., it is the product of the secret fraction and the rate at which entanglement is distributed. This can be interpreted as the number of private-key bits produced per time unit (up to possibly a constant factor to account for sifting, which is the filtering out of measurement results obtained when both parties did not measure in the same basis). What the secret fraction looks like depends on the specific QKD protocol considered, see, e.g., Ref. [76] for an overview. In Chapters 4 and 5 we consider specifically the entanglement-based BB84 protocol [73, 74]. Assuming the QBER is the same for each of the two measurement bases used, the secret fraction can be written as [78–80]

$$f_{\text{BB84}} = \max(0, 1 - 2h(\text{QBER})), \quad (2.13)$$

where $h(x) = -x \ln x - (1-x) \ln(1-x)$ is the binary-entropy function. The BB84 asymptotic secret key rate is used as a performance metric for various experiments [12, 68, 81] and quantum-network analyses [32, 33, 35, 39, 58, 70, 82].

2.3.3 Blind quantum computing

An advantage of using the secret-key rate to quantify quantum-network performance is that it is an application-driven metric. However, not all applications may have the same requirements, and therefore considering only QKD may result in a skewed perspective on what good quantum networks are. For instance, QKD is a single-qubit application, meaning that individual entangled states are directly processed after they have been created. In contrast, other applications may require multiple live entangled qubits simultaneously for further processing. Especially if these qubits need to be stored in noisy quantum memories until all required states are present, a quantum network that is good at performing QKD may not be as good at performing such other applications. Therefore, in this thesis, we also consider an application-driven performance metric that is not based on QKD. Specifically, we use the application of Blind Quantum Computation (BQC) [83–89]. This is an application that allows a client to execute a quantum program on a quantum-computing server without the server learning what program is executed. We focus on a minimal version of

this application, where only two-qubit quantum programs are executed at the server, in accordance with the protocol presented in Ref. [89]. In this protocol, the client determines randomly per round whether it is a computation round (such that it contributes to the client learning the desired computational result), and test rounds. Test rounds are used to verify the server's honesty, but noise in distributed entangled states can also lead to test failure. It is therefore impossible to tell whether the server is dishonest or the quality of entangled states is bad, making the test-round success probability in case of an honest server an important metric for how well the protocol can be executed.

References

- [1] T. E. Northup and R. Blatt, *Quantum information transfer using photons*, *Nature Photon* **8**, 356 (2014).
- [2] K. Azuma, S. E. Economou, D. Elkouss, P. Hilaire, L. Jiang, H.-K. Lo, and I. Tzitrin, *Quantum repeaters: From quantum networks to the quantum internet*, (2022), arXiv:2212.10820 .
- [3] C. Cabrillo, J. I. Cirac, P. García-Fernández, and P. Zoller, *Creation of entangled states of distant atoms by interference*, *Phys. Rev. A* **59**, 1025 (1999).
- [4] S. D. Barrett and P. Kok, *Efficient high-fidelity quantum computation using matter qubits and linear optics*, *Phys. Rev. A* **71**, 060310 (2005).
- [5] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, *Phys. Rev. Lett.* **70**, 1895 (1993).
- [6] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, *Inside Quantum Repeaters*, *IEEE Journal of Selected Topics in Quantum Electronics* **21**, 78 (2015).
- [7] S. Khatrī and M. M. Wilde, *Principles of Quantum Communication Theory: A Modern Approach*, (2020), arXiv:2011.04672 .
- [8] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, tenth ed. (Cambridge University Press, USA, 2011).
- [9] J. Watrous, *The Theory of Quantum Information*, 1st ed. (Cambridge University Press, 2018).
- [10] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, *Quantum entanglement*, *Rev. Mod. Phys.* **81**, 865 (2009).
- [11] F. Basso Basset, M. B. Rota, C. Schimpf, D. Tedeschi, K. D. Zeuner, S. F. Covre da Silva, M. Reindl, V. Zwiller, K. D. Jöns, A. Rastelli, and R. Trotta, *Entanglement Swapping with Photons Generated on Demand by a Quantum Dot*, *Phys. Rev. Lett.* **123**, 160501 (2019).
- [12] M. K. Bhaskar, R. Riedinger, B. Machielse, D. S. Levonian, C. T. Nguyen, E. N. Knall, H. Park, D. Englund, M. Lončar, D. D. Sukachev, and M. D. Lukin, *Experimental demonstration of memory-enhanced quantum communication*, *Nature* **580**, 60 (2020).

- [13] V. Krutyanskiy, M. Canteri, M. Meraner, J. Bate, V. Krcmarsky, J. Schupp, N. Sangouard, and B. P. Lanyon, *A telecom-wavelength quantum repeater node based on a trapped-ion processor*, (2023), arXiv:2210.05418 .
- [14] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, *Experimental Entanglement Swapping: Entangling Photons That Never Interacted*, Phys. Rev. Lett. **80**, 3891 (1998).
- [15] M. Pompili, S. L. N. Hermans, S. Baier, H. K. C. Beukers, P. C. Humphreys, R. N. Schouten, R. F. L. Vermeulen, M. J. Tiggelman, L. dos Santos Martins, B. Dirkse, S. Wehner, and R. Hanson, *Realization of a multinode quantum network of remote solid-state qubits*, Science **372**, 259 (2021).
- [16] M. Riebe, T. Monz, K. Kim, A. S. Villar, P. Schindler, M. Chwalla, M. Hennrich, and R. Blatt, *Deterministic entanglement swapping with an ion-trap quantum computer*, Nature Phys **4**, 839 (2008).
- [17] P. C. Humphreys, N. Kalb, J. P. J. Morits, R. N. Schouten, R. F. L. Vermeulen, D. J. Twitchen, M. Markham, and R. Hanson, *Deterministic delivery of remote entanglement on a quantum network*, Nature **558**, 268 (2018), 1712.07567 .
- [18] L. Slodička, G. Hétet, N. Röck, P. Schindler, M. Hennrich, and R. Blatt, *Atom-Atom Entanglement by Single-Photon Detection*, Phys. Rev. Lett. **110**, 083603 (2013).
- [19] H. Bernien, B. Hensen, W. Pfaff, G. Koolstra, M. S. Blok, L. Robledo, T. H. Taminiau, M. Markham, D. J. Twitchen, L. Childress, and R. Hanson, *Heralded entanglement between solid-state qubits separated by three metres*, Nature **497**, 86 (2013).
- [20] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenbergh, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, *Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres*, Nature **526**, 682 (2015).
- [21] L. J. Stephenson, D. P. Nadlinger, B. C. Nichol, S. An, P. Drmota, T. G. Ballance, K. Thirumalai, J. F. Goodwin, D. M. Lucas, and C. J. Ballance, *High-Rate, High-Fidelity Entanglement of Qubits Across an Elementary Quantum Network*, Phys. Rev. Lett. **124**, 110501 (2020).
- [22] V. Krutyanskiy, M. Galli, V. Krcmarsky, S. Baier, D. A. Fioretto, Y. Pu, A. Mazloom, P. Sekatski, M. Canteri, M. Teller, J. Schupp, J. Bate, M. Meraner, N. Sangouard, B. P. Lanyon, and T. E. Northup, *Entanglement of trapped-ion qubits separated by 230 meters*, Phys. Rev. Lett. **130**, 050803 (2023).
- [23] J. Calsamiglia and N. Lütkenhaus, *Maximum efficiency of a linear-optical Bell-state analyzer*, Appl Phys B **72**, 67 (2001).
- [24] W. P. Grice, *Arbitrarily complete Bell-state measurement using only linear optical elements*, Phys. Rev. A **84**, 042331 (2011).
- [25] F. Mitschke, *Fiber Optics: Physics and Technology* (Heidelberg ; New York, 2010).

- [26] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication*, Phys. Rev. Lett. **81**, 5932 (1998).
- [27] C. E. Bradley, S. W. de Bone, P. F. W. Möller, S. Baier, M. J. Degen, S. J. H. Loenen, H. P. Bartling, M. Markham, D. J. Twitchen, R. Hanson, D. Elkouss, and T. H. Taminiau, *Robust quantum-network memory based on spin qubits in isotopically engineered diamond*, npj Quantum Inf **8**, 1 (2022).
- [28] P. Drmota, D. Main, D. P. Nadlinger, B. C. Nichol, M. A. Weber, E. M. Ainley, A. Agrawal, R. Srinivas, G. Araneda, C. J. Ballance, and D. M. Lucas, *Robust Quantum Memory in a Trapped-Ion Quantum Network Node*, (2022), arXiv:2210.11447 .
- [29] P. Wang, C.-Y. Luan, M. Qiao, M. Um, J. Zhang, Y. Wang, X. Yuan, M. Gu, J. Zhang, and K. Kim, *Single ion qubit with estimated coherence time exceeding one hour*, Nature Communications **12**, 233 (2021).
- [30] Á. G. Iñesta, G. Vardoyan, L. Scavuzzo, and S. Wehner, *Optimal entanglement distribution policies in homogeneous repeater chains with cutoffs*, (2022), arXiv:2207.06533 .
- [31] S. Khatri, *Policies for elementary links in a quantum network*, Quantum **5**, 537 (2021).
- [32] B. Li, T. Coopmans, and D. Elkouss, *Efficient Optimization of Cutoffs in Quantum Repeater Chains*, IEEE Transactions on Quantum Engineering **2**, 1 (2021).
- [33] F. Rozpędek, K. Goodenough, J. Ribeiro, N. Kalb, V. C. Vivoli, A. Reiserer, R. Hanson, S. Wehner, and D. Elkouss, *Parameter regimes for a single sequential quantum repeater*, Quantum Sci. Technol. **3**, 034002 (2018).
- [34] S. Santra, L. Jiang, and V. S. Malinovsky, *Quantum repeater architecture with hierarchically optimized memory buffer times*, Quantum Sci. Technol. **4**, 025010 (2019).
- [35] F. Rozpędek, R. Yehia, K. Goodenough, M. Ruf, P. C. Humphreys, R. Hanson, S. Wehner, and D. Elkouss, *Near-term quantum-repeater experiments with nitrogen-vacancy centers: Overcoming the limitations of direct transmission*, Phys. Rev. A **99**, 052330 (2019).
- [36] W. Kozłowski, A. Dahlberg, and S. Wehner, *Designing a quantum network protocol*, in *Proceedings of the 16th International Conference on Emerging Networking EXperiments and Technologies*, CoNEXT '20 (Association for Computing Machinery, New York, NY, USA, 2020) pp. 1–16.
- [37] N. Sinclair, E. Saglamyurek, H. Mallahzadeh, J. A. Slater, M. George, R. Ricken, M. P. Hedges, D. Oblak, C. Simon, W. Sohler, and W. Tittel, *Spectral Multiplexing for Scalable Quantum Photonics using an Atomic Frequency Comb Quantum Memory and Feed-Forward Control*, Phys. Rev. Lett. **113**, 053603 (2014).
- [38] T. Chakraborty, H. van Brug, A. Das, O. Pietx-Casas, P.-C. Wang, G. C. do Amaral, A. L. Tchibotareva, and W. Tittel, *Frequency multiplexed photon pairs and detection for quantum repeaters*, (2022), arXiv:2205.10028 .

- [39] S. Guha, H. Krovi, C. A. Fuchs, Z. Dutton, J. A. Slater, C. Simon, and W. Tittel, *Rate-loss analysis of an efficient quantum repeater architecture*, Phys. Rev. A **92**, 022357 (2015), 1404.7183 .
- [40] C. Simon, H. de Riedmatten, M. Afzelius, N. Sangouard, H. Zbinden, and N. Gisin, *Quantum Repeaters with Photon Pair Sources and Multimode Memories*, Phys. Rev. Lett. **98**, 190503 (2007).
- [41] S. B. van Dam, P. C. Humphreys, F. Rozpędek, S. Wehner, and R. Hanson, *Multiplexed entanglement generation over quantum networks using multi-qubit nodes*, Quantum Sci. Technol. **2**, 034002 (2017).
- [42] D. Lago-Rivera, S. Grandi, J. V. Rakonjac, A. Seri, and H. de Riedmatten, *Telecom-heralded entanglement between multimode solid-state quantum memories*, Nature **594**, 37 (2021).
- [43] M. Businger, L. Nicolas, T. S. Mejia, A. Ferrier, P. Goldner, and M. Afzelius, *Non-classical correlations over 1250 modes between telecom photons and 979-nm photons stored in 171Yb3+:Y2SiO5*, Nat Commun **13**, 6438 (2022).
- [44] M. Afzelius, C. Simon, H. de Riedmatten, and N. Gisin, *Multimode quantum memory based on atomic frequency combs*, Phys. Rev. A **79**, 052329 (2009).
- [45] M.-X. Dong, W.-H. Zhang, L. Zeng, Y.-H. Ye, D.-C. Li, G.-C. Guo, D.-S. Ding, and B.-S. Shi, *Highly efficient storage of 25-dimensional photonic qudit in a cold-atom-based quantum memory*, (2023), arXiv:2301.00999 .
- [46] A. Ortu, J. V. Rakonjac, A. Holzäpfel, A. Seri, S. Grandi, M. Mazzera, H. de Riedmatten, and M. Afzelius, *Multimode capacity of atomic-frequency comb quantum memories*, Quantum Sci. Technol. **7**, 035024 (2022).
- [47] J. V. Rakonjac, D. Lago-Rivera, A. Seri, M. Mazzera, S. Grandi, and H. de Riedmatten, *Entanglement between a Telecom Photon and an On-Demand Multimode Solid-State Quantum Memory*, Phys. Rev. Lett. **127**, 210502 (2021).
- [48] A. Seri, D. Lago-Rivera, A. Lenhard, G. Corrielli, R. Osellame, M. Mazzera, and H. de Riedmatten, *Quantum Storage of Frequency-Multiplexed Heralded Single Photons*, Phys. Rev. Lett. **123**, 080502 (2019).
- [49] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, *Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels*, Phys. Rev. Lett. **76**, 722 (1996).
- [50] W. Dür and H. J. Briegel, *Entanglement purification and quantum error correction*, Rep. Prog. Phys. **70**, 1381 (2007), 0705.4165 .
- [51] F. Rozpędek, T. Schiet, L. P. Thinh, D. Elkouss, A. C. Doherty, and S. Wehner, *Optimizing practical entanglement distillation*, Phys. Rev. A **97**, 062333 (2018).
- [52] S. Krastanov, V. V. Albert, and L. Jiang, *Optimized Entanglement Purification*, Quantum **3**, 123 (2019).

- [53] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, *Ultrafast and Fault-Tolerant Quantum Communication across Long Distances*, Phys. Rev. Lett. **112**, 250501 (2014).
- [54] J. Roffe, *Quantum Error Correction: An Introductory Guide*, Contemporary Physics **60**, 226 (2019).
- [55] B. M. Terhal, *Quantum Error Correction for Quantum Memories*, Rev. Mod. Phys. **87**, 307 (2015).
- [56] E. Knill and R. Laflamme, *Theory of quantum error-correcting codes*, Phys. Rev. A **55**, 900 (1997).
- [57] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, *Quantum repeater with encoding*, Phys. Rev. A **79**, 032325 (2009).
- [58] Y. Jing and M. Razavi, *Quantum Repeaters with Encoding on Nitrogen-Vacancy-Center Platforms*, Phys. Rev. Appl. **18**, 024041 (2022).
- [59] W. J. Munro, K. A. Harrison, A. M. Stephens, S. J. Devitt, and K. Nemoto, *From quantum multiplexing to high-performance quantum networking*, Nature Photon **4**, 792 (2010).
- [60] A. M. Stephens, J. Huang, K. Nemoto, and W. J. Munro, *Hybrid-system approach to fault-tolerant quantum communication*, Phys. Rev. A **87**, 052333 (2013).
- [61] T. Coopmans, R. Knegjens, A. Dahlberg, D. Maier, L. Nijsten, J. de Oliveira Filho, M. Papendrecht, J. Rabbie, F. Rozpędek, M. Skrzypczyk, L. Wubben, W. de Jong, D. Podareanu, A. Torres-Knoop, D. Elkouss, and S. Wehner, *NetSquid, a NETWORK Simulator for QUantum Information using Discrete events*, Commun Phys **4**, 1 (2021).
- [62] A. Labay Mora, *Genetic algorithm-based optimisation of entanglement distribution to minimise hardware cost*, (2021).
- [63] J. Borregaard, H. Pichler, T. Schröder, M. D. Lukin, P. Lodahl, and A. S. Sørensen, *One-Way Quantum Repeater Based on Near-Deterministic Photon-Emitter Interfaces*, Phys. Rev. X **10**, 021071 (2020).
- [64] A. G. Fowler, D. S. Wang, C. D. Hill, T. D. Ladd, R. Van Meter, and L. C. L. Hollenberg, *Surface code quantum communication*, Phys. Rev. Lett. **104**, 180503 (2010).
- [65] M. Varnava, D. E. Browne, and T. Rudolph, *Loss Tolerance in One-Way Quantum Computation via Counterfactual Error Correction*, Phys. Rev. Lett. **97**, 120501 (2006).
- [66] K. Azuma, K. Tamaki, and H.-K. Lo, *All-photonic quantum repeaters*, Nature Communications **6**, 1 (2015).
- [67] T. van Leent, M. Bock, R. Garthoff, K. Redeker, W. Zhang, T. Bauer, W. Rosenfeld, C. Becher, and H. Weinfurter, *Long-Distance Distribution of Atom-Photon Entanglement at Telecom Wavelength*, Phys. Rev. Lett. **124**, 010510 (2020).

- [68] J. Yin, Y.-H. Li, S.-K. Liao, M. Yang, Y. Cao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, S.-L. Li, R. Shu, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, X.-B. Wang, F. Xu, J.-Y. Wang, C.-Z. Peng, A. K. Ekert, and J.-W. Pan, *Entanglement-based secure quantum cryptography over 1,120 kilometres*, Nature , 1 (2020).
- [69] J. Hofmann, M. Krug, N. Ortegel, L. Gérard, M. Weber, W. Rosenfeld, and H. Weinfurter, *Heralded Entanglement Between Widely Separated Atoms*, Science **337**, 72 (2012).
- [70] L. Kamin, E. Shchukin, F. Schmidt, and P. van Loock, *Exact rate analysis for quantum repeaters with imperfect memories and entanglement swapping as soon as possible*, (2022), arXiv:2203.10318 .
- [71] A. Gilchrist, N. K. Langford, and M. A. Nielsen, *Distance measures to compare real and ideal quantum processes*, Phys. Rev. A **71**, 062310 (2005).
- [72] S. Pirandola, S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, J. S. Shaari, M. Tomamichel, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, *Advances in quantum cryptography*, Adv. Opt. Photon., AOP **12**, 1012 (2020).
- [73] C. H. Bennett, G. Brassard, and N. D. Mermin, *Quantum cryptography without Bell's theorem*, Phys. Rev. Lett. **68**, 557 (1992).
- [74] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, Theoretical Computer Science Theoretical Aspects of Quantum Cryptography – Celebrating 30 Years of BB84, **560**, 7 (2014).
- [75] A. K. Ekert, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett. **67**, 661 (1991).
- [76] G. Murta, F. Rozpędek, J. Ribeiro, D. Elkouss, and S. Wehner, *Key rates for quantum key distribution protocols with asymmetric noise*, Phys. Rev. A **101**, 062321 (2020).
- [77] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *The security of practical quantum key distribution*, Rev. Mod. Phys. **81**, 1301 (2009).
- [78] P. W. Shor and J. Preskill, *Simple Proof of Security of the BB84 Quantum Key Distribution Protocol*, Phys. Rev. Lett. **85**, 441 (2000).
- [79] R. Renner, *Security of Quantum Key Distribution*, (2006), arXiv:0512258 .
- [80] B. Kraus, N. Gisin, and R. Renner, *Lower and upper bounds on the secret key rate for QKD protocols using one-way classical communication*, Phys. Rev. Lett. **95**, 080501 (2005).
- [81] S. Langenfeld, P. Thomas, O. Morin, and G. Rempe, *Quantum Repeater Node Demonstrating Unconditionally Secure Key Distribution*, Phys. Rev. Lett. **126**, 230506 (2021).

- [82] G. Vardoyan and S. Wehner, *Quantum Network Utility Maximization*, (2022), arXiv:2210.08135 .
- [83] A. M. Childs, *Secure assisted quantum computation*, *Quantum Info. Comput.* **5**, 456 (2005).
- [84] A. Broadbent, J. Fitzsimons, and E. Kashefi, *Universal blind quantum computation*, 2009 50th Annual IEEE Symposium on Foundations of Computer Science , 517 (2009), 0807.4154 .
- [85] T. Morimae and K. Fujii, *Blind quantum computation protocol in which Alice only makes measurements*, *Phys. Rev. A* **87**, 050301 (2013).
- [86] J. F. Fitzsimons and E. Kashefi, *Unconditionally verifiable blind quantum computation*, *Phys. Rev. A* **96**, 012303 (2017).
- [87] P. Arrighi and L. Salvail, *Blind quantum computation*, *Int. J. Quantum Inform.* **04**, 883 (2006).
- [88] T. Kapourniotis, E. Kashefi, D. Leichtle, L. Music, and H. Ollivier, *A Framework for Verifiable Blind Quantum Computation*, (2022), arXiv:2206.00631 .
- [89] D. Leichtle, L. Music, E. Kashefi, and H. Ollivier, *Verifying BQP Computations on Noisy Devices with Minimal Overhead*, *PRX Quantum* **2**, 040302 (2021).

3

3

Requirements for a processing-node quantum repeater on a real-world fiber grid

**Guus Avis*, Francisco Ferreira da Silva*,
Tim Coopmans, Axel Dahlberg, Hana
Jirovská, David Maier, Julian Rabbie, Ar-
iana Torres-Knoop and Stephanie Wehner.**

We numerically study the distribution of entanglement between the Dutch cities of Delft and Eindhoven realized with a processing-node quantum repeater and determine minimal hardware requirements for verifiable blind quantum computation using color centers and trapped ions. Our results are obtained considering restrictions imposed by a real-world fiber grid and using detailed hardware-specific models. By comparing our results to those we would obtain in idealized settings we show that simplifications lead to a distorted picture of hardware demands, particularly on memory coherence and photon collection. We develop general machinery suitable for studying arbitrary processing-node repeater chains using NetSquid, a discrete-event simulator for quantum networks. This enables us to include time-dependent noise models and simulate repeater protocols with cut-offs, including the required classical control communication. We find minimal hardware requirements by solving an optimization problem using genetic algorithms on a high-performance-computing cluster. Our work provides guidance for further experimental progress, and showcases limitations of studying quantum-repeater requirements in idealized situations.

Part of the challenge in building quantum repeaters is that their hardware requirements remain largely unknown. Extensive studies have been conducted to estimate such

*These authors contributed equally.

This chapter is based on the preprint arXiv:2207.10579.

requirements both analytically (see, e.g., [1–24]), as well as using numerical simulations (see, e.g., [25–33]). While greatly informative in helping us understand minimal hardware requirements needed to bridge long distances, they have mostly been conducted in idealized settings where all repeaters are equally spaced, and one assumes a uniform loss of typically 0.2 dB/km on each fiber segment (exceptions are [20–22]). Furthermore, with few exceptions [8, 21, 22, 24, 31], such studies only provide rough approximations of time-dependent noise, and do not take into account platform-specific physical effects such as noise on the memory qubits during entanglement generation on NV centers [34] or collective Gaussian dephasing in ion traps (see Figure 3.1).

3.1 Results

In this chapter, we present the first study that takes into account time-dependent noise, platform-specific noise sources and classical control communication, as well as constraints imposed by a real-world fiber network, and optimizes over parameters of the repeater protocols used to generate entanglement. Our investigation is conducted using fiber data from SURF, an organization that provides connectivity to educational institutions in the Netherlands. Specifically, we will consider a network path connecting the Dutch cities of Delft and Eindhoven, separated by 226.5 km of optical fiber (see Figure 3.1 (a)). In placing equipment, we restrict ourselves to SURF locations, which leads to the repeater being located closer to Delft than to Eindhoven. Intermediary stations used for heralded entanglement generation (see Figure 3.1 (b)) cannot be placed equidistantly from both nodes either, as is generally assumed in idealized studies. We emphasize that we restrict ourselves to existing infrastructure, and therefore do not investigate the possibility of altering the fiber links. We direct the interested reader to related work which focuses on determining hardware requirements while taking into account how many repeaters to use and their placement [35].

We consider the case where the network path is used to support an advanced quantum application, namely Verifiable Blind Quantum Computation (VBQC) [36], with a client located in Eindhoven and a powerful quantum-computing server located in Delft. We chose VBQC because since their introduction blind-quantum-computing protocols have attracted a lot of interest, being widely cited as one of the principal future applications of quantum networks (see, e.g., [36–43]). While it is true that VBQC is somewhat unique in that it is highly asymmetrical in terms of the resources it requires from client and server, it is representative for many other quantum-networking applications in that it requires multiple live qubits. Additionally, the noise resilience of the specific VBQC protocol we consider [36] makes it particularly suitable to study the performance of such applications in the presence of hardware imperfections. Specifically, we consider the smallest instance of VBQC, where two entangled pairs are generated between the client and the server. Such entanglement is used to send qubits from the client to the server. We show in Section 3.7 that this can be done through remote state preparation [44]. To set the requirements of our quantum-network path, we impose that its hardware must be good enough to execute VBQC with the largest acceptable error rate [36]. This demand can be translated to requirements on the fidelity and rate at which entanglement is produced. Both depend on the lifetime of the server’s memory, as the server needs to be able to wait until both qubit states have been generated before it can begin processing. Additionally, the requirements on the fidelity and rate can also be understood as the fidelity and rate at which we can

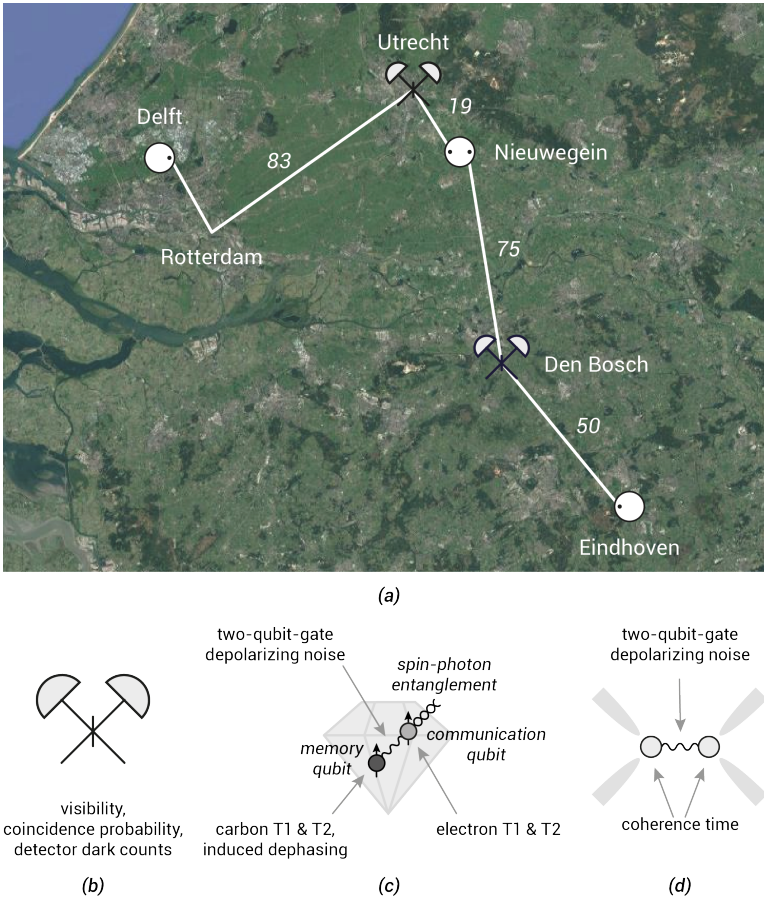


Figure 3.1: **(a)** Satellite photo of the Netherlands overlaid with a depiction of the hypothetical one-repeater setup connecting the Dutch cities of Delft and Eindhoven that we investigate. The white circles represent processing nodes, connected to each other and to heralding stations through fiber drawn in white. The black dots within the processing nodes represent qubits (the distinction between communication and memory qubits is not represented here). The placement of nodes and heralding stations is constrained by the fiber network, and their position on the figure roughly approximates their actual geographic location. All distances are given in kilometers, with a total fiber distance between Delft and Eindhoven of 226.5 km. **(b)** Heralding station. Photons emitted by a processing node travel through the optical fiber and are interfered at a beam splitter. Photon detection heralds entanglement between processing nodes. This process is affected by the overall probability that emitted photons are detected, the coincidence probability, i.e., the probability that photons arrive in the same time window, the imperfect indistinguishability of the photons as measured by the visibility and dark counts in the detector. **(c)** Color center in diamond, one of the processing nodes we investigate. We consider an optically-active electronic spin used as a communication qubit, and a carbon spin used as a memory qubit. Decoherence in both qubits is modeled through amplitude damping and phase damping channels with characteristic times T_1 and T_2 , respectively. These are different for the two qubits. The existence of an always-on interaction between the qubits allows for the execution of two-qubit gates, but also means that entangling attempts with the communication qubit induce noise on the memory qubit. **(d)** Ion trap, the other processing node we investigate. We consider two optically active ions trapped in an electromagnetic field generated by electrodes, whose energy levels are used as qubits. The ions interact through their collective motional modes, which enables the implementation of two-qubit gates. They are subject to collective Gaussian dephasing noise characterized by a coherence time.

deterministically teleport unknown data qubits between the client and the server. Therefore, while our investigation focuses on VBQC, our results can also be interpreted from the perspective of quantum teleportation.

In our study, we obtain the following results, described in more detail below: First, we investigate the *minimal hardware requirements* that are needed to realize target fidelities and rates that allow executing VBQC using our network path. These correspond to the minimal improvements over state-of-the-art hardware parameters that enable meeting the targets. Specifically, we consider parameters measured for networked color centers (specifically, for NV centers in diamond) [45–52] and ion traps [53–60]. We find that considerable improvements are needed even to bridge relatively modest distances, with our study also shining light on which parameters require significantly more improvement than others. To obtain this result, we have built an extensive simulation framework on top of the discrete event simulator NetSquid [61], which includes models of color centers (specifically adapted from NV centers in diamond), ion traps, a general abstract model applicable to all processing nodes, as well as different schemes of entanglement generation. Our framework can be readily re-configured to study other network paths of this form, including the ability to configure other types of processing-node hardware, or entanglement-generation schemes. Being able to simulate the Delft-Eindhoven path, we then perform parameter optimization based on genetic algorithms to search for parameter improvements that minimize a cost function (see Section 6.3 for details) on SURF’s high-performance-computing cluster Snellius.

Second, we examine the *absolute minimal requirements* for all parameters in our models (for color centers and ion traps), if all other parameters are set to their perfect value (except for photon loss in fiber). We observe that the minimal hardware requirements impose higher demands on each individual parameter than the absolute minimal requirements. This highlights potential dangers in trying to maximize individual parameters without taking into account global requirement trade-offs. However, somewhat surprisingly, we find that the absolute minimal requirements are typically of the same order of magnitude as the minimal requirements, and can therefore still be valuable as a first-order approximation. Our results are obtained using the same NetSquid simulation, by incrementally increasing the value of a parameter until the target requirements are met.

Finally, we investigate whether the idealized network paths usually employed in the repeater literature would lead to significantly different minimal hardware improvements. Specifically, in such idealized setups all repeaters and heralding stations are equally spaced, all fibers are taken to have 0.2 dB/km attenuation, and the models employed for the processing-node hardware are largely platform-agnostic. We find that considering real-world network topologies such as the SURF grid imposes significantly more stringent demands.

Let us now be more precise about the setup of our network path, as well as the requirements imposed by VBQC:

3.1.1 Quantum-Network Path

The network path we consider consists of three processing nodes that are assumed to all have the same hardware. That is, the stated hardware requirements are sufficient for all nodes and we do not differentiate between the three nodes. On an abstract level, all processing nodes have at least one so-called communication qubit, which can be used to generate entanglement with a photon. The repeater node in the middle (Nieuwegein,

Figure 3.1 (a)) has two qubits available (at least one of which is a communication qubit) that it can use to simultaneously hold entanglement with the node in Delft, as well as the one in Eindhoven. Once entanglement has been generated with both Delft and Eindhoven, the repeater node may perform an entanglement swap [62] in order to create end-to-end entanglement between Delft and Eindhoven (see Figure 3.2). On processing nodes, such a swap can be realized deterministically, i.e., with success probability 1, since it can be implemented using quantum gates and measurements on the processor. We note that even when the gates and measurements are noisy the swap remains deterministic, although it will induce noise on the resulting entangled state.

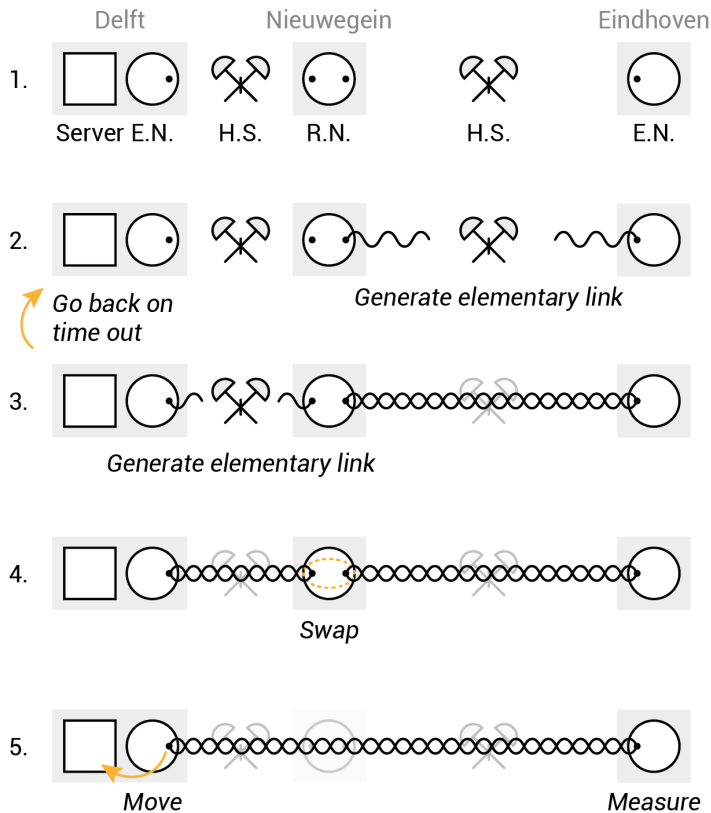


Figure 3.2: Protocol executed in the setup we investigate. 1. No entanglement is shared *a priori*. E.N. stands for End Node, R.N. stands for Repeater Node and H.S. stands for Heralding Station. 2. Entanglement generation attempts begin along the longer link, which connects the repeater node to the Eindhoven node. 3. After entanglement has been established along the longer link, attempts for entanglement generation along the shorter link start. In case this takes longer than a given cut-off time, the previously generated entanglement is discarded and we go back to 2. 4. After entanglement is generated on both links, the repeater node performs an entanglement swap, creating an end-to-end entangled state. 5. The Delft node maps its half of the state to a powerful quantum-computing server, while the Eindhoven node measures its half.

For all types of processing nodes, we here assume the repeater to act sequentially [21] due to hardware restrictions. That is, it can only generate entanglement with one of the other two nodes at a time. To minimize the memory requirements at the repeater node (Nieuwegein), we will always first produce entanglement with the farthest node (Eindhoven). Once this entanglement has been produced, the repeater generates entanglement with the closest node (Delft). To combat the effect of memory decoherence, entangled qubits are discarded after a cut-off time [21]. This means that if entanglement between Delft and Nieuwegein is not produced within a specific time window following the successful generation of entanglement between Nieuwegein and Eindhoven, all entanglement is discarded and we restart the protocol by regenerating entanglement between Nieuwegein and Eindhoven. Classical communication is used to initiate entanglement generation between nodes and notify all nodes when swaps or discards are performed.

We consider three types of processing nodes (see Figure 3.1 (c) and (d)): (1) color centers, specifically modeled on NV centers in diamond, (2) ion traps and (3) a general abstract model applicable to all processing nodes. Let us now provide more specific details on each of these models required for the parameter analysis below.

(1) NV centers are a prominent example of color centers for which significant data is available from quantum-networking experiments [45–50]. Here, the color center’s optically-active electronic spin is employed as a communication qubit. The second qubit is given by the long-lived spin state of a Carbon-13 atom, which is coupled to the communication qubit and used as a memory qubit. Our color-center model accounts for the following:

- Restricted topology, with one optically-active communication qubit and one memory qubit (note however that larger registers have been realized, for example in [52]);
- Restricted gate set, with arbitrary rotations on the communication qubit, Z-rotations on the memory qubit and a controlled rotation gate between the two qubits;
- Depolarizing noise in all gates, bit-flip noise in measurement;
- Qubit decoherence in memory modeled through amplitude damping and dephasing channels with decay times T_1 and T_2 (we consider the experimentally-realized times of $T_1 = 1$ hour (10 hours) and $T_2 = 0.5$ s (1 s) for the communication (memory) qubit [50–52]);
- Induced dephasing noise on the memory qubit whenever entanglement generation using the communication qubit is attempted [34, 49].

The efficiency of the photonic interface in NV centers is limited to 3% due to the zero-phonon line (ZPL). It is likely that executing VBQC using the path we investigate will require overall photon detection probabilities higher than 3%. Little data is presently available for other color centers (SiV, SnV). We hence focus on the NV model, but do allow a higher emission probability, which could be achieved either by using a color center with a more favorable ZPL (65-90% for SiV [63], 57% for SnV [63]), or by placing the NV in a cavity [64]. More details about our color-center model, and a validation of the model against experimental data for NV centers, can be found in Section 3.6.

(2) Trapped ions are charged atoms suspended in an electromagnetic trap, the energy levels of which can be used as qubits. Our trapped-ion model accounts for the following:

- Two identical, optically active ions in a trap;
- Restricted gate set as described in [65], with arbitrary single-qubit Z rotations, arbitrary collective rotations around axes in the XY plane, and an entangling Mølmer-Sørensen gate [66];
- Depolarizing noise in all gates, bit-flip noise in measurement;
- Qubit decoherence modeled as collective Gaussian dephasing, with a characteristic coherence time [31];
- Off-resonant scattering that adds a random delay to the emission time of photons, which is counteracted using a tunable coincidence time window (as captured by a toy model introduced in Section 3.9).

More details about our trapped-ion model, and a validation of the model against experimental data, can be found in Section 3.6.

(3) We further investigate an abstract, platform-agnostic processing-node model. This model accounts for depolarizing noise in all gates and in photon emission, as well as amplitude-damping and phase-damping noise in the memory. It does not account for any platform-specific restrictions on topology, gate set or noise sources. Later on, we show that using the abstract model instead of hardware-specific models leads to an inaccurate picture of minimal hardware requirements. Even so, the abstract model can be valuable to study systems for which hardware-specific models are as of yet unavailable. Additionally, we note that the smaller number of hardware parameters in the abstract model as compared to the hardware-specific models means that the parameter space can be explored more efficiently, making it easier to, e.g., find minimal hardware parameters.

To entangle two processing nodes, one can use different schemes for entanglement generation, and we here consider the so-called single-click [67] and double-click schemes [68]. Both of these start with two distant nodes generating matter-photon entanglement and sending the photon to a heralding station. In the single (double)-click protocol, matter-matter entanglement is heralded by the detection of one (two) photons after interference. The trapped-ion nodes we investigate perform only double-click entanglement generation as single-click entanglement generation has not been realized for the type of trapped-ion devices we consider, i.e., trapped ions in a cavity. The color-center nodes and abstract nodes perform both single and double click. Our entanglement-generation models account for the following physical effects:

- Emission of the photon in the correct mode, modeled through a loss channel;
- Imperfect photon emission modeled through a depolarizing channel;
- Capture of the photon into the fiber, modeled through a loss channel;
- Photon frequency conversion, modeled through a loss channel (as a first-order approximation, we assume this is a noiseless process);
- Photon attenuation in fiber, modeled through a loss channel;
- Photon delay in fiber;

- Photon detection at the detector, modeled through a loss channel;
- Detector dark counts;
- Photon arrival at the detector at different times;
- Imperfect photon indistinguishability.

While photon attenuation losses depend on the characteristics (such as the length) of the fiber that is used to deploy a quantum network, the other losses depend only on the quantum hardware that is used. For convenience we collect all the hardware-related losses into a single parameter, called the photon detection probability excluding attenuation losses.

The hardware parameters used in our models are based on quantum-networking experiments with NV centers (single-click [47–50] and double-click [45, 46]), and trapped ions (double-click [54]).

3.1.2 Blind Quantum Computation

Having discussed our modeling of the path between Delft and Eindhoven, we turn to the end nodes.

Both end nodes are processing nodes. The end node in Eindhoven takes the role of client in the VBQC protocol. In Delft, there is not only an end node, but also a powerful quantum-computing server. After entanglement is established by the end node in Delft it transfers its half of the entangled state to this server. The client in Eindhoven simply measures its half of the entangled state. The Delft scenario is similar to the setting investigated in [69], where the authors consider an architecture in which a node contains two NV centers, one of them used for networking and the other for computing. Here, we make some simplifying assumptions that allow us to focus on the network path: we take the state transfer process to be instantaneous and noiseless, and assume that the computing node is always available to receive the state. Further, we assume that the quantum gates performed by the server are noiseless and instantaneous, and that their qubits are subject to depolarizing noise with memory coherence time $T = 100$ s. Because of these assumptions, the requirements we find are limited primarily by imperfections in the network path itself rather than in the computing node.

We investigate hardware requirements on three processing nodes (two end nodes and one repeater node) so that a client in Eindhoven can perform 2-qubit VBQC, a particular case of the protocol described in [36], using the Delft server. In this protocol, the client prepares qubits at the server, which are then used to perform either computation or test rounds. In test rounds, the results of the computation returned by the server are compared to expected results. The protocol is only robust to noise if the noise does not cause too large an error rate. The protocol is shown in [36] to remain correct if the *maximal* probability of error in a test round can be upper-bounded by 25%. We prove in Section 3.7 that the protocol is still correct if the *average* probability of error in a test round can be upper-bounded by 25%. We further prove in the same section that if the entangled pairs distributed by the network path can be used to perform quantum teleportation at a given rate and quality, the protocol can be executed successfully. Namely, this is true if the average fidelity at which unknown pure quantum states can be teleported using the entangled pairs distributed by the network path (F_{tel}) and the entangling rate R satisfy a specific bound. We note that this bound takes into account potential jitter in the delivery

of entanglement (i.e., the fact that the time required to generate entanglement, and hence the time entangled states need to be stored in memory, can fluctuate around its expected value). We consider two distinct pairs of F_{tel} and R that satisfy this bound as our target metrics, namely:

- Target 1: $F_{\text{tel}} = 0.8717$, $R = 0.1$ Hz,
- Target 2: $F_{\text{tel}} = 0.8571$, $R = 0.5$ Hz.

The choice of these specific values was motivated by the fact that there is no fidelity $F_{\text{tel}} \leq 1$ for $R \approx 0.014$ Hz such that the VBQC condition is satisfied, therefore all target rates should satisfy $R > 0.014$ Hz, preferably with some margin to avoid trivial solutions. Additionally, Target 1 is achievable using either the single-click or double-click protocol and using either one or zero repeaters on the fiber path under consideration, given sufficient hardware improvements. In contrast, Target 2 is achievable only using the single-click protocol and one repeater (see also Sections 3.14.3 and 3.14.4). This suggests that the difference between the two targets is large enough to lead to significantly different results.

The derivation of this bound assumes that the client prepares qubits at the server by first generating them locally and then transmitting them to the server using quantum teleportation. We note that alternatively the remote-state-preparation protocol [44] can be used, which will likely be more feasible in a real experiment as it requires fewer quantum operations by the client. In Section 3.7 we describe a way how the VBQC protocol [36] can be performed using remote state preparation. Note however that we have not investigated the security of the protocol in this case. We show that under the assumption that local operations are noiseless, quantum teleportation and remote state preparation lead to the exact same requirements on the network path. Thus, in case the target is met, VBQC can be successfully executed using either quantum teleportation or remote state preparation. Lastly, we note that there is a linear relation between the average teleportation fidelity F_{tel} and the fidelity of the entangled pair [70].

3.1.3 Minimal Hardware Requirements.

Here, we aim to find the smallest improvements over current hardware to generate entanglement enabling VBQC. These are shown at the bottom of Figure 3.3 for color centers (left) and trapped ions (right). In the table at the top of Figure 3.3 we show a selection of the actual values for the minimal hardware requirements (the set of parameters representing the smallest improvement over state-of-the-art parameters, see Section 6.3 for details on how we determine this), as well as the absolute minimal requirements (the minimal value for each parameter assuming that every other parameter except for photon loss in fiber is perfect). All the parameters are explained in Section 6.3, and their state-of-the-art values that we consider are given in Table 5.1.

The minimal color-center hardware requirements for Target 1 (blue line in Figure 3.3, bottom left) correspond to the usage of a double-click protocol, as we found that this allows for laxer requirements than using a single-click protocol. On the other hand, the minimal requirements for Target 2 (orange line in Figure 3.3, bottom left) correspond to the usage of a single-click entanglement-generation protocol. This is because achieving Target 2 in the setup we studied is not possible at all with a double-click protocol even if every parameter except for photon loss in fiber is perfect. Therefore, and since we do not

model single-click entanglement generation with trapped ions, the bottom-right plot of Figure 3.3 depicts only the requirements for trapped ions to achieve Target 1.

We thus find that in the setup we investigated performance targets with relatively higher fidelity and lower rate are better met by using a double-click protocol. On the other hand, higher rates can only be achieved with single-click protocols. This was to be expected, as (a) states generated with single-click protocols are inherently imperfect, even with perfect hardware and (b) the entanglement-generation rate of double-click protocols scales poorly with both the distance and the detection probability due to the fact that two photons must be detected to herald success.

3

3.1.4 Absolute Minimal Requirements.

We now aim to find the minimal parameter values that enable meeting the targets, if the only other imperfection were photon loss in fiber. These are the absolute minimal requirements, presented in the table at the top of Figure 3.3. We observe that while there is a gap between them and the minimal hardware requirements, it is perhaps surprisingly small. For example, the minimal photon detection probability excluding attenuation losses required to achieve Target 1 with color centers is roughly 1.5 times larger than the corresponding absolute minimal requirement. However, both requirements represent a three order of magnitude increase with respect to the state-of-the-art, which makes a factor of 1.5 seem small in comparison.

We remark on the feasibility of achieving the minimal hardware requirements for color centers. NV centers, on which we have based the state-of-the-art parameters used in this work, are the color center that has been most extensively used in quantum-networking experiments (see [63] for a review). As discussed in Section 6.1, the efficiency of the photonic interface in this system is limited to 3% due to the zero-phonon line. Both targets we investigated place an absolute minimal requirement on the photon detection probability excluding attenuation losses above this value. Improving the photonic interface of NV centers beyond the limit imposed by the zero-phonon line is only possible through integration of the NV center into a resonant cavity [64]. Alternatively, other color centers with a more efficient photonic interface could be considered as alternatives for long-distance quantum communication [63].

Setup			p_{det}	T_{coh} (s)
CC	Baseline		0.00051	0.5
	R = 0.1 Hz	Minimal hardware requirement	0.71	7.2
		Absolute minimal requirement	0.48	1.0
	R = 0.5 Hz	Minimal hardware requirement	0.88	7.5
		Absolute minimal requirement	0.22	1.0
TI	Baseline		0.12	0.085
	R = 0.1 Hz	Minimal hardware requirement	0.96	0.67
		Absolute minimal requirement	0.59	0.42

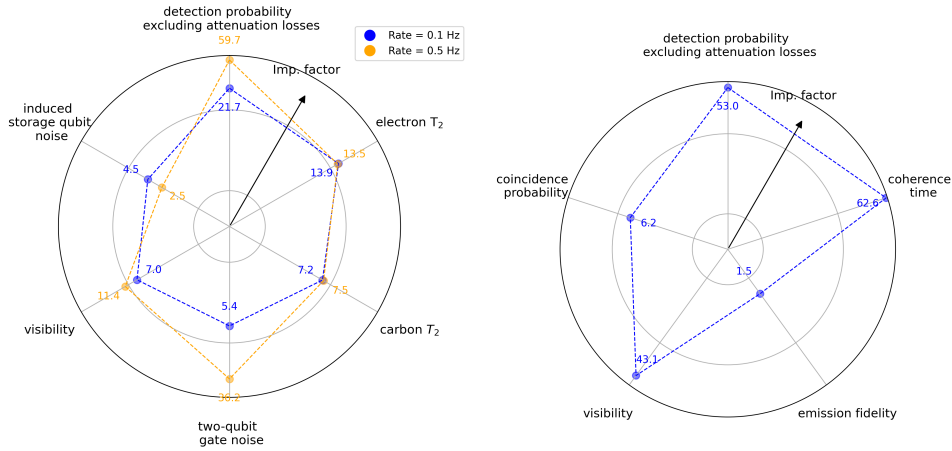


Figure 3.3: **Top:** Parameter values required to connect the Dutch cities of Delft and Eindhoven using color-center (CC) and trapped-ion (TI) repeaters for an entanglement-generation rate of 0.1 Hz and an average teleportation fidelity of 0.8717 (Target 1) and a rate of 0.5 Hz and average teleportation fidelity of 0.8571 (Target 2). The baseline parameter values have been demonstrated in state-of-the-art experiments. The absolute minimal requirements are the required parameter values assuming that there are no other sources of noise or loss with the exception of fiber attenuation. The coherence-time values in the table are the communication-qubit dephasing time for CC and the collective dephasing time for TI (see Section 6.3 for an explanation of these parameters). The TI requirements are for running a double-click entanglement-generation protocol. The CC requirements are for running a double-click protocol for Target 1, and a single-click protocol for Target 2. We note that all the minimal requirements found have a photon detection probability excluding attenuation losses above 30%, the current state-of-the-art value for frequency conversion [57]. **Bottom:** Directions along which hardware must be improved to connect the Dutch cities of Delft and Eindhoven using a CC (**left**) and TI (**right**) repeater. The further away the line is from the center towards a given parameter, the larger improvement that parameter requires. Improvement is measured in terms of the “improvement factor”, which tends to infinity as a parameter tends to its perfect value (see Section 6.3 for the definition). In both plots a logarithmic scale is used. The origin of the plots corresponds to an improvement factor of 1, i.e., no improvement with respect to the state of the art. On the **bottom left** (CC), the blue (orange) line corresponds to the minimal requirements for Target 1 (Target 2). Improvement is depicted for the following parameters, clockwise from the top: photon detection probability excluding attenuation losses in fiber, dephasing time of the communication qubit, dephasing time of the memory qubit, noise in the two-qubit gate, visibility of photon interference and dephasing noise induced on memory qubits when entanglement generation is attempted. On the **bottom right** (TI), the line corresponds to the minimal requirements for Target 1. Improvement is depicted for the following parameters, clockwise from the top: photon detection probability excluding attenuation losses in fiber, qubit collective dephasing coherence time, spin-photon emission fidelity, visibility of photon interference and probability that two emitted photons coincide at the detection station. All parameters are explained in Section 6.3, and their state-of-the-art values that are being improved upon are given in Table 5.1.

3.2 Discussion

3.2.1 Hardware Requirements in Simplified Settings.

Since we made use of real-life fiber data and elaborate, platform-specific hardware models, the results above would be difficult to obtain analytically. For instance, collective Gaussian dephasing in ion traps could be challenging to analyze. Analytical results are however attractive, as they provide a more intuitive picture of the problem at hand. In order to find them, an approach commonly taken in the literature is to simplify the setup under study so that it becomes analytically tractable. A usual simplification is to assume what we name the *standard* scenario, in which nodes and heralding stations are equally spaced, and where the fiber attenuation is 0.2 dB/km throughout. Another common simplification is to consider simplified physical models for the nodes and the entangled states they generate (see, among others, [19, 71–73]). In order to investigate how hardware requirements change if such simplifications are used, we now apply our methodology to these two simplified situations and compare the resulting hardware requirements with the ones for our setup. We hope to understand whether considering these setups leads to similar results, indicating that the simplifying approach is a good one, or if doing so paints an unrealistic picture of the hardware requirements, which would favor our approach.

a. Effect of Existing Fiber Networks on Hardware Requirements We investigate how the hardware requirements in the standard scenario differ from the fiber-network-based setup. We thus present in Figure 3.4 a comparison of the hardware requirements for color centers in the two situations. In both cases, we consider double-click entanglement generation, targeting an entanglement-generation rate of 0.1 Hz and an average teleportation fidelity of 0.8717. Significant improvements over the state-of-the-art are required in both scenarios, but the magnitude of these improvements would be understated in case one were to consider the standard scenario and ignore existing fiber infrastructure. For example, doing so would lead to underestimating the required coherence time of the memory qubits by a factor of four. More broadly, we see that the improvement required is larger in the fiber-network scenario for (i) the photon detection probability excluding attenuation losses and (ii) memory parameters (coherence times and tolerance to entanglement-generation attempts). Both of these results can be explained by the fact that when a real-world fiber network is considered there is more attenuation and the nodes are not evenly spaced. As a consequence, better photonic interfaces are required to achieve similar rates, and states likely spend a longer time in memory, necessitating longer coherence times. This emphasizes the need for considering limitations imposed by existing fiber infrastructure when estimating requirements on repeater hardware.

b. Effect of Platform-Specific Modeling on Hardware Requirements Finally, we look into how the hardware requirements are affected if the processing nodes are modeled in a simplified, platform-agnostic way. We thus compare the hardware requirements for color-center and trapped-ion repeaters with those for a platform-agnostic abstract model for a quantum repeater. This is a simple processing-node model that accounts for generic noise sources such as memory decoherence and imperfect photon indistinguishability, but does not take platform-specific considerations such as restricted topologies into account. For more details on the platform-agnostic abstract model, see Section 3.6.7. We consider double-click entanglement generation in the fiber-network-based setup, targeting an entanglement-generation rate of 0.1 Hz and an average teleportation fidelity of 0.8717.

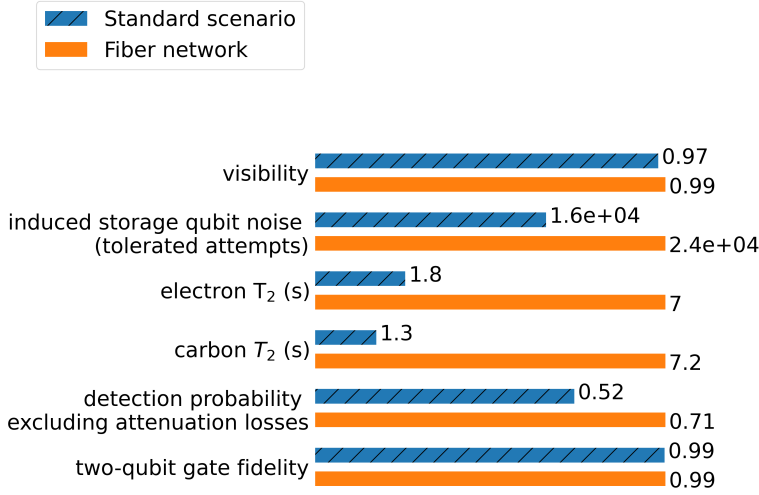


Figure 3.4: Hardware requirements for connecting the Dutch cities of Delft and Eindhoven using a color center repeater performing double-click entanglement generation on an actual fiber network (blue) and assuming the standard scenario (orange, dashed). Requirements are for achieving an entanglement-generation rate of 0.1 Hz and an average teleportation fidelity of 0.8717. Parameters shown are, from top to bottom: visibility of photon interference, dephasing noise induced on memory qubits when entanglement generation is attempted, dephasing time of communication qubit, dephasing time of memory qubit, photon detection probability excluding attenuation losses in fiber and two-qubit gate fidelity.

To perform the comparison, we proceed as follows: (i) map the state-of-the-art hardware parameters to abstract-model parameters, (ii) run the optimization process for the platform-specific model and the abstract model in order to find the minimal hardware requirements for both, (iii) map the obtained platform-specific hardware requirements to the abstract model and (iv) compare them to the hardware requirements obtained by running the optimization process for the abstract model. The results of this comparison can be seen in Figure 3.5. The hardware requirements are significantly different for the abstract model and for the trapped-ion and color-center models. This can be explained by the greater simplicity of the abstract model. Take coherence time as an example. The communication and memory qubits of color centers decohere at different rates, a complexity which is not present in the abstract model. Therefore, improving the coherence time in the abstract model has a bigger impact than improving a given coherence time in the color center model. This means that in the abstract model it is comparatively cheaper to achieve the same performance by improving the coherence time rather than other parameters. The fact that memory noise in trapped ions is modeled differently than in the abstract model (the trapped-ion memory noise is Gaussian, arising from a collective dephasing process. See Equations 3.7 and 3.9) could also explain the difference in the requirements for the coherence times seen in that case.

3.2.2 Entanglement Without a Repeater.

We note that one of the set of targets we investigated, namely an entanglement-generation rate of 0.1 Hz and an average teleportation fidelity of 0.8717, could also be achieved in

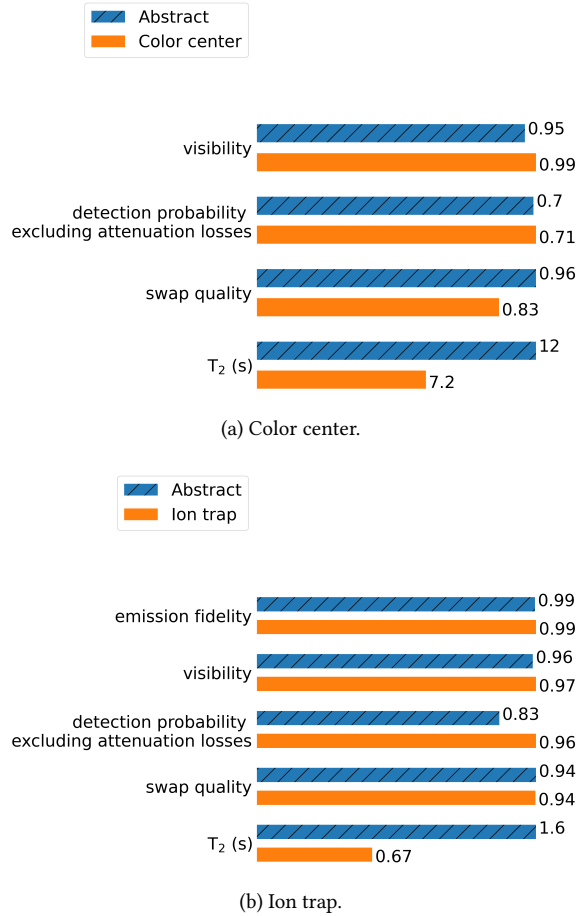


Figure 3.5: Comparison of hardware requirements for connecting the Dutch cities of Delft and Eindhoven using a repeater performing double-click entanglement generation considering a simple abstract model and more detailed color center (left) and ion trap (right) models. Requirements are for achieving an entanglement-generation rate of 0.1 Hz and an average teleportation fidelity of 0.8717. Parameters shown are, from top to bottom: spin-photon emission fidelity (trapped ion only), visibility of photon interference, photon detection probability excluding attenuation losses in fiber, fidelity of entanglement swap and qubit coherence time.

the setup we investigated without using a repeater node if a single-click entanglement-generation protocol were employed. Furthermore, the hardware improvements required would be more modest in this case than if a repeater were used. For more details on this, see Section 3.14.3.

3.2.3 Outlook.

In order to design and realize real-world quantum networks, it is important to determine minimal hardware requirements in more complex scenarios such as heterogeneous networks with multiple repeaters and end nodes. The method presented in this work is well suited for this. Furthermore, it would be valuable to investigate what limitations the assumptions we have made in our modeling place on our results. For example, we did not consider the effects of fiber dispersion. These effects could hamper entanglement generation and hence affect the minimal hardware requirements. Even though preliminary investigations suggest that these effects might be small, quantifying them would represent a step forward in determining realistic minimal repeater-hardware requirements. Another interesting open question is what effect the use of entanglement-distillation protocols (see [74] for a review) would have on the minimal hardware requirements.

3.3 Methods

In this section we elaborate on our approach for determining the minimal and absolute minimal hardware requirements for processing-node repeaters to generate entangled states enabling VBQC.

3.3.1 Conditions on Network Path to Enable VBQC.

In our setup, a client wishes to perform 2-qubit VBQC, a particular case of the protocol described in [36], on a powerful remote server whose qubits are assumed to suffer from depolarizing noise with coherence time $T = 100$ s. We further assume that the computation itself is perfect, with the only imperfections arising from the network path used to remotely prepare the qubits. This protocol is shown in [36] to be robust to noise, remaining correct if the *maximal* probability of error in a test round can be upper-bounded by 25%. We argue in Section 3.7 that the protocol is still correct if the *average* probability of error in a test round can be upper-bounded by 25%, as long as we assume that the error probabilities are independent and identically distributed across different rounds of the protocol. This is the case for the setup studied here, as the state of the network is fully reset after entanglement swapping takes place at the repeater node. This condition, together with the assumption on the server's coherence time, can be used to derive bounds on the required average teleportation fidelity and entanglement-generation rate, as shown in Section 3.7.

3.3.2 Average Teleportation Fidelity.

We use the average teleportation fidelity F_{tel} that can be obtained with the teleportation channel Λ_σ arising from the end-to-end entangled state σ generated by the network we investigate as a target metric:

$$F_{\text{tel}}(\sigma) \equiv \int_{\psi} \langle \psi | \Lambda_\sigma(|\psi\rangle\langle\psi|) | \psi \rangle d\psi, \quad (3.1)$$

where the integral is taken over the Haar measure. See Section 3.7.1 for more details.

3.3.3 Hardware Improvement for VBQC as an Optimization Problem.

We want to find the minimal hardware requirements that achieve a given average teleportation fidelity F_{target} and entanglement-generation rate R_{target} . We restate this as a constrained optimization problem: we wish to minimize the hardware improvement, while ensuring that the performance constraints are met. These constraints are relaxed through scalarization, resulting in a single-objective problem in which we aim to minimize the sum of the hardware improvement and two penalty terms, one for the rate target and one for the teleportation fidelity target. The resulting cost function is given by

$$\begin{aligned} C = & w_1 \left(1 + (F_{target} - F_{tel})^2 \right) \Theta(F_{target} - F_{tel}) \\ & + w_2 \left(1 + (R_{target} - R)^2 \right) \Theta(R_{target} - R) \\ & + w_3 H_C(x_1, \dots, x_N), \end{aligned} \quad (3.2)$$

where H_C is the hardware cost associated with parameter set $\{x_1, \dots, x_N\}$, w_i are the weights of the objectives, Θ is the Heaviside function and F_{tel} and R are the average teleportation fidelity and entanglement-generation rate achieved by the parameter set, respectively. The hardware cost function H_C maps sets of hardware parameters to a cost that represents how large of an improvement over the state of the art the set requires. To compute this consistently across different parameters we use no-imperfection probabilities, as done in [61] (where they are called no-error probabilities). A parameter is improved by a factor k , called the *improvement factor*, if its corresponding no-imperfection probability p_{ni} becomes $\sqrt[k]{p_{ni}}$. For example, if the error probability of a gate is 40%, its probability of no-imperfection is 0.6. After improving it by a factor of 4 the no-imperfection probability becomes $\sqrt[4]{0.6} \approx 0.88$, corresponding to an error probability of approximately 12%. The hardware cost associated with a set of hardware parameters is the sum of the respective improvement factors, i.e.,

$$H_C(x_1, \dots, x_N) = \sum_{i=1}^N \frac{\ln\{p_{ni}(b_i)\}}{\ln\{p_{ni}(x_i)\}}, \quad (3.3)$$

where $p_{ni}(x_i)$ is the no-imperfection probability corresponding to the value x_i of parameter i and $p_{ni}(b_i)$ is the no-imperfection probability corresponding to the baseline value b_i of parameter i . We have here for concreteness used natural logarithms, but the hardware cost is invariant to changes in the logarithms' bases. We note that these improvement factors are the quantities shown in Figure 3.3. The weights w_i are chosen such that the first two terms are larger than the last one for near-term parameters, guaranteeing that the set of parameters minimizing C meets performance targets. We are then effectively restricted to the region of parameter space in which the performance constraints are satisfied, as all points corresponding to near-term parameters in this region have a lower cost than points outside it. The problem then becomes one of minimizing the hardware cost in this region. We have verified that the expected values of the average teleportation fidelity and entanglement-generation rate of the parameter sets found meet the constraints, thus enabling VBQC conditional on our assumptions. Our method guarantees that the set

of parameters found is 'minimal' in the sense that making any of the parameters worse would result in the target not being met. However, we note that there exist many such solutions, and if specific knowledge is available about how hard it is to improve particular parameters, the cost function could be adapted to pick out minimal parameter sets that may be easier to attain. An example of this is the efficiency of the NV center's photonic interface, which is limited to 3% due to the ZPL. Going beyond this limit requires integration into a cavity, which carries with it a host of challenges [63, 64]. One could then modify the cost function to make improving the efficiency of the photonic interface beyond 3% more expensive than improving other parameters. However, as it is challenging to accurately estimate the hardness associated with specific improvements and, furthermore, the hardness may depend on the specific expertise available within a given research group, we have refrained from making such estimates.

3.3.4 Optimization Parameters.

Using the methodology described later on in this section, we perform an optimization over both protocol and hardware parameters. First we enumerate the protocol parameters:

- Cut-off time, the time after which a stored qubit is discarded;
- Bright-state parameter (single-click entanglement generation only), the fraction of a matter qubit's superposition state that is optically active;
- Coincidence time window (double-click entanglement generation with ion traps only), the maximum amount of time between the detection of two photons for which a success is heralded. We model the effect of the coincidence time window using a toy model, see Section 3.9.

Second, we enumerate the hardware parameters:

- The Hong-Ou-Mandel visibility [75] is a measure for the indistinguishability of interfering photons and is defined by [76]

$$1 - \frac{C_{\min}}{C_{\max}}. \quad (3.4)$$

Here C_{\min} is the probability (coincidence count rate) that two photons that are interfered on a 50:50 beamsplitter are detected at two different detectors when the indistinguishability is optimized (as is the case when using interference to generate entanglement), while C_{\max} is the same probability when the photons are made distinguishable.

- The probability of double excitation is the probability that two photons are emitted instead of one in entanglement generation with color centers;
- The induced memory qubit noise is the dephasing suffered by the memory qubit when the communication qubit is used to attempt entanglement generation. The number given for this parameter in Table 5.1 corresponds to the number of electron spin pumping cycles after which the Bloch vector length of the memory qubit in the state $(|0\rangle + |1\rangle)/\sqrt{2}$ in the $X - Y$ plane of the Bloch sphere has shrunk to $1/e$ when the communication qubit has bright-state parameter 0.5 [34];

3

- The interferometric phase uncertainty is the uncertainty in the phase acquired by the two interfering photons when they travel through the fiber in single-click entanglement generation with color centers;
- The photon detection probability excluding attenuation losses is the probability that a photon is detected given that emission was attempted, and assuming that the fiber length is negligible, i.e., considering every form of photon loss (including coupling to fiber) except the length-dependent attenuation loss in fiber;
- Every gate is parameterized by a depolarizing-channel fidelity;
- For color centers, T_1 and T_2 are the characteristic times of the time-dependent amplitude damping and phase damping channels affecting the qubits, and are different for the communication and memory qubits. The effect of the amplitude (phase) damping channel after time t is given by equation (3.5) ((3.6))

$$\begin{aligned} \rho \rightarrow & \left(|0\rangle\langle 0| + \sqrt{e^{-t/T_1}} |1\rangle\langle 1| \right) \rho \\ & \left(|0\rangle\langle 0| + \sqrt{e^{-t/T_1}} |1\rangle\langle 1| \right)^\dagger \\ & + \sqrt{1 - e^{-t/T_1}} |0\rangle\langle 1| \rho \left(\sqrt{1 - e^{-t/T_1}} |0\rangle\langle 1| \right)^\dagger \end{aligned} \quad (3.5)$$

$$\begin{aligned} \rho \rightarrow & \left(1 - \frac{1}{2} \left(1 - e^{-t/T_2} e^{-t/(2T_1)} \right) \right) \rho \\ & + \frac{1}{2} \left(1 - e^{-t/T_2} e^{-t/(2T_1)} \right) Z \rho Z; \end{aligned} \quad (3.6)$$

- For ion traps, the coherence time characterizes the time-dependent collective Gaussian dephasing process that the qubits undergo, which is given by [31]:

$$\rho \rightarrow \int_{-\infty}^{\infty} K_r \rho K_r^\dagger p(r) dr, \quad (3.7)$$

where

$$K_r = \exp \left(-ir \frac{t}{\tau} \sum_{j=1}^n Z_j \right), \quad (3.8)$$

Z_j denotes a Pauli Z acting on qubit j , n is the total number of ions in the trap, τ the coherence time and t the storage time, and

$$p(r) = \frac{1}{\sqrt{2\pi}} e^{-r^2/2}; \quad (3.9)$$

- The noise on matter-photon emission is parameterized by a depolarizing-channel fidelity (i.e., the matter-photon state directly after emission is a mixture between a maximally entangled state and a maximally mixed state);
- The dark-count probability is the probability that a detection event is registered at a detector without a photon arriving.

The state-of-the-art values we use for the hardware parameters are shown in Table 5.1. For more details on how the effects of the different hardware parameters are included in our models, see Section 3.6. We note that some of the hardware parameters we consider in fact conceal trade-offs. For example, the probability of getting a double excitation when using color centers to emit photons can to an extent be tuned. In this case, a lower probability of double excitation would come at the cost of getting fewer events. However, optimizing over all such trade-offs is beyond the scope of this work.

	Color center	Ion trap
Visibility	0.9 [50]	0.89 [54]
Probability of double excitation	0.06 [50]	-
Induced memory qubit noise (entanglement attempts until dephasing)	5300 [50]	-
Interferometric phase uncertainty (rad)	0.21 [50]	-
Photon detection probability excluding attenuation losses	5.1×10^{-4} [50]	0.111 [55–57]
Two-qubit gate fidelity	0.97 [47]	0.95 [53]
Two-qubit gate duration	500 μ s [47]	107 μ s [53]
Communication T1	1 h [51]	-
Communication T2	0.5 s [50]	-
Memory T1	10 h [52]	-
Memory T2	1 s [52]	-
Coherence time	-	85 ms [53]
Matter-photon emission fidelity	1 [77]	0.99 [78]
Matter-photon emission duration	3.8 μ s [49]	50 μ s [53, 56]
Dark count probability	1.5×10^{-7} [50]	1.4×10^{-5} [55]

Table 3.1: State-of-the-art color center and trapped-ion hardware parameters. For the trapped-ion parameters, a detection time window of 17.5 μ s and a coincidence time window of 0.5 μ s are assumed (see Section 3.6 for more details). All fidelities are depolarizing-channel fidelities. A dash (“-”) indicates that a value would not be well defined (for instance, there is no T1 or T2 time defined for trapped ions, while there is no coherence time defined for color centers). We note that not all of these parameter values have been realized in a single experiment.

3.3.5 Evaluating Hardware Quality.

In order to minimize the cost function C , we require an efficient way of evaluating the performance attained by each parameter set. We do this through simulation of end-to-end entanglement generation using NetSquid. The full density matrix of the states generated, as well as how long their generation took in simulation time are recorded and used to compute the average teleportation fidelity and rate of entanglement generation. Since entanglement generation is a stochastic process, multiple simulation runs are performed in order to collect representative statistics.

3.3.6 Framework for Simulating Quantum Repeaters.

In our NetSquid simulation framework, we have implemented hardware models for color centers, trapped ions and a platform-agnostic abstract model. This includes the implementation of different circuits for entanglement swapping and moving states for each

platform, conditioned on their respective topologies and gate sets. Additionally, we have implemented both single and double-click entanglement-generation protocols. In order to combine these different building blocks that are required to simulate end-to-end entanglement distribution, we define services that each have a well-defined input and output but can have different implementations. For example, the entanglement-generation service can either use the single-click or double-click protocol, and entanglement swapping can be executed on either color center or trapped-ion hardware. End-to-end entanglement generation is then orchestrated using a link-layer protocol (inspired on the one proposed in [79]) that makes calls to the different services, agnostically of how the services are implemented. This allows us to use the same protocol for each different configuration of the simulation. Switching between configurations in our simulation framework then only requires editing a human-readable configuration file. The modularity of the simulation framework would make it simple to investigate further hardware platforms and protocols.

The link-layer protocol is itself an implementation of the link-layer service defined in [79]. From a user perspective, this simplifies using the simulation as all that needs to be done to generate entanglement is make a call to the well-defined link-layer service, without any knowledge of the protocol that implements the service. In this work, the link-layer protocol is the one for a single sequential repeater illustrated in Figure 3.2. However, the protocols included in our simulation code are able to simulate entanglement generation on chains of an arbitrary number of (sequential) repeaters that use classical communication to negotiate when to generate entanglement and that implement local cut-off times.

3.3.7 Finding Minimal Hardware Improvements.

In order to find the sets of parameters minimizing the cost function C , we employ the optimization methodology introduced in [80], which integrates genetic algorithms and NetSquid simulations. A genetic algorithm is an iterative optimization method, which initiates by randomly generating a population consisting of many sets of parameters, also known as individuals. These are then evaluated using the NetSquid simulation and the cost function, and a new population is bred through mutation and crossover of individuals in the previous population. The process then iterates, with better-performing individuals being more likely to propagate to further iterations. For further details on the optimization methodology employed, see Section 3.11 and [80].

This methodology is computationally intensive, so we execute it on the Snellius supercomputer. We use one node of the Snellius supercomputer, which contains 128 2.6 GHz cores and a total of 256 GiB of memory. Based on previously observed data reported in [80], we employ a population size of 150 evolving for 200 generations. The simulation is run 100 times for each set of parameters, as we have empirically determined that this constitutes a good balance between accuracy and computation time. The time required for the procedure to conclude is hardware, protocol and parameter dependent, but we have observed that 10 wall-clock hours are typically enough. We stress that this approach is general, modular and freely available [80].

3.3.8 Finding Absolute Minimal Hardware Requirements.

In order to find these requirements, which are the minimal parameter values enabling meeting the performance targets if the only other imperfection is photon loss in fiber, we perform a sweep of each parameter, starting at the state-of-the-art value and termi-

nating when the targets are met. For each value of each parameter, we sweep also over the protocol parameters, i.e., the cut-off time, coincidence time window (for double-click entanglement generation with ion traps) and bright-state parameter (for single-click entanglement generation).

3.4 Data availability

The data presented in this work have been made available at <https://doi.org/10.4121/19746748>.

3

3.5 Code availability

The code that was used to perform the simulations and generate the plots in this chapter has been made available at <https://gitlab.com/softwarequtech/simulation-code-for-requirements-for-a-processing-node-quantum-repeater-on-a-real-world-fiber-grid>.

Author contributions

G.A. led the development of hardware models and the simulation of repeater protocols. F.F.S. led the development and execution of optimizations. G.A. and F.F.S. devised the target metric and proved the underlying theorems related to verifiable blind quantum computation. G.A., F.F.S., D.M., T.C., A.D., H.J. and J.R. contributed to the development of the code used in the simulations. A.T. contributed to the optimal execution of simulations on computing clusters. G.A., F.F.S. and S.W. wrote the manuscript. All authors revised the manuscript. S.W. conceived and supervised the project.

3.6 Setup

In this section, we elaborate on our modeling of the setup we study. We go over the topology of the fiber network we considered, the protocols employed by the repeater nodes, the modeling of the nodes themselves and of entanglement generation.

3.6.1 Fiber network and node placement

Deployment of quantum networks in the real world will likely make use of existent fiber infrastructure, as we have discussed in Chapter 1. In order to accurately account for this in our investigation of repeater hardware requirements, we used data of SURF's fiber network in our simulation. SURF is a network provider for education and research institutions in the Netherlands. The data we have access to consists of the physical location in which nodes are placed, the length of the fibers connecting them, the measured attenuation of each fiber and their dispersion. We restricted the placement of quantum nodes and heralding stations to existing nodes in the network, and we assumed that they were connected by the shortest length of fiber possible. We note that in the case we studied this corresponds also to the least overall attenuation. Although dispersion was not considered in our models, an investigation of its effects would constitute an interesting extension to this work. There are four nodes in the shortest connection between Delft and Eindhoven in SURF's network, as depicted in Figure 3.6. This means we are restricted to placing a single repeater between the end nodes, as a two-repeater setup would require five nodes in total, two for the repeaters and three for the heralding stations. A single-repeater setup, on

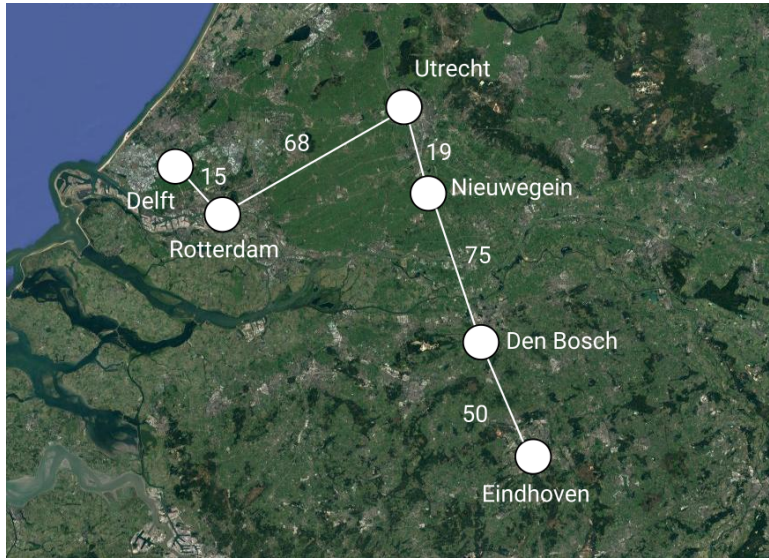


Figure 3.6: Satellite photo of the Netherlands overlaid with depiction of the shortest connection between the Dutch cities of Delft and Eindhoven in SURF’s fiber network. The white circles represent locations where processing nodes and heralding stations can be placed, and are connected to one another through white fibers. The position of the circles in the figure roughly approximates their actual physical location. All distances are given in kilometers.

the other hand, requires only three nodes, one for the repeater itself and two for heralding stations. One of the connection’s nodes must therefore not be used, and there are two possible choices for how this can be done, as depicted in Figure 3.7. We applied our methodology to both of these paths and determined that the one on the left in Figure 3.7 requires a smaller improvement over current hardware. Therefore, all the results presented in Section 6.1 pertain to it. For more details, see Section 3.14.2.

3.6.2 Repeater protocol

We now elaborate on the protocol executed by the nodes. We note that the repeaters we investigate are sequential, which means that they can only generate entanglement with one neighbor at a time.

1. A request for end-to-end entanglement generation is placed at one of the end nodes.
2. This end node sends a classical message through the fiber to the other end node, in order to verify whether it is ready to initiate the entanglement generation protocol.
3. If that is the case, the second end node sends a confirmation message back, as well as an activation message for the repeater node.

The next step is the generation of elementary link states. We begin by generating entanglement on the Eindhoven - Nieuwegein link, which is longest, so as to minimize the time states remain in memory.



Figure 3.7: Two possible choices for processing node (white circles, black circles within represent qubits) and heralding station placement in the SURF network's shortest connection between the Dutch cities of Delft and Eindhoven. In the path on the left, the Rotterdam node is unused, thereby directly connecting the Delft - Rotterdam and Rotterdam - Utrecht links. Similarly, the Den Bosch node is unused in the path on the right.

4. The neighboring Eindhoven and Nieuwegein nodes share classical messages sent through the fiber connecting them to ensure that both agree to generate entanglement.
5. Once they have established agreement, entanglement generation attempts begin and continue until success.
6. Steps 4 and 5 are repeated by the repeater and the Delft end node.
7. The repeater performs a Bell-state measurement on the two qubits it holds, thereby creating an entangled state held by the end nodes.
8. The outcome of this measurement is sent as a classical message to both end nodes.
9. The end nodes become aware that end-to-end entanglement has been established and perform the appropriate correction on the Bell state.

We also employ a cut-off protocol. If the generation of the second entangled state lasted longer than a predefined cut-off time, the first state, corresponding to the longer link, is discarded. Entanglement generation then restarts along the longer link.

Such a protocol involving sequential repeaters and a cut-off timer has been studied before, e.g., in [22]. The steps above are sufficient to generate one end-to-end entangled state. If the generation of multiple states had been requested, steps 4-9 would be repeated until enough pairs had been generated. We note that we do not simulate the application of the Bell-state correction, but instead record which correction should have been applied and handle it in post-processing.

Information on how we implemented such a protocol in a scalable and hardware-agnostic fashion can be found in Section 3.13.

3.6.3 Quantum-computing server

After the end-to-end entangled state has been generated, we assume the end node in Delft transfers its half of it to a powerful quantum-computing server. This is a similar setting as the one investigated in [69], where the authors consider an architecture in which a node contains two NV centers, one of them used for networking and the other for computing. We assume that the state transfer process is instantaneous and noiseless and that the server is always available to receive the state. Additionally, we assume that all quantum gates performed by the server are noiseless and instantaneous, and that qubits stored in the server are subject to depolarizing memory noise with a coherence time of $T = 100$ s.

3.6.4 Processing nodes

The quantum nodes we investigated are processing nodes, i.e. quantum nodes that are capable of storage and processing of quantum information. This processing is done through noisy quantum gates. The specific gate set available to the nodes depends on the particular hardware, but we model the gate noise of all of them with depolarizing channels. Measurements are also noisy, which is captured by a bit-flip channel, i.e. with some probability a $|0\rangle$ ($|1\rangle$) is read as 1 (0). Furthermore, as already mentioned, all the nodes we investigate are sequential, which means that they can only generate entanglement with one other node at a time.

We now elaborate on the details of our modeling for each of the three nodes we study.

3.6.5 Color centers

In Table 3.2, we present the baseline values of all color center hardware parameters relevant to our simulations, as well as references reporting their experimental demonstration.

Parameter	Noise	Duration/Time
Visibility	0.9 [50]	-
Probability of double excitation	0.06 [50]	-
$N_{1/e}$: Nuclear dephasing during electron initialization	5300 [50]	-
Dark count probability	1.5×10^{-7} [50]	-
σ_{phase} : Interferometric phase uncertainty (rad)	0.21 [50]	-
Photon detection probability excluding attenuation losses	5.1×10^{-4} [50]	-
Spin-photon emission	F = 1 [77]	3.8 μs [77]
Electron readout	F=0.93(0), 0.995(1) [50]	3.7 μs [48]
Carbon initialization	F=0.99 [52]	300 μs [81]
Carbon Z-rotation	F=0.999 [82]	20 μs [82]
Electron-carbon controlled X-rotation	F=0.97 [47]	500 μs [47]
Electron initialization	F=0.995 [52]	2 μs [83]
Electron single-qubit gate	F=0.995 [50]	5 ns [47]
Electron T1	-	1 hours [51]
Electron T2	-	0.5 s [50]
Carbon T1	-	10 hours [52]
Carbon T2	-	1 s [52]

Table 3.2: Baseline color center hardware parameters.

Color center nodes are modeled with a star topology, with the communication qubit in the middle. The memory qubits can all interact with the communication qubit, but not with one another. The communication qubit owes its name to the fact that it is optically active, which means it can be used for light-matter entanglement generation. The spin states of the memory qubits are long-lived, so they are typically used for information storage. We model memory decoherence in color center qubits through amplitude damping and phase damping channels with T_1 and T_2 lifetimes. The effect of the amplitude (phase) damping channel after time t is given by equation (3.10) ((3.11)).

$$\begin{aligned} \rho \rightarrow & \left(|0\rangle\langle 0| + \sqrt{e^{-t/T_1}} |1\rangle\langle 1| \right) \rho \left(|0\rangle\langle 0| + \sqrt{e^{-t/T_1}} |1\rangle\langle 1| \right)^\dagger \\ & + \sqrt{1 - e^{-t/T_1}} |0\rangle\langle 1| \rho \left(\sqrt{1 - e^{-t/T_1}} |0\rangle\langle 1| \right)^\dagger \end{aligned} \quad (3.10)$$

$$\rho \rightarrow \left(1 - \frac{1}{2} \left(1 - e^{-t/T_2} e^{-t/(2T_1)} \right) \right) \rho + \frac{1}{2} \left(1 - e^{-t/T_2} e^{-t/(2T_1)} \right) Z \rho Z \quad (3.11)$$

The T_1 and T_2 lifetimes of the communication qubit are different from those of the memory qubits. An entangling gate is available in the form of a controlled X-rotation between the communication qubit and each memory qubit. Furthermore, arbitrary single-qubit rotations can be implemented on the communication qubit.

The constrained topology and gate set of the color center place some limitations on the quantum circuits to be executed. First of all, the typical Bell-state-measurement circuit must be adapted, as depicted in Figure 17 (d) of the Supplementary Information of [61]. Furthermore, since only the communication qubit can be used to generate light-matter entanglement, the repeater node must move its half of the first entangled state it generates from the communication qubit to a memory qubit in order to free it up to generate the second entangled state. The circuit for this move operation can be seen in Figure 17 (a) of the Supplementary Information of [61].

Finally, we note that it might be advantageous for the end node in Eindhoven, which generates entanglement with the repeater first and then has to wait, to map its half of the elementary link entangled state from the communication qubit to the memory qubit while it waits for the repeater node to generate entanglement with the Delft node. Note that this has nothing to do with the fact that the end node in Delft transfers its qubit to the powerful quantum-computing server after end-to-end entanglement is established. There is however a trade-off: while mapping the state means that it will be held in a qubit with a longer coherence time, it will also undergo extra decoherence due to the noise in the gates that constitute the circuit for the move operation. We have investigated this trade-off by applying our methodology to the two situations, and found that not mapping requires a smaller improvement over current hardware. Therefore, the color center results shown in the main text pertain to the situation in which the Eindhoven node does not map its half of the entangled state to a memory qubit. We must however note that this finding is specific to both the topology we study and the baseline hardware quality we consider. For more details on the comparison between mapping and not mapping, see Section 3.14.1.

The color center hardware model we employed builds on previous work [22, 79], and its NetSquid implementation has been validated against experiments [61]. This includes the model for the processor as well as for the entangled states generated through a single-click protocol. The main novelty introduced in this work regarding color center modelling is a model for the entangled states generated through the Barrett-Kok protocol [68]. This is essentially the model introduced in Section 3.8, with the addition of induced dephasing noise. This addition accounts for the fact that every entanglement generation attempt induces dephasing noise on the color center's memory qubits [34]. We simulate this effect using a dephasing channel. The dephasing probability p , accumulated after possibly multiple entanglement generation attempts, is given by equation (3.12).

$$p = \frac{1 - (1 - 2p_{\text{single}})^k}{2}. \quad (3.12)$$

In this equation, p_{single} is the probability of dephasing after a entanglement generation attempt and k is the number of required entanglement generation attempts. In our simulations, we apply a dephasing channel of parameter p twice after entanglement has been successfully generated, to reflect the fact that each attempt requires the emission of two photons. p_{single} can be related to $N_{1/e}$, the number of electron spin pumping cycles after which the Bloch vector length of a nuclear spin in the state $(|0\rangle + |1\rangle)/\sqrt{2}$ in the $X - Y$

plane of the Bloch sphere has shrunk to $1/e$ when the electron spin state has bright-state parameter $\alpha = 0.5$, through equation (3.13).

$$p_{\text{single}} = (1 - \alpha)(1 - e^{-1/N_{1/e}}). \quad (3.13)$$

$N_{1/e}$ can in turn be experimentally determined, and $N_{1/e} = 5300$ for state-of-the-art color center experiments [49].

The double-click model is the only component of our color center simulations that had not yet been compared to experimental data. With this in mind, we validated it against the experiment reported in [45]. There, the authors demonstrated heralded entanglement generation between two color centers separated by three meters using the Barrett-Kok protocol. After establishing entanglement, measurements of the two entangled qubits were performed to investigate whether the outcomes were correlated as expected. This was repeated for the X and Z bases, and for the states $|\Psi^\pm\rangle = 1/\sqrt{2}(|01\rangle \pm |10\rangle)$. We replicated this setup using our color center NetSquid model and ran the experiment 10000 times per measurement basis in order to gather relevant statistics. The results of this validation are shown in Figure 3.8. The results obtained with our simulation model broadly replicate

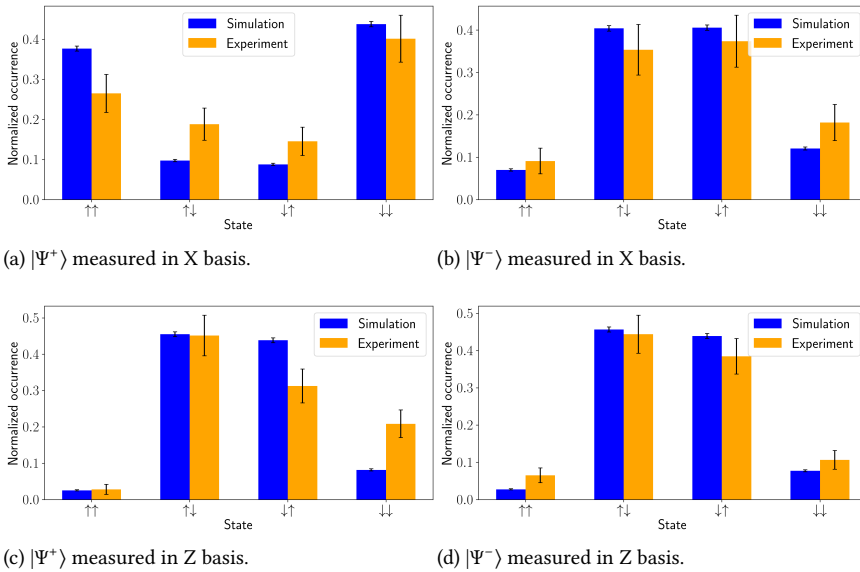


Figure 3.8: Comparison of measurement outcomes of the entangled state generated using the Barrett-Kok protocol in the experiment described in [45] and our simulation of the same scenario. The plots on the left (right) correspond to the case in which the state $|\Psi^+\rangle = 1/\sqrt{2}(|01\rangle + |10\rangle)$ ($|\Psi^-\rangle = 1/\sqrt{2}(|01\rangle - |10\rangle)$) is generated. The plots above (below) show the outcomes when measuring in the X (Z) basis. The error bars depict the standard error of the mean. Anti-correlation of the spin states is expected for every plot except for the one in the top left, for which we expect to see a correlation. The smaller dimension of the simulation error bars can be attributed to the number of executions of the protocol, which was of the order of 10000 per plot. This is two orders of magnitude more than what was performed experimentally.

the experimental results, although they do not lie within the statistical error bars. Overall, the simulation results are closer to the ideal case of perfect (anti-)correlation. This

can be explained by the fact that our model for the double-click states is quite simple and hardware-agnostic, ignoring noise sources such as the probability of double photon emission. Further, the number of experimental data points is small, of the order of a total of 100 events for each of the plots in the figure. Nonetheless, considering the simplicity of the model, we believe that the level of agreement is satisfactory.

3.6.6 Trapped ions

3

In Table 3.3, we present the baseline values of all trapped-ion hardware parameters relevant to our simulations, as well as references to the articles reporting their experimental demonstration.

Parameter	Noise	Duration/Time
Visibility	0.89 [54]	-
Dark count probability	1.4×10^{-5} [55]	-
Photon detection probability excluding attenuation losses	0.111 [55–57]	-
Ion-photon emission	$F = 0.99$ [78]	$50 \mu\text{s}$ [53, 56]
Readout	$F=0.999(0), 0.99985(1)$ [58]	1.5 ms [54]
Initialization	$F=0.999$ [59]	$36 \mu\text{s}$ [53]
Z-rotation	$F=0.99$ [60]	$26.6 \mu\text{s}$ [60]
Mølmer-Sørensen gate	$F=0.95$ [53]	$107 \mu\text{s}$ [53]
Coherence time	-	85 ms [53]

Table 3.3: Baseline trapped-ion hardware parameters. A detection time window of $17.5 \mu\text{s}$ is assumed. For the visibility, a coincidence time window of $0.5 \mu\text{s}$ is assumed (see Section 3.6.6 for further explanation). The photon detection probability excluding attenuation losses includes a 30% efficiency factor for quantum frequency conversion [57]. It is based on a detection efficiency of 0.43 for a 46(1) MHz drive laser and a detection time window of $17.5 \mu\text{s}$ [56]. However, the number from [56] is based on a detector efficiency of 0.87(2) for photons at 854 nm. The detection efficiency at telecom frequency would instead be 0.75 using superconducting nanowire detectors [55], giving an additional conversion factor of $0.75/0.87$. The dark count probability is based on a 0.8 Hz dark count rate for telecom superconducting nanowire detectors [55] multiplied by $17.5 \mu\text{s}$. The ion-photon emission fidelity has been corrected for the 1.5% infidelity due to dark counts in [78]. The initialization duration includes time for cooling sequences and repumping (3 ms of cooling for 230 photon generation attempts on one ion, with $40 \mu\text{s}$ for repumping and optical pumping in 30 of the attempts and $20 \mu\text{s}$ in 200 of the attempts, averaging at $\sim 36 \mu\text{s}$ per attempt [60]).

In this work, we present for the first time a NetSquid model for trapped-ion nodes in quantum networks. The trapped-ion nodes we model are based on the state of the art for trapped ions in a cavity, which consists of $^{40}\text{Ca}^+$ ions in a linear Paul trap [31, 55, 56, 65, 78, 84–90] (we note that promising results have also been achieved for trapped ions without cavities, these systems are however not considered in this work [91–95]). In our model they have all-to-all connectivity, their qubits all have the same coherence time and can all be used to generate light-matter entanglement. However, the node can only generate entanglement with one remote node at a time.

Decoherence in n trapped-ion qubits is modeled through a collective Gaussian dephas-

ing channel that has the following effect on the n -qubit state ρ [31]:

$$\rho \rightarrow \int_{-\infty}^{\infty} K_r \rho K_r^\dagger p(r) dr, \quad (3.14)$$

where

$$K_r = \exp\left(-ir \frac{t}{\tau} \sum_{j=1}^n Z_j\right), \quad (3.15)$$

Z_j denotes a Pauli Z acting on qubit j , τ the coherence time and t the storage time, and

$$p(r) = \frac{1}{\sqrt{2\pi}} e^{-r^2/2}. \quad (3.16)$$

This can be read as follows: the qubits dephase because they undergo Z -rotations at an unknown constant rate of $-2r$ per coherence time τ . This is modeled by sampling the Gaussian distribution for the dephasing rate, $p(r)$, for each ion trap each time its state is reset. The qubits are then time-evolved by applying unitary rotations in accordance with the sampled value for r . The baseline value $\tau = 85$ ms included in Table 3.3 is obtained from [53]. However, the value for the coherence time reported there is 62 ± 3 ms. The reason for this discrepancy is a difference in convention. To see this, we can evaluate equation (3.14) for $n = 1$, i.e., for a single qubit. In that case, we find

$$\rho \rightarrow \lambda \rho + (1 - \lambda) Z \rho Z, \quad (3.17)$$

where

$$\lambda = \frac{1}{2} \left(1 - e^{-2\left(\frac{t}{\tau}\right)^2} \right). \quad (3.18)$$

The single-qubit dephasing model used in [53] instead has

$$\rho \rightarrow \lambda' \rho + (1 - \lambda') Z \rho Z, \quad (3.19)$$

where

$$\lambda' = \frac{1}{2} \left(1 - e^{-\left(\frac{t}{\tau'}\right)^2} \right). \quad (3.20)$$

Here, τ' is the coherence time in their model. The models are exactly equivalent for $\tau = \sqrt{2}\tau'$. Therefore, the reported value $\tau' = 62 \pm 3$ ms corresponds to $\tau = 88 \pm 4$ ms. The value we use, $\tau = 85$ ms, represents a conservative interpretation of the result presented in [53]. Our model for the storage of quantum states in ionic qubits has been validated against experimental data from [53]. In this experiment, ion-photon entanglement is created with one ion in a two-ion device. Next, ion-photon entanglement is created with the other ion every $330\mu\text{s}$. Our simulation results are compared to the experimental results in Figure 3.9.

The entangling gate available to the trapped-ion qubits as we model them is the Mølmer-Sørensen gate [66]. The gate set also includes arbitrary single-qubit Z -rotations and collective rotations around a tunable axis in the XY plane [65]. The Bell-state-measurement

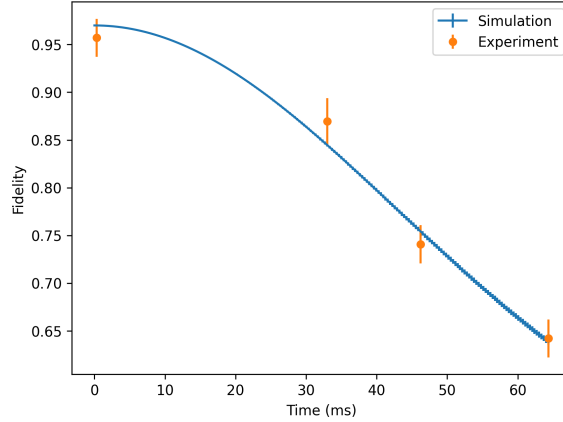


Figure 3.9: Validation of our trapped-ion decoherence model against an experiment in [53]. In the experiment, a trap with two ions first emits a photon entangled with the first ion, and then keeps emitting new photons entangled with the second ion every $330 \mu\text{s}$. The figure shows the evolution of the fidelity to the perfect Bell state of the state shared by the first ion and the photon entangled to it as a function of time. Error bars of the simulation results represent the standard error of the mean and are sometimes hard to distinguish because of their size. The simulation has been conducted using the baseline coherence time $\tau = 85 \text{ ms}$, which is the value obtained from [53]. The ion-photon emission fidelity has been set to $F = 0.97$ to tune the fidelity at time zero such that good agreement between the simulation and the experiment is obtained. All other parameters have been set to their perfect values.

circuit is implemented as a Z-rotation of angle $\pi/4$ for one qubit and $-\pi/4$ for the other, a Mølmer-Sørensen gate and a measurement of both qubits in the computational basis. All gates are modeled as a perfect gate followed by depolarizing channels on all partaking qubits.

Just as for color centers, entanglement generation through the Barrett-Kok protocol is modeled using the model introduced in Section 3.8. A difference with color centers, however, is that the photons emitted by ions are typically temporally impure due to off-resonant scattering [87], resulting in low Hong-Ou-Mandel visibility and hence entangled-state fidelity. This can be counteracted by using a stringent detection time window and by imposing a coincidence time window. A click pattern is then only heralded as a success in case both clicks fall within the detection time window and the time between the two clicks does not exceed the coincidence time window. The detection time window and coincidence time window can be tuned to increase the visibility, but at the cost of having a smaller success probability. In order to account for the effect of the detection time window, we employ a toy model for the temporal state of photons emitted from trapped-ion devices. This toy model does not accurately represent the true state of the emitted photons, but as we show in Figure 3.10, it can be used to capture the trade-off between success probability and visibility well. In this toy model, we model photons as mixtures of pure photons emitted at different times. The pure photons have one-sided exponential wavefunctions, and the emission time is also distributed according to a one-sided exponential. Under these assumptions, the detection probability, coincidence probability and visibility can all be exactly calculated as a function of the in total two parameters that describe these two exponentials. These calculations are performed in Section 3.9, and the results can be used

in conjunction with the model in Section 3.8 to calculate the success probability and state. To show that this model can be used to capture the success probability and visibility with good accuracy, we have performed a joint least-square procedure for the detection-time probability density function, the coincidence probability and the visibility to match the two free parameters to the data presented in [87]. This data has been produced by emitting two photons from the same trapped-ion device, frequency converting these photons, and then making them interfere. In Figure 3.10 (a), we show the resulting theoretical results and compare them to the experimental results.

Instead of basing the parameters we use in our simulations on [87], we base them on data for the interference of photons emitted by two distinct ion traps [54], as this more accurately represents the scenario we investigate in this study. We determine again the two parameters that describe the two exponentials by fitting to the data using the exact same method as above. The half-life time of the fitted exponentials representing the wave function and the emission time were found to be $3.01 \mu\text{s}$ and $6.79 \mu\text{s}$ respectively, with the fits and the data shown in Figure 3.10 (b). This data has been taken using a detection time window of $17.5 \mu\text{s}$. Therefore, for consistency, we use a fixed detection time window of $17.5 \mu\text{s}$ throughout our simulations, and hence the parameters shown in Table 3.3 (such as, e.g., the photon detection probability excluding attenuation losses and the dark count probability) all assume a detection time window of $17.5 \mu\text{s}$. On the other hand, the coincidence time window is treated as a freely tunable parameter, allowing for a trade-off between rate and fidelity. The value for the visibility reported in Table 3.3 and Table II of the main text was obtained from the model in Section 3.9 using the fitted parameters reported above, a detection time window of $17.5 \mu\text{s}$ and a coincidence time window of $0.5 \mu\text{s}$.

We note that [87] includes a physically-motivated theoretical model for the trade-off between coincidence probability and visibility as a function of the detection and coincidence time windows. We have not used their model here as it requires numerical integration to evaluate, while our model can be rapidly evaluated using an analytical closed-form expression. Additionally, our goal here is not to predict the behaviour of a specific physical system but to accurately represent the trade-off between rate and fidelity without overfitting to experimental data. Finally, as our toy model does not attempt to closely capture the physics of any individual system, it can be considered to be system agnostic. It could thus be fitted to different types of photon sources, giving it a potentially broader scope of application.

3.6.7 Abstract nodes

The purpose of the abstract nodes is to provide a general model for processing nodes. Therefore, their modeling is kept simple and platform-agnostic: there is all-to-all connectivity between the qubits, all of them can be used to generate light-matter entanglement, they all have the same coherence time properties and all quantum gates are available. The Bell-state measurement circuit implemented by abstract nodes is the usual one: a controlled-NOT gate, followed by a Hadamard on the control qubit and a measurement of both qubits in the computational basis. We note that this model and its NetSquid implementation are not novel, having first been introduced in [80].

In order to quantify the level of accuracy that is sacrificed by considering a model with a higher degree of abstraction, we compare the performance of a single abstract-

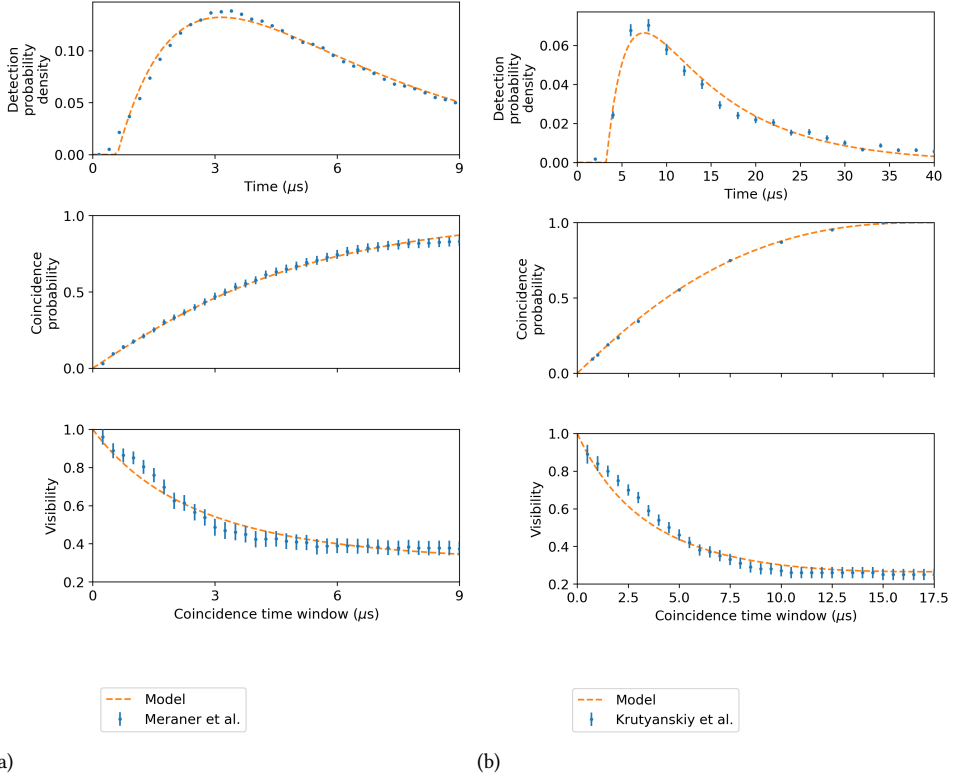


Figure 3.10: Comparison between data from two different experiments and the toy model introduced in Section 3.9. In both experiments, the detection probability density and coincidence probability were not conditioned on the successful detection of two photons. To account for this, we have multiplied both the detection-probability-density data and the coincidence-probability-density data by a different overall scaling factor. Both the scaling factors, the parameters of the two exponentials describing the photon state and an offset for the detection probability density have been determined using a least-squares procedure. The least-squares procedure has been performed jointly for the three data sets corresponding to the same experiment by summing the square errors of all three. Here, the largest weight has been given to the detection probability density (10^6), the second largest to the visibility (10^5), and the smallest to the coincidence probability (1). (a) Comparison to data from Meraner et al. [87]. In the experiment, the Rabi pulse was terminated after approximately $9 \mu\text{s}$, therefore we have only compared the first nine μs . Because of the terminated pulse the detection probability density falls to zero at approximately $12 \mu\text{s}$. Therefore, effectively the entire wave packet is detected. To reproduce this in our model, we have not implemented a detection time window (or equivalently, have set the detection time window to infinite). The fitted half-life times of the exponentials representing the wave function and emission time are $2.40 \mu\text{s}$ and $2.76 \mu\text{s}$ respectively. (b) Comparison to data from Krutyanskiy et al. [54] We base the modeling for the visibility and coincidence probability of ion traps in this paper on the fit shown here. A detection time window of $17.5 \mu\text{s}$ was used in the experiment. The detection-probability-density data used here corresponds to “node A” from [54]. The fitted half-life times of the exponentials representing the wave function and emission time are $3.01 \mu\text{s}$ and $6.79 \mu\text{s}$ respectively.

node repeater in the Delft-Eindhoven path to the equivalent color center and trapped ion setups. To do so, we require a method of converting hardware parameters from the more in-depth models to the abstract model. We therefore start by introducing this mapping.

Color center to abstract model mapping

The emission fidelity, visibility, dark count probability and probability of photon detection excluding attenuation losses are mapped without change from the color center model to the abstract model. An entanglement swap in an NV platform consists of one-qubit gates on both carbon and electron, two-qubit gates and measurement and initialization of the electron (see Figure 17 in Supplementary Note 5 of [61] for an image of the circuit). Imperfections in gates and initialization are modelled by depolarizing channels in the NV model, while the measurement error is modelled by probabilistic bit flips. In mapping to the abstract model we approximate the measurement error as a depolarizing channel. All the errors associated to the operations in the circuit are then multiplied together to obtain a single parameter s_q . $1 - s_q$ is used to parameterize a depolarizing channel applied after a perfect Bell-state measurement. The action of this depolarizing channel on a given state ρ as a function of s_q is given by equation (3.21), from which we can see that s_q is a measure of the quality of an entanglement swap.

$$\phi(\rho, s_q) = \left(\frac{1 + 3s_q}{4} \right) \rho + \frac{1 - s_q}{4} (X\rho X + Y\rho Y + Z\rho Z). \quad (3.21)$$

In our color center model, the coherence times of the carbon spins are different from those of the electron spin. This subtlety is lost in the abstract model, where we take the coherence time of all qubits to be the same as the carbon spins'. Other dephasing processes such as induced dephasing [34], which are present in our color center model, are ignored in the abstract model. In Table 3.4, we present the abstract model parameters obtained from the color center baseline hardware parameters as shown in Table 3.2.

Parameter	Noise	Duration/Time
Visibility	0.9	-
Dark count probability	1.5×10^{-7}	-
Photon detection probability excluding attenuation losses	5.1×10^{-4}	-
Spin-photon emission	F = 1	3.8 μ s
Swap quality	0.83	503.7 μ s
T1	-	10 hours
T2	-	1 s

Table 3.4: Baseline abstract model hardware parameters mapped from color center baseline shown in Table 3.2.

Having introduced the process by which we map color center parameters to the abstract model, we now proceed with the results of validating the abstract model against the NV model. To do so, the following steps were taken: (i) define the values of the baseline hardware parameters for the more in-depth model and map them to the abstract model following the procedure described above, thus obtaining the corresponding abstract model baseline, (ii) run the simulation, (iii) improve both baselines using the improvement factor technique introduced in Section 6.3 and (iv) repeat steps (ii) and (iii) for improvement factors in the desired range.

This analysis is done both for single and double-click entanglement generation, as we simulated color center repeaters running both protocols.

Color center validation

In Figure 3.11 we show the results of the validation for the abstract model against the NV model, for single-click (top) and double-click (bottom) entanglement generation.

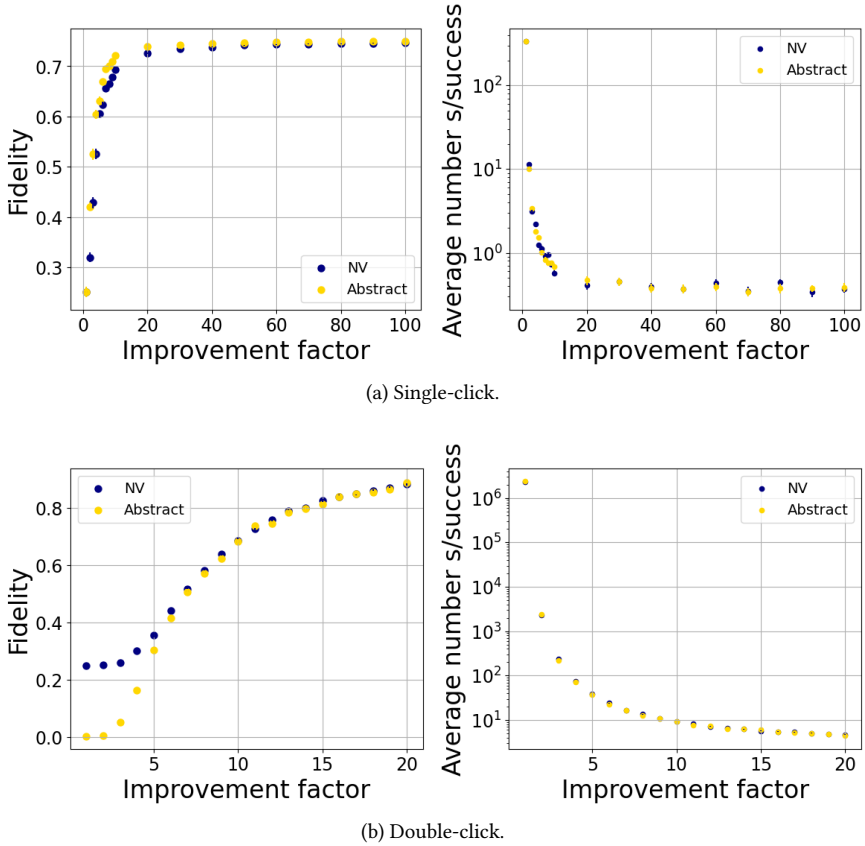


Figure 3.11: Performance of color center nodes and abstract nodes on the Delft - Eindhoven setup, with single-click (top) and double-click (bottom) entanglement generation. The leftmost point on both plots corresponds to the baseline hardware values. The points to the right were obtained by uniformly improving the hardware over this baseline. The error bars represent the standard error of the mean and are often smaller than the markers. “Average number s/success” is the average number of seconds per entangled pair that is successfully distributed.

The agreement is similar for both protocols. The rate of entanglement generation, shown on the plots on the right side, is identical for both models. The only source of difference timing-wise is in how long it takes to perform an entanglement swap, with color center taking slightly longer due to its more complex circuit. However, the low success probability of generating entanglement means that many attempts are required, rendering the time devoted to local operations negligible. Since the time taken per entanglement generation attempt is equal in both models, it is to be expected that the rate is identical.

For small improvement factors, there is a sizeable gap in the average teleportation fidelity achievable in each model, as shown on the plots on the left side. This fidelity is significantly larger for the abstract model. We conjecture that this is due to sources of

noise that are present in the NV model but not in the abstract model. These include induced dephasing noise, probability of double photon excitation and deviations in interferometric phase, the last two being single-click specific. As parameters improve, the magnitude of these noise sources drops, and so does the gap between the fidelity achieved by the two setups.

Overall, the abstract model captures the behavior of the more in-depth NV model reasonably well. However, it does result in a more optimistic picture regarding the parameter quality required to achieve certain fidelity targets. For example, in the abstract model with double-click entanglement generation, an improvement factor of 5 suffices to reach an average teleportation fidelity of 0.7. This same target requires an improvement factor of 7 in the NV model. This supports the need for detailed hardware models, which take platform-specific limitations and sources of noise into account.

Trapped ion to abstract model mapping

The visibility, dark count probability, photon detection probability excluding attenuation losses and spin-photon emission parameters are mapped without change from the trapped ion model to the abstract model. The process by which the swap quality parameter is obtained is identical to the one described in Section 3.6.7. There is a notable difference between how memory decoherence is accounted for in the two models. In our trapped ion model, states stored in memory suffer from collective dephasing and no relaxation is considered. Our abstract model, on the other hand, considers a T_1 , T_2 memory noise model, as empirically it has been found to fit well to a large variety of physical systems. When mapping from trapped ion parameters to abstract model parameters, we take the abstract model's T_2 to be given by the collective dephasing coherence time of the trapped ion and we set T_1 to infinity, i.e. we consider no relaxation in the abstract model. The collective dephasing affecting trapped ion qubits follows a Gaussian shape, whereas the dephasing in the abstract model follows a simple exponential. In Table 3.5, we present the abstract model parameters obtained from the trapped ion baseline hardware parameters as shown in Table 3.3.

Parameter	Noise	Duration/Time
Visibility	0.89	-
Dark count probability	1.5×10^{-5}	-
Photon detection probability excluding attenuation losses	0.0288	-
Spin-photon emission	$F = 0.99$	$50 \mu\text{s}$
Swap quality	0.94	1.91 ms
T_1	-	-
T_2	-	6 ms

Table 3.5: Baseline abstract model hardware parameters mapped from trapped ion baseline shown in Table 3.3.

Trapped ion validation

In this section, we investigate how well the simpler abstract model captures the behavior of the trapped ion model. We do this considering only double-click entanglement generation, as this was the only entanglement generation protocol we considered when performing

trapped ion simulations.

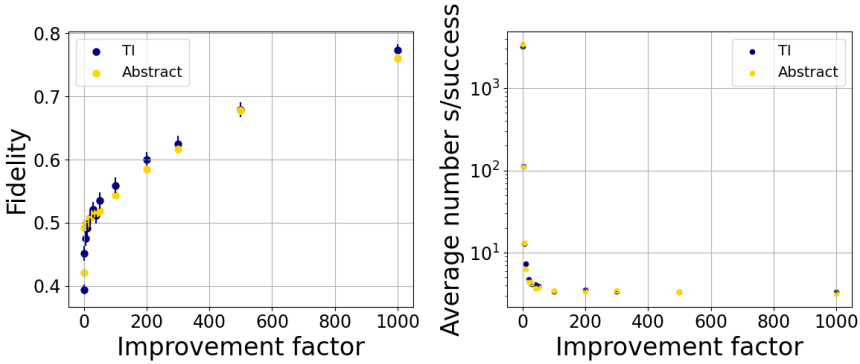


Figure 3.12: Performance of trapped ion nodes and abstract nodes on the Delft - Eindhoven setup, double-click entanglement generation. The leftmost point on both plots corresponds to the baseline hardware values. The points to the right were obtained by uniformly improving the hardware over this baseline. The error bars represent the standard error of the mean.

In Figure 3.12 we show the results of the validation of the abstract model against the trapped ion model. The agreement in terms of the entanglement generation rate is perfect, with the rates overlapping for all values of the improvement factor. This is to be expected, since the end-to-end entanglement generation time is dominated by the time spent attempting to generate elementary links, and each attempt takes the same amount of time in both models. The average teleportation fidelity follows the same trend for both models, starting at very low values for current hardware parameters and quickly rising as hardware parameters are improved. We note that for low improvement factors, the abstract model achieves a higher fidelity. The opposite seems to be true for high improvement factors, although there the difference is small and does not exceed one error bar. This can be explained by the Gaussian nature of the trapped ion dephasing. In the trapped ion model, the probability of a state stored in memory dephasing over a given period of time t is $1 - e^{-t^2/T^2}$, with T being the coherence time. In the abstract model, this probability is $1 - e^{-t/T}$. This means that for $t/T < 1$, the probability of error for trapped ions is smaller, while the opposite is true for $t/T > 1$. At low values of the improvement factor, the success probability of entanglement generation is small, as are coherence times. Therefore, the time a state is expected to stay in memory is likely larger than the coherence time, and we expect that the error rate is higher in the trapped ion model. As parameters improve, it becomes more likely that states remain in memory for periods of time smaller than the coherence time, which is the regime in which the error rate is higher in the abstract model. This is in line with what is observed in Figure 3.12. Overall, the agreement is better than what was observed in Section 3.6.7. There, owing to noise sources present in the color center model that were ignored in the abstract model, the latter performed better than the former. No noise sources were ignored when mapping from the trapped ion model to the abstract model, so this better agreement was to be expected. We conclude that the abstract model captures the behavior of the more detailed trapped ion model almost perfectly in the setup we considered.

3.6.8 Entanglement generation

For near-term parameters, the success probability of entanglement generation is very low. This means that many entanglement generation attempts are required, and that a simulation of this process would spend most of its time simulating failed attempts. This is computationally very inefficient, so we instead perform entangled state insertion, through a process we call *magic* [96]. This process was first introduced in [79].

Magic works as follows: once two nodes have decided to generate entanglement together, we sample from a geometric distribution in order to determine how many attempts would have been required to succeed. The success probability of this geometric distribution is limited by the product of the probabilities of emitting the photon in the correct mode, capturing it into the fiber, frequency-converting it, transmitting it through the fiber and detecting it at the detector. Furthermore, imperfections such as the imperfect indistinguishability of interfering photons and detector dark counts also impact the success probability. Their effect depends on whether a single-click or double-click protocol is used.

The elapsed time for the entanglement generation process is given by the product of the sampled number of required attempts and the duration of one attempt, which is in turn given by the sum of the emission time and the photon travel time.

The state generated is given by an analytical model which is different for single and double-click entanglement generation. For more details, see Section 3.8.

3.7 Target metric

In this section, we explain the target metric used in this chapter. As discussed in the main text, there are two conditions on end-to-end entanglement distribution that define the target. The first is on the average fidelity with which qubits can be teleported using the generated entangled states, and the second is on the rate at which such states are generated. The target values for the teleportation fidelity and entangling rate are chosen such that the quantum link would be able to support Verifiable Blind Quantum Computation (VBQC) [36] when the server consists of a powerful quantum computer with a coherence time of 100 seconds. We show that if the targets are met, the client would be able to execute VBQC by preparing states at the powerful quantum computer using either quantum teleportation or remote state preparation (for remote state preparation, see Section 3.7.5).

The following results presented in this section are novel:

- the constraint equation that, when solved, guarantees VBQC is feasible (Theorems 3.1 and 3.4);
- the extension of the noise robustness theorem in [36] to guarantee that VBQC is feasible when the *average* error probability can be bounded instead of the *maximum* error probability, assuming that the error probabilities across different rounds are independent and identically distributed (Theorem 3.2 and Section 3.7.4);
- a modified version of the VBQC protocol [36] that is based on remote state preparation instead of qubit transmission (Protocol 3.1) and a proof that, in the absence of local noise, it is equivalent to the original protocol where some effective quantum channel is used for qubit transmission (thereby guaranteeing that the correctness of

the original protocol is inherited; we note that we have not otherwise investigated the security of this protocol) (Theorem 3.3).

3.7.1 Teleportation fidelity

We consider the following quantum-teleportation protocol [36]. A one-qubit information state ρ is teleported using a two-qubit resource state σ shared by two parties. A Bell-state measurement is performed between the qubit holding the information state and one of the qubits in the resource state. If the outcome of the measurement corresponds to Bell state

$$|\Phi_{ij}\rangle \equiv X^i Z^j |\Phi^+\rangle \quad (3.22)$$

with $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ then the Pauli correction $X^i Z^j$ is performed on the one remaining qubit. Executing this protocol results in transmitting the information state through the teleportation channel Λ_σ .

Definition 3.1 *Teleportation channel.* The teleportation channel associated with the two-qubit state σ is given by the single-qubit quantum channel

$$\Lambda_\sigma(\rho) \equiv \sum_{i,j} (X^i Z^j \otimes \langle \Phi_{ij} |) (\sigma \otimes \rho) (X^i Z^j \otimes | \Phi_{ij} \rangle). \quad (3.23)$$

We note that if $\sigma = |\Phi_{00}\rangle\langle\Phi_{00}|$ then Λ_σ is the identity map. The average teleportation fidelity corresponding to the resource state σ is given by $F_{\text{tel}}(\sigma)$.

Definition 3.2 *Average teleportation fidelity.* The average teleportation fidelity associated with the two-qubit state σ is given by

$$F_{\text{tel}}(\sigma) \equiv \int_{\psi} \langle \psi | \Lambda_\sigma(|\psi\rangle\langle\psi|) | \psi \rangle d\psi, \quad (3.24)$$

where the integral is over the Haar measure.

We note that by the Haar measure, we here mean the uniform measure over single-qubit quantum states, i.e. the uniform measure on the unit sphere in \mathcal{C}^2 . It is the unique measure that is invariant under unitary transformations [97].

Finally, we note that if the sender and receiver agree on a unitary U , then teleportation can also be executed as follows. First, the sender applies U to the information state. Second, the sender teleports the resulting information state to the receiver. Last, the receiver applies the unitary U^\dagger to undo the original unitary and obtain the information state. The qubit is then transmitted through a rotated teleportation channel.

Definition 3.3 *Rotated teleportation channel.* The rotated teleportation channel associated with the two-qubit state σ and the unitary U is given by

$$\Lambda_{\sigma,U}(\rho) = U^\dagger \Lambda_\sigma(U\rho U^\dagger) U \quad (3.25)$$

We remark that the average teleportation fidelity is not affected by the introduction of the unitary U because of the invariance of the Haar measure, i.e.

$$F_{\text{tel}}(\sigma) = \int_{\psi} d\psi \langle \psi | \Lambda_{\sigma,U}(|\psi\rangle\langle\psi|) | \psi \rangle, \quad (3.26)$$

Using a unitary to turn a teleportation channel into a rotated teleportation channel can be advantageous when not every state on the Bloch sphere needs to be transmitted with equal fidelity, and σ is such that not all states can be transmitted with equal fidelity. By applying the unitary U , the Bloch sphere can potentially be rotated in such a way to make states for which high-fidelity transmission is desirable coincide with states that can be transmitted at high fidelity.

3.7.2 Requirements from VBQC

We consider the scenario where two nodes are connected using the one-repeater quantum connection studied in this work. These two nodes use the entanglement generated by this quantum connection to perform VBQC. Specifically, the first node (the client) utilizes VBQC to execute a two-qubit computation on the quantum processor of the second node (the server) in a verified and blind fashion. It is assumed that the server is able to execute gates without noise and has a coherence time of 100 seconds. Our target metric is chosen such that it guarantees that the quantum connection is able to support this protocol.

A single round of the VBQC protocol involves the preparation of two qubits by the client at the server, and the execution of a series of quantum gates and measurements on those qubits by the server. The client can use the remote-state-preparation protocol [98] to use one entangled state to prepare one qubit at the server. Some rounds are computation rounds, the results of which are sent classically by the server to the client. All other rounds are test rounds. In a test round, some of the qubits transmitted to the server are traps; if the server tries to measure these qubits or performs another operation than the one specified by the client, this will become apparent from the returned computation results. However, tampering by the server is indistinguishable from noise. Only if noise is within certain bounds can the protocol be performed successfully.

This defines minimum requirements on the quantum connection used by the client to prepare the qubits at the server. First, the fidelity at which states can be prepared needs to be large enough. Second, the rate at which they can be prepared needs to be large enough as well. The reason for this is that after the first qubit is prepared at the server, it will undergo memory decoherence while waiting for the second qubit to be prepared.

Specifically, we consider the case of depolarizing memory.

Definition 3.4 *Depolarizing memory.* If a single-qubit quantum state ρ is stored in a depolarizing memory with coherence time T for a time t , it is subjected to a depolarizing channel

$$\mathcal{D}_p(\rho) = p\rho + (1-p)\frac{\mathbf{1}}{2} \quad (3.27)$$

where the depolarizing parameter p is given by

$$p = e^{-\frac{t}{T}}. \quad (3.28)$$

The minimum requirements are then defined by the following theorem.

Theorem 3.1 *Requirements on entanglement generation for VBQC.* Assume a quantum link generates the two-qubit state σ between a client and a server with average rate R , and that the distribution times are independent and identically distributed. Furthermore, assume that

qubits at the server are stored in a depolarizing memory with coherence time T . Lastly, assume that all local operations are noiseless and instantaneous. If the client prepares qubits at the server using the rotated teleportation channel $\Lambda_{\sigma,U}$ for some unitary U , then a unitary U exists such that the VBQC protocol proposed in [36], for a two-qubit deterministic quantum computation, can be executed in a way that is composable secure with exponentially small ϵ if

$$F_{\text{tel}}(\sigma) > \frac{1}{2} \left(1 + \frac{1}{\sqrt{2}} e^{\frac{1}{2RT}} \right). \quad (3.29)$$

3

Practically speaking, Theorem 3.1 means that VBQC with two qubits and no failure probability that is inherent to the computation is feasible in case equation (3.83) holds. A requirement is that the state σ is the same for each delivery of entanglement, and that the distribution times are independent and identically distributed. We note that this is the case for the one-repeater setup studied in this chapter. After entanglement swapping at the repeater node takes place, the end-to-end entangled state is removed from the end nodes and the state of the network path is fully reset, making each entanglement delivery completely independent from the last, with identical distributions for both delivery times and errors. In general, the state that is delivered will depend on the amount of time entangled qubits are stored before entanglement swapping takes place at the repeater node, resulting in a state that is not the same each round. However, if the processing of the entangled state is not conditioned on the amount of storage time, the final state will effectively look like a constant mixture over all values that the storage time can take.

In this chapter, we consider two different sets of target teleportation fidelity and target rate, namely $(F_{\text{tel}}, R) = (0.8717, 0.1 \text{ Hz})$ and $(0.8571, 0.5 \text{ Hz})$. Both of these have been chosen to satisfy Eq. (3.83) for $T = 100$ seconds.

3.7.3 Proving Theorem 3.1

In [36], it is shown that the VBQC protocol is composable secure with exponentially small ϵ in case the noise is such that the failure probability of each individual test round can be upper bounded. Key to proving Theorem 3.1 is a relaxation of this condition: two-qubit VBQC is also feasible if instead the *average* failure probability of test rounds can be upper bounded, in case the failure probabilities are independent and identically distributed. This is stated in the following theorem.

Theorem 3.2 (*Local correctness of VBQC protocol on Noisy Devices*) *Let p denote the inherent error probability of the quantum computation, which is executed using a k -colorable graph state. Assume that, for every test round, the probability that at least one of the trap-measurement outcomes is incorrect is a random variable. Furthermore, assume that these are independent and identically distributed for all test rounds. Let q be the expected value of these random variables. The VBQC protocol presented in [36] is ϵ_{cor} -locally-correct with exponentially low ϵ_{cor} if $q < (1/k)(2p - 1)/(2p - 2)$.*

Theorem 3.2 is proven in Section 3.7.4 and allows us to derive the following lemma.

Lemma 3.1 *Two-qubit VBQC for deterministic computations is composable secure with exponential ϵ if the probabilities that the trap-measurement outcome is incorrect are independent and identically distributed for all test rounds and the average probability that the trap-measurement outcome in a single test round is incorrect, q , satisfies $q < 1/4$.*

Proof: First, we note that all two-qubit graph states are at least two-colorable, i.e., $k \leq 2$. Second, we note that for deterministic computations the inherent error probability of the computation is zero, i.e. $p = 0$. Then, from Theorem 3.2, it follows that if $q < 1/4$ is true, then the VBQC protocol is ϵ_{cor} -locally-correct with exponentially low ϵ_{cor} . Additionally, as shown in [36], the VBQC protocol is ϵ_{bl} -local-blind and ϵ_{ver} -local-verifiable with ϵ_{ind} -independent-verification, with ϵ_{bl} , ϵ_{ver} and ϵ_{ind} exponentially low. Therefore, as in [36], it follows that the protocol is composable secure with exponential ϵ . \square

During a test round, the client randomly designates one of the two qubits that it prepares at the server the “dummy” qubit and the other the “trap” qubit. The client that remotely prepares the dummy qubit in $|d\rangle$, where d is chosen uniformly at random by the client from $\{0, 1\}$. It prepares the trap qubit in the state $|+\rangle_\theta$ defined by

$$|\pm_\theta\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm e^{i\theta}|1\rangle), \quad (3.30)$$

where the client chooses θ uniformly at random from $\Theta \equiv \{i\pi/4\}_{0 \leq i \leq 7}$. That is, the trap qubit will be in one of eight equidistant quantum states on the equator of the Bloch sphere. The server will perform a CZ gate between the two qubits, measure them in the basis $\{|+\delta\rangle, |-\delta\rangle\}$, and send the measurement outcomes to the client. Here, $\delta = \theta + r\pi$, where r is chosen uniformly at random by the client from $\{0, 1\}$. The test round is declared a success if the measurement on the trap qubit yields $d \oplus r$ and a failure otherwise. If the server is honest and there is no noise, test rounds are always successful. Otherwise, we show that the following Lemma holds:

Lemma 3.2 *If, during a test round of two-qubit VBQC, the trap qubit is prepared with fidelity F_{trap} and the dummy qubit is prepared with fidelity F_{dummy} , then the probability that the measurement outcome on the trap qubit is incorrect is given by*

$$p_{\text{fail}} = F_{\text{dummy}}(1 - F_{\text{trap}}) + F_{\text{trap}}(1 - F_{\text{dummy}}). \quad (3.31)$$

Proof: Consider the case $d = r = 0$. In that case, we can write

$$\rho_{\text{dummy, server}} = F_{\text{dummy}}|0\rangle\langle 0| + (1 - F_{\text{dummy}})|1\rangle\langle 1| + a|0\rangle\langle 1| + a^*|1\rangle\langle 0| \quad (3.32)$$

for some constant a and

$$\rho_{\text{trap, server}} = F_{\text{trap}}|+\rangle_\theta\langle +| + (1 - F_{\text{trap}})|-\rangle_\theta\langle -| + b|+\rangle_\theta\langle -| + b^*|-\rangle_\theta\langle +| \quad (3.33)$$

for some constant b . Here, we have made use of the fact that both $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle_\theta, |-\rangle_\theta\}$ are complete bases for the single-qubit Hilbert space.

After receiving both states, the server will perform a CZ gate between the two qubits, and then measure the trap qubit in the $\{|+\rangle_\theta, |-\rangle_\theta\}$ basis. Whether the test round is successful or not depends on whether the expected outcome $d \oplus r = 0$, i.e. $|+\rangle_\theta$, is obtained from this measurement. In order to get the measurement statistics on the trap qubit, we can first trace out the dummy qubit. With that in mind, let's look at what happens with the term

$$\begin{aligned} & a\text{CZ}|0\rangle\langle 1|\rho_{\text{trap, server}}\text{CZ} + a^*\text{CZ}|1\rangle\langle 0|\rho_{\text{trap, server}}\text{CZ} \\ & = a|0\rangle\langle 1|\rho_{\text{trap, server}}Z + a^*|1\rangle\langle 0|Z\rho_{\text{trap, server}}. \end{aligned} \quad (3.34)$$

After the CZ has been performed, the off-diagonal terms of $\rho_{\text{dummy, server}}$ are still off diagonal. These will vanish when tracing out the dummy qubit and can therefore be safely ignored. Therefore, we make the substitution

$$\rho_{\text{dummy, server}} \rightarrow F_{\text{dummy}} |0\rangle\langle 0| + (1 - F_{\text{dummy}}) |1\rangle\langle 1|. \quad (3.35)$$

Then, the effect of the CZ is easy to evaluate, giving

$$\rho_{\text{after CZ}} = F_{\text{dummy}} |0\rangle\langle 0| \rho_{\text{trap, server}} + (1 - F_{\text{dummy}}) |1\rangle\langle 1| Z \rho_{\text{trap, server}} Z \quad (3.36)$$

which, after tracing out the dummy qubit, gives

$$\begin{aligned} \rho_{\text{trap, after CZ}} = & \left(F_{\text{dummy}} F_{\text{trap}} + (1 - F_{\text{dummy}})(1 - F_{\text{trap}}) \right) |+\theta\rangle\langle +\theta| \\ & + \left(F_{\text{dummy}}(1 - F_{\text{trap}}) + F_{\text{trap}}(1 - F_{\text{dummy}}) \right) |-\theta\rangle\langle -\theta| \\ & + c |+\theta\rangle\langle -\theta| + c^* |-\theta\rangle\langle +\theta|, \end{aligned} \quad (3.37)$$

where c is a function of b , F_{dummy} and F_{trap} . Applying a POVM with elements $|+\theta\rangle\langle +\theta|$ and $|-\theta\rangle\langle -\theta|$ then gives a failure probability of the test round of

$$p_{\text{fail}} = \text{Tr} \left(|-\theta\rangle\langle -\theta| \rho_{\text{trap, after CZ}} \right) = F_{\text{dummy}}(1 - F_{\text{trap}}) + F_{\text{trap}}(1 - F_{\text{dummy}}). \quad (3.38)$$

This calculation can be repeated for all three cases where $d = r = 0$ is false, each time giving the exact same outcome. \square

We now have a formula for the probability that a test round fails, given by equation (3.38). However, this formula depends on the fidelity with which specific states are transmitted over the teleportation channel. These states are randomly chosen during each test round ($|0\rangle$ or $|1\rangle$ for the dummy qubit, $|+\theta\rangle$ for the trap qubit). This means that, in general, the failure probability is not constant per round. Before we are able to use Lemma 3.1, we need to know something about the average failure probability per round. Additionally, we need to account for decoherence in the server's memory while waiting for the second qubit to be prepared at the server. Both are accounted for in the following lemma.

Lemma 3.3 *Assume a quantum link generates the two-qubit state σ between a client and a server with average rate R , and that the distribution times are independent and identically distributed. Additionally assume that a unitary U has been chosen such that dummy qubits can be transmitted through a rotated teleportation channel with average fidelity*

$$\bar{F}_{\text{dummy}} \equiv \frac{1}{2} \left(\langle 0 | \Lambda_{\sigma, U} (|0\rangle\langle 0|) | 0 \rangle + \langle 1 | \Lambda_{\sigma, U} (|1\rangle\langle 1|) | 1 \rangle \right) \quad (3.39)$$

and trap qubits with average fidelity

$$\bar{F}_{\text{trap}} \equiv \frac{1}{8} \sum_{\theta \in \Theta} \langle +\theta | \Lambda_{\sigma, U} (|+\theta\rangle\langle +\theta|) | +\theta \rangle. \quad (3.40)$$

Assume that the condition

$$\bar{F}_{\text{dummy}}(1 - \bar{F}_{\text{trap}}) + \bar{F}_{\text{trap}}(1 - \bar{F}_{\text{dummy}}) \leq \frac{1}{2} \quad (3.41)$$

holds. Furthermore, assume that qubits received by the server are stored in depolarizing quantum memory with coherence time T . Lastly, assume that all local operations are noiseless and instantaneous. In that case, for two-qubit VBQC, the average test-round failure probability is bounded by

$$q \leq e^{-\frac{1}{RT}} \left[\bar{F}_{dummy}(1 - \bar{F}_{trap}) + \bar{F}_{trap}(1 - \bar{F}_{dummy}) \right] + \frac{1}{2} \left(1 - e^{-\frac{1}{RT}} \right). \quad (3.42)$$

Proof: Let Δt be the time between the generation of the first and second entangled state. Then, the first qubit is stored for time Δt in depolarizing memory until the second qubit is prepared at the server. If the qubit was prepared at the server with fidelity F , the depolarizing noise will have the effect

$$F \rightarrow e^{-\frac{\Delta t}{T}} F + \frac{1}{2} \left(1 - e^{-\frac{\Delta t}{T}} \right). \quad (3.43)$$

We note that equation (3.31) is symmetric under interchange of F_{dummy} and F_{trap} . Therefore, we can assume that the dummy qubit is prepared first without loss of generality. Writing F_{dummy} and F_{trap} for the fidelities with which the qubits are teleported to the server (i.e. excluding the effect of memory decoherence), it follows that

$$p_{fail} = e^{-\frac{\Delta t}{T}} \left[F_{dummy}(1 - F_{trap}) + F_{trap}(1 - F_{dummy}) \right] + \frac{1}{2} \left(1 - e^{-\frac{\Delta t}{T}} \right). \quad (3.44)$$

Now, to calculate the average failure probability $q \equiv \langle p_{fail} \rangle$, we note that F_{dummy} , F_{trap} and Δt are all independent random variables; the first depends on the choice of d (i.e. whether to prepare $|0\rangle$ or $|1\rangle$), the second depends on the choice of θ (i.e. which $|\psi\rangle$ to prepare), and the last depends on the probability distribution for the entanglement delivery time. This allows us to write

$$q = \left\langle e^{-\frac{\Delta t}{T}} \right\rangle \left[\bar{F}_{dummy}(1 - \bar{F}_{trap}) + \bar{F}_{trap}(1 - \bar{F}_{dummy}) \right] + \frac{1}{2} \left(1 - \left\langle e^{-\frac{\Delta t}{T}} \right\rangle \right). \quad (3.45)$$

Because the exponential function is convex, Jensen's inequality [99] gives

$$\left\langle e^{-\frac{\Delta t}{T}} \right\rangle \geq e^{-\frac{\langle \Delta t \rangle}{T}}. \quad (3.46)$$

The times between the distribution of two entangled states are by assumption all independent and identically distributed, i.e., they are all copies of the same Δt . The (average) entangling rate is therefore simply equal to

$$R = \frac{1}{\langle \Delta t \rangle}, \quad (3.47)$$

and therefore we find

$$\left\langle e^{-\frac{\Delta t}{T}} \right\rangle \geq e^{-\frac{1}{RT}}. \quad (3.48)$$

In case equation (3.41) holds equation (3.48) can be combined with equation (3.45) to obtain equation (3.42). \square We note that the use of Jensen's inequality above accounts for any kind

of potential jitter in the delivery of entangled qubits to the server. Whatever the distribution on the waiting time Δt looks like and at however irregular intervals entanglement is delivered, Jensen's inequality will guarantee that Eq. (3.42) holds.

Now, we want to use the average teleportation fidelity F_{tel} instead of the quantities \bar{F}_{dummy} and \bar{F}_{trap} to bound q . The final building block towards obtaining such a bound and proving Theorem 3.1 is the following lemma.

Lemma 3.4 *There exists a unitary U such that*

$$\bar{F}_{\text{dummy}} = \bar{F}_{\text{trap}} = F_{\text{tel}}, \quad (3.49)$$

where \bar{F}_{dummy} is defined in equation (3.39), \bar{F}_{trap} in equation (3.40) and F_{tel} in equation (3.24) (with σ left implicit).

Proof: While \bar{F}_{dummy} and \bar{F}_{trap} are fidelity averages over specific subsets of the Bloch sphere, F_{tel} is an average over the entire Bloch sphere. This allows us to find the relationship

$$F_{\text{tel}} = \frac{1}{3}\bar{F}_{\text{dummy}} + \frac{2}{3}\bar{F}_{\text{trap}}. \quad (3.50)$$

To see how this relationship follows, we first note that the average fidelity over the entire Bloch sphere can be written as an average over any six states that form a regular octahedron on the Bloch sphere [100]. One example of such an octahedron is given by the six eigenstates of the Pauli operators, which gives

$$\begin{aligned} F_{\text{tel}} &= \frac{1}{6} \left(\langle 0 | \Lambda_{\sigma,U} (|0\rangle\langle 0|) | 0 \rangle + \langle 1 | \Lambda_{\sigma,U} (|1\rangle\langle 1|) | 1 \rangle \right. \\ &\quad + \langle +_0 | \Lambda_{\sigma,U} (|+_0\rangle\langle +_0|) | +_0 \rangle + \langle -_0 | \Lambda_{\sigma,U} (|-_0\rangle\langle -_0|) | -_0 \rangle \\ &\quad + \left\langle +\frac{\pi}{2} \middle| \Lambda_{\sigma,U} \left(\left| +\frac{\pi}{2} \right\rangle\langle +\frac{\pi}{2} \right) \middle| +\frac{\pi}{2} \right\rangle + \left\langle -\frac{\pi}{2} \middle| \Lambda_{\sigma,U} \left(\left| -\frac{\pi}{2} \right\rangle\langle -\frac{\pi}{2} \right) \middle| -\frac{\pi}{2} \right\rangle \right) \\ &= \frac{1}{6} \left(\langle 0 | \Lambda_{\sigma,U} (|0\rangle\langle 0|) | 0 \rangle + \langle 1 | \Lambda_{\sigma,U} (|1\rangle\langle 1|) | 1 \rangle + \sum_{i=0}^4 \left\langle +\frac{i\pi}{2} \middle| \Lambda_{\sigma,U} \left(\left| +\frac{i\pi}{2} \right\rangle\langle +\frac{i\pi}{2} \right) \middle| +\frac{i\pi}{2} \right\rangle \right). \end{aligned} \quad (3.51)$$

Another such octahedron is obtained by rotating these six eigenstates around the Z axis by an angle of $\pi/4$. This gives the relation

$$\begin{aligned} F_{\text{tel}} &= \frac{1}{6} \left(\langle 0 | \Lambda_{\sigma,U} (|0\rangle\langle 0|) | 0 \rangle + \langle 1 | \Lambda_{\sigma,U} (|1\rangle\langle 1|) | 1 \rangle \right. \\ &\quad + \sum_{i=0}^4 \left\langle +\frac{(2i+1)\pi}{4} \middle| \Lambda_{\sigma,U} \left(\left| +\frac{(2i+1)\pi}{4} \right\rangle\langle +\frac{(2i+1)\pi}{4} \right) \middle| +\frac{(2i+1)\pi}{4} \right\rangle \right). \end{aligned} \quad (3.52)$$

Adding equations (3.51) and (3.52) together and dividing by two then gives

$$F_{\text{tel}} = \frac{1}{6} \left(\langle 0 | \Lambda_{\sigma,U} (|0\rangle\langle 0|) | 0 \rangle + \langle 1 | \Lambda_{\sigma,U} (|1\rangle\langle 1|) | 1 \rangle \right) + \frac{1}{12} \left(\sum_{\theta \in \Theta} \langle +\theta | \Lambda_{\sigma,U} (|+\theta\rangle\langle +\theta|) | +\theta \rangle \right), \quad (3.53)$$

which is equivalent to Eq. (3.50).

While the unitary U will leave the average over the entire Bloch sphere, F_{tel} , invariant, the same does not hold for \bar{F}_{dummy} . The unitary rotates the Bloch sphere and thus effectively turns \bar{F}_{dummy} into an average over any pair of antipodal points on the Bloch sphere. Each pair of antipodal points can be described using only one of the two points. The average over pairs of antipodal points can therefore be described as a function f with as domain one half of the Bloch sphere. This function f maps each point on that half of the Bloch sphere to the average fidelity of that point and its antipodal point. Now, \bar{F}_{dummy} can be chosen to correspond to any of the values in f 's range. Additionally, the average of f over its domain is equal to the average fidelity over all points on the entire Bloch sphere, i.e. F_{tel} . By the mean value theorem, we can conclude that there is a value in the range of the function that equals the average of the function. That is, there exists a choice for the unitary U such that $\bar{F}_{\text{dummy}} = F_{\text{tel}}$. Then, equation (3.50) implies that if $\bar{F}_{\text{dummy}} = F_{\text{tel}}$, then $\bar{F}_{\text{trap}} = F_{\text{tel}}$. \square

Theorem 3.1 is then finally proven by combining Lemmas 3.1, 3.3, and 3.4.

3.7.4 Proving Theorem 3.2

In Section F of [36], the authors show that their VBQC protocol is robust to noise, assuming that the probability of error in each round can be upper-bounded by some maximum probability of error p_{max} . More specifically, they show that the protocol can be configured in such a way that it is ϵ_{cor} -locally-correct with exponentially small ϵ_{cor} .

Here we argue that if we assume that the error probabilities are independent and identically distributed across different rounds of the protocol, then the error probability in each round is effectively equal to the average probability of error. It then suffices that this average be bounded to obtain local correctness per the result of [36], as the error probability becomes constant and the maximum error probability is equal to the average error probability. We hereby prove Theorem 3.2.

We assume that for each round, there is a “true” probability of error. This true probability of error is a random variable, with a second-order probability distribution determining what values it takes and with what probabilities [101]. Let p_{error_i} be the probability of there being an error in round i , i.e., the value taken by the true probability of error in round i , drawn from the second-order probability distribution. By the law of total probability, this can be written as:

$$p_{\text{error}_i} = \int P(\text{error}|p = p_e) P(p = p_e) dp_e, \quad (3.54)$$

where $P(\text{error}|p = p_e)$ is the probability that there is an error given that the true probability of error takes the value p_e and $P(p = p_e)$ is the probability density that this happens. By definition, $P(\text{error}|p = p_e) = p_e$, therefore we can rewrite the equation as:

$$p_{\text{error}_i} = \int p_e P(p = p_e) dp_e = \overline{p_e}, \quad (3.55)$$

with $\overline{p_e}$ being the expected value of the second-order probability distribution from which each round's probability of error is sampled. The second-order probability distribution can then be ignored, and the probability that an error occurs in a given round is simply

given by a first-order probability. It follows that the probability of error in every round is $\overline{p_e}$, i.e., the average probability of error, so it suffices that the average probability of error be bounded.

3.7.5 Remote state preparation

Here, we introduce a modified version of the VBQC protocol [36] in which the client “sends” qubits to the server using remote state preparation (Protocol 3.1). Remote state preparation is experimentally simpler than teleportation. Therefore, it is likely that early VBQC demonstrations will be more feasible when using remote state preparation than when using teleportation. We show that, when local operations are noiseless, the modified protocol is equivalent to the protocol introduced in [36] but using some specific effective quantum channel to send qubits from the client to the server. This result is expressed in Theorem 3.3. Therefore, the correctness property carries over from the protocol in [36] to the modified protocol, showing that it is indeed possible to use remote state preparation to execute VBQC. Additionally, we show that the conclusions about the feasibility of VBQC found above (Theorem 3.1) also hold for the modified protocol. That is, when the rate and fidelity of entanglement generation are good enough to support VBQC through quantum teleportation with noiseless local operations, they are also good enough to support VBQC through remote state preparation with noiseless local operations. This result is expressed in Theorem 3.4.

As preliminaries to proving the above, we first introduce two definitions.

Definition 3.5 *U-NOT operation. The U-NOT operation Y is defined as [102]*

$$Y(\alpha|0\rangle + \beta|1\rangle) = \beta^*|0\rangle - \alpha^*|1\rangle. \quad (3.56)$$

That is, Y maps any qubit state to a state that is orthogonal to it.

We note that the U-NOT operation Y is anti-unitary and hence cannot be physically implemented [102]. It maps all states on the Bloch sphere to their antipodal points, which cannot be realized with rotations only. However, mapping a specific point on the Bloch sphere to its antipodal point can always be achieved by rotating the Bloch sphere by π around any axis that is orthogonal to the axis intersecting the point. Such a mapping is provided by the following definition.

Definition 3.6 *$|\psi\rangle$ -NOT operations. The family of $|\psi\rangle$ -NOT operations $\mathcal{A}_{\phi,|\psi\rangle}$ is defined by*

$$\mathcal{A}_{\phi,|\psi\rangle} \equiv e^{-i\phi} Y(|\psi\rangle) \langle\psi| + e^{i\phi} |\psi\rangle \langle Y(|\psi\rangle)| \quad (3.57)$$

The parameter ϕ in $\mathcal{A}_{\phi,|\psi\rangle}$ represents the freedom in choosing which axis to use for the π rotation that maps $|\psi\rangle$ to $Y(|\psi\rangle)$ and vice versa. We note that $\mathcal{A}_{\phi,|\psi\rangle}^\dagger = \mathcal{A}_{\phi,|\psi\rangle}$. Now, we define a modified version of the VBQC protocol that makes use of remote state preparation instead of quantum teleportation.

Protocol 3.1 *VBQC with remote state preparation. This protocol is the same as the VBQC protocol presented in [36], except for the following.*

- Before starting the protocol, the client and server agree on a one-qubit unitary operation U .

- Whenever the client would send a qubit v in the state $|\psi\rangle$ to the server, it instead measures its half of a two-qubit resource state shared with the server in the basis $\{U|\psi\rangle, Y(U|\psi)\}$. The outcome of this measurement is stored at the client as c_v , with $c_v = 0$ corresponding to outcome $U|\psi\rangle$ and $c_v = 1$ corresponding to outcome $Y(U|\psi)$. The server applies the operation U^\dagger to its local entangled qubit. This qubit held by the server is now considered the qubit as received from the client.
- In a computation round, the measurement outcome δ_v obtained from qubit v is bit flipped by the client in case $c_v = 1$. That is,

$$\delta_v \rightarrow \delta_v \oplus c_v \quad (\text{computation round}). \quad (3.58)$$

- In a test round, for each trap qubit v , the measurement outcome δ_v is bit flipped by the client in case $c_v = 1$, and once more for every neighboring dummy qubit w for which $c_w = 1$. That is,

$$\delta_v \rightarrow \delta_v \oplus c_v \oplus \bigoplus_{w \in N_G(v)} c_w \quad (\text{test round}). \quad (3.59)$$

Here, G is the computation graph used in the VBQC protocol and $N_G(v)$ is the neighbourhood of qubit v in graph G .

The outcomes c_v are never shared with the server.

Lemma 3.5 *Effective remote-state-preparation channel. Let $|\psi\rangle$ be some pure single-qubit state and let σ be some two-qubit density matrix shared by Alice and Bob. Let $\phi_{|\psi\rangle}$ be some function mapping the single-qubit state $|\psi\rangle$ to a real number. Furthermore, let U be some single-qubit unitary operation. If the first of two qubits holding the state σ is measured in the basis $\{U|\psi\rangle, Y(U|\psi)\}$ with measurement outcome c ($c = 0$ corresponding to $U|\psi\rangle$, $c = 1$ corresponding to $Y(U|\psi)$) after which the operation $U^\dagger \mathcal{A}_{\phi_{|\psi\rangle}, U|\psi}^c$ is applied to the second qubit and the first qubit is traced out, then this is equivalent to sending a qubit in the state $|\psi\rangle$ through the rotated effective remote-state-preparation $\Lambda_{\phi_{|\psi\rangle}, \sigma, U}$ channel given by*

$$\Lambda_{\phi_{|\psi\rangle}, \sigma, U}(|\psi\rangle) = U^\dagger \Lambda_{\phi_{|\psi\rangle}, \sigma}(U|\psi)U, \quad (3.60)$$

where $\Lambda_{\phi_{|\psi\rangle}, \sigma}$ is the effective remote-state-preparation channel given by

$$\begin{aligned} \Lambda_{\phi_{|\psi\rangle}, \sigma}(|\psi\rangle) = & \left(\langle \psi | \otimes \mathbf{1} \right) \sigma \left(|\psi\rangle \otimes \mathbf{1} \right) \\ & + \left(\langle \psi | \otimes \mathbf{1} \right) \left(\mathcal{A}_{\phi_{|\psi\rangle}, |\psi\rangle} \otimes \mathcal{A}_{\phi_{|\psi\rangle}, |\psi\rangle} \right) \sigma \left(\mathcal{A}_{\phi_{|\psi\rangle}, |\psi\rangle} \otimes \mathcal{A}_{\phi_{|\psi\rangle}, |\psi\rangle} \right) \left(|\psi\rangle \otimes \mathbf{1} \right). \end{aligned} \quad (3.61)$$

Proof: In case the state $U|\psi\rangle$ is measured on the first qubit, i.e., $c = 0$, the unnormalized post-measurement state after tracing out the first qubit and applying $U^\dagger \mathcal{A}_{\phi_{|\psi\rangle}, U|\psi}^0 = U^\dagger$ is

$$\rho'_{c=0} = U^\dagger \left(\langle \psi | U^\dagger \otimes \mathbf{1} \right) \sigma \left(U|\psi\rangle \otimes \mathbf{1} \right) U. \quad (3.62)$$

This measurement outcome is obtained with probability $p_{c=0} = \text{Tr}\{\rho_{c=0}\}$, and the corresponding normalized state is $\rho_{c=0} = \rho'_{c=0}/p_{c=0}$. In case the state $Y(U|\psi)$ (which is equal

op to global phase to $\mathcal{A}_{\phi_{|\psi\rangle}, U|\psi\rangle} U|\psi\rangle$ is measured, i.e., $c = 1$, the unnormalized state after tracing out the first qubit and applying $U^\dagger \mathcal{A}_{\phi_{|\psi\rangle}, U|\psi\rangle}^1 = U^\dagger \mathcal{A}_{\phi_{|\psi\rangle}, U|\psi\rangle}$ is instead

$$\begin{aligned} \rho'_{c=1} &= U^\dagger \mathcal{A}_{\phi_{|\psi\rangle}, U|\psi\rangle} \left(\langle \psi | U^\dagger \mathcal{A}_{\phi_{|\psi\rangle}, U|\psi\rangle} \otimes \mathbf{1} \right) \sigma \left(\mathcal{A}_{\phi_{|\psi\rangle}, U|\psi\rangle} U|\psi\rangle \otimes \mathbf{1} \right) \mathcal{A}_{\phi_{|\psi\rangle}, U|\psi\rangle} U \\ &= U^\dagger \left(\langle \psi | U^\dagger \otimes \mathbf{1} \right) \left(\mathcal{A}_{\phi_{|\psi\rangle}, U|\psi\rangle} \otimes \mathcal{A}_{\phi_{|\psi\rangle}, U|\psi\rangle} \right) \sigma \left(\mathcal{A}_{\phi_{|\psi\rangle}, U|\psi\rangle} \otimes \mathcal{A}_{\phi_{|\psi\rangle}, U|\psi\rangle} \right) \left(U|\psi\rangle \otimes \mathbf{1} \right) U \end{aligned} \quad (3.63)$$

with measurement probability $p_{c=1} = \text{Tr}\{\rho_{c=1}\}$ and normalized state $\rho_{c=1} = \rho'_{c=1}/p_{c=1}$. The resulting state can be described as a mixture between the states corresponding to the different measurement outcomes weighted by their respective probabilities, i.e.,

$$\rho = p_{c=0}\rho_{c=0} + p_{c=1}\rho_{c=1} = \rho'_{c=0} + \rho'_{c=1} = \Lambda_{\phi_{|\psi\rangle}, \sigma, U}(|\psi\rangle). \quad (3.64)$$

□

We note that the effective remote-state-preparation channel is not a true quantum channel, i.e., it is not a completely positive trace-preserving (CPTP) map between density matrices. In fact, it is only defined for pure states, and can not (straightforwardly) be rephrased as a linear operator on a density matrix. However, the output state is a valid density matrix with trace 1, as it should be as it is the result of a measurement on and unitary evolution of the resource state σ .

Theorem 3.3 *Equivalence of VBQC with remote state preparation. Assume all local operations at both the server and the client are noiseless. Then, there exists a function $\phi_{|\psi\rangle}$ that maps single-qubit states to real numbers such that Protocol 3.1 is equivalent to the unaltered VBQC protocol described in [36] using the rotated effective remote-state-preparation channel $\Lambda_{\phi_{|\psi\rangle}, \sigma, U}$ to send qubits in pure states from the client to the server. Here, σ is the resource state used in Protocol 3.1.*

Proof: In Protocol 3.1, the client performs bit flips on the measurement outcomes received from the server. Every measurement the server performs is in a basis of the form $\{|+\theta\rangle, |-\theta\rangle\}$ (defined in equation (3.30)). These states are mapped to each other by the Pauli Z operator, which is a $|+\theta\rangle$ -NOT operation

$$Z = \mathcal{A}_{-\theta, |+\theta\rangle}. \quad (3.65)$$

Therefore, each measurement performed by the server in Protocol 3.1 of which the result is bit flipped in case some number c is equal to one (i.e., $\delta \rightarrow \delta \oplus c$ where δ is the measurement result) can effectively be replaced by a unitary operation Z^c followed by a measurement of which the result is not bit flipped. It is thus as if the server applies the operation Z^c , even though the server never actually learns the value of c . This equivalence is essential to the proof.

First, we show that a computation round in Protocol 3.1 is equivalent to a computation round in the unaltered VBQC protocol when sending the qubits using $\Lambda_{\phi_{|\psi\rangle}, \sigma, U}$ in case a specific condition on $\phi_{|\psi\rangle}$ holds. In a computation round, for each of the qubits held by the server, it first performs the unitary operation U^\dagger . Then, it executes a number of CZ gates between the qubit and some other qubits. We remind the reader that CZ gates are symmetric in the two partaking qubits; we can thus always choose which qubit we consider the control qubit and which we consider the target qubit as we find convenient. These gates

are followed by a measurement in the basis $\{|+\theta\rangle, |-\theta\rangle\}$, where the angle θ is specified by the client. The outcome δ of the measurement is bit flipped by the client according to $\delta \rightarrow \delta \oplus c_v$. In shorthand, we will write the sequence as: U^\dagger , CZs, measurement, bit flip. We will show that this sequence is equivalent to a sequence that we can apply Lemma 3.5 to. As a first step, we use the equivalence stated in the first paragraph of this proof to replace the measurement followed by a bit flip by a measurement preceded by the operation Z^{c_v} . The sequence is thus equivalent to the sequence: U^\dagger , CZs, Z^{c_v} , measurement. As a second step, because Z commutes with CZ, we rewrite the sequence as: U^\dagger , Z^{c_v} , CZs, measurement.

Now, using equation (3.65), the sequence can be rewritten as follows: U^\dagger , $\mathcal{A}_{-\theta, |+\theta\rangle}^{c_v}$, CZs, measurement. To enable us to move the operator U^\dagger in this sequence, we represent the unitary U in general matrix form

$$U = \begin{bmatrix} a & b \\ -e^{i\varphi} b^* & e^{i\varphi} a^* \end{bmatrix}, \quad (3.66)$$

where $|a|^2 + |b|^2 = 1$ and $\varphi \in [0, 2\pi)$. This can be used to verify that

$$Y(U|\psi\rangle) = e^{-i\varphi} UY(|\psi\rangle). \quad (3.67)$$

Therefore, for every U , there exists a φ such that for every ϕ and every $|\psi\rangle$

$$\begin{aligned} U^\dagger \mathcal{A}_{\phi-\varphi, U|\psi\rangle} &= U^\dagger \left[e^{-i(\phi-\varphi)} e^{-i\varphi} UY(|\psi\rangle) \langle\psi| U^\dagger + e^{i(\phi-\varphi)} U|\psi\rangle (e^{-i\varphi} UY(|\psi\rangle))^\dagger \right] \\ &= \mathcal{A}_{\phi, |\psi\rangle} U^\dagger. \end{aligned} \quad (3.68)$$

From this, we conclude that there exists a φ (determined by U) such that the sequence on qubit v is equivalent to: $\mathcal{A}_{-(\theta_v+\varphi), U|+\theta_v\rangle}^{c_v}$, U^\dagger , CZs, measurement. At this point, we are able to invoke Lemma 3.5. From this lemma, it follows that the client performing its measurement followed by the server applying the above sequence is equivalent to the client sending the state $|+\theta_v\rangle$ through a channel $\Lambda_{\phi_{|\psi\rangle}, \sigma, U}$ for which $\phi_{|+\theta\rangle} = -\theta - \varphi$, after which the server applies the sequence: CZs, measurement. This is exactly the sequence of operations in the unaltered VBQC protocol. Therefore it follows that a computation round in Protocol 3.1 is equivalent to a computation round in the unaltered VBQC protocol where the channel $\Lambda_{\phi_{|\psi\rangle}, \sigma, U}$ is used to send qubits from the client to the server in case the condition $\phi_{|+\theta\rangle} = -\theta - \varphi$ is met.

It now remains to show the same equivalence between the two protocols for test rounds. For the trap qubit v , we can again replace the measurement followed by $c_v \oplus \bigoplus_{w \in N_G(v)} c_w = \bar{c}$ bit flips by a measurement without bit flips preceded by the operator $Z^{\bar{c}}$. The sequence of operations on the trap then becomes: U^\dagger , CZ gates with dummy qubits, $Z^{\bar{c}}$, and then a measurement. Now, the identity

$$CZ(\mathbf{1} \otimes Z) = (X \otimes \mathbf{1}) CZ (X \otimes \mathbf{1}) \quad (3.69)$$

can be used to move every bit flip due to a measurement outcome in the preparation of a dummy qubit by the client to the corresponding qubit at the server. That is, each Z^{c_w} for $w \in N_G(v)$ is moved to the qubit w . What remains at the trap qubit v itself is then exactly

the same sequence of operations as in a computation round. From what we have shown above for computation rounds, it follows that we can treat trap qubits in test rounds of Protocol 3.1 as if they are trap qubits in test rounds of the unaltered VBQC protocol, where the qubits are sent from the client to the server using the channel $\Lambda_{\phi_{|\psi\rangle}, \sigma, U}$ if $\phi_{|+\theta\rangle} = -\theta - \varphi$. It then remains only to show that the equivalence holds for the dummy qubits.

Now, we focus on one of the dummy qubits, which we denote w . Consider the scenario where the client attempts to send the qubit w in the state $|d\rangle$, where $d \in \{0, 1\}$, to the server as in Protocol 3.1. This qubit is the server's half of the resource state σ . The client measures its half of σ in the basis $\{U|d\rangle, Y(U|d)\rangle\}$, with measurement outcome c_w . At the server, the following sequence of operations is applied to the qubit w : U^\dagger , $\prod_{u \in N_G(w)} CZ_{w,u}$, measurement in the basis $\{|+\theta\rangle, |-\theta\rangle\}$ for some θ . Let us first consider the case where all $u \in N_G(w)$ are trap qubits. Then, by moving the effects of bit flips from trap qubits to dummy qubits as described above, every $CZ_{w,u}$ is effectively replaced by $(X^{c_w} \otimes \mathbf{1})CZ_{w,u}(X^{c_w} \otimes \mathbf{1})$. Because $X^2 = \mathbf{1}$, this has the effect of transforming the sequence into the following: U^\dagger , X^{c_w} , $\prod_{u \in N_G(w)} CZ_{w,u}$, X^{c_w} , measurement. The second occurrence of X^{c_w} changes the outcome of the measurement on the dummy qubit. However, the measurement outcome of the dummy qubits is of no consequence in the VBQC protocol (the outcome is sent by the server to the client and then discarded by the client). Therefore, we can effectively remove the second occurrence of X^{c_w} from the sequence. For the first occurrence, we note that X is both a $|1\rangle$ -NOT gate and a $|0\rangle$ -NOT gate,

$$X = \mathcal{A}_{|1\rangle} = -\mathcal{A}_{|0\rangle}. \quad (3.70)$$

Therefore, up to a global phase in case $d = 0$, the sequence becomes equivalent to: U^\dagger , $\mathcal{A}_{|d\rangle}$, $\prod_{u \in N_G(w)} CZ_{w,u}$, measurement. We note that the unitary U is here the same as for the trap qubit (it is the same for all qubits in Protocol 3.1). Therefore, we can invoke equation (3.68) again to rewrite the sequence as: $\mathcal{A}_{-\varphi, U|d\rangle}$, U^\dagger , $\prod_{u \in N_G(w)} CZ_{w,u}$, measurement. It then immediately follows from Lemma 3.5 that this is equivalent to the client sending the qubit w in the pure state $|d\rangle$ using a quantum channel $\Lambda_{\phi_{|\psi\rangle}, \sigma, U}$ for which $\phi_{|d\rangle} = -\varphi$. After the server receives the qubit through this effective channel, the remaining sequence is: $\prod_{u \in N_G(w)} CZ_{w,u}$, measurement. This is the same as in the unaltered VBQC protocol, and therefore we can treat dummy qubits in test rounds of Protocol 3.1 as if they are dummy qubits in the unaltered VBQC protocol that are transmitted using $\Lambda_{\phi_{|\psi\rangle}, \sigma, U}$ with the condition $\phi_{|0\rangle} = \phi_{|1\rangle} = -\varphi$, provided they are only adjacent to trap qubits in the computation graph G .

As final part of our proof, we show that the above derivation for dummy qubits still holds in case they are adjacent to other dummy qubits in the computation graph. Every CZ with a trap qubit results in two X^{c_w} s. When the dummy qubit is only adjacent to trap qubits, X^{c_w} s resulting from neighboring CZs then cancel out in the middle (because $X^2 = \mathbf{1}$), such that only operators at the beginning and ending of the entire sequence remain. However, a CZ with another dummy qubit does not give any X^{c_w} s. X^{c_w} s from CZs with trap qubits that enclose one or more CZs with dummy qubits can then no longer cancel against one another. A way out is offered by the following identity:

$$(\mathbf{1} \otimes X)CZ = CZ(Z \otimes X). \quad (3.71)$$

This means that X can be commuted through CZs at the cost of inducing a Z at the other qubit partaking in the CZ. Now, if a Z is induced on a dummy qubit, it can be commuted

through all CZs the dummy partakes in and placed in front of the measurement. Here, it results in an effective bit flip on the measurement outcome. Since again the measurement outcomes at the dummy qubits are inconsequential, the operator can safely be ignored. This means that X^{c_w} s can safely commute through all the CZs with other dummy qubits, allowing them to cancel out as before and get again to a sequence where there is one X^{c_w} before all the CZs and one after. The sequence then is the same as when the dummy qubit would not be adjacent to other dummy qubits, and the same conclusion derived in the above paragraph holds.

Combining all the above, we conclude that Protocol 3.1 is equivalent to the VBQC protocol [36] using the channel $\Lambda_{\phi_{|\psi\rangle}, \sigma, U}$ to send pure state from the client to the server. This holds for any function $\phi_{|\psi\rangle}$ that satisfies

$$\phi_{|+\theta\rangle} = -\theta - \varphi, \quad (3.72)$$

$$\phi_{|d\rangle} = -\varphi, \quad (3.73)$$

for any $d \in \{0, 1\}$, for any $\theta \in [0, 2\pi)$, and where φ depends on the choice of unitary U in Protocol 3.1 (it is the parameter appearing in equation (3.66)). There exists an infinite number of functions satisfying this condition (note that it is not required that the function is continuous; in fact it does not matter in the least how the function behaves away from $|d\rangle$ and $|+\theta\rangle$ as these are the only states that are ever sent through the channel), and therefore the theorem is proven. \square

Lemma 3.6 *Equivalence of remote state preparation and quantum teleportation. The average fidelity of the effective remote-state-preparation channel (equation (3.61)) corresponding to the two-qubit state σ ,*

$$F_{RSP}(\sigma) \equiv \int_{\psi} d\psi \langle \psi | \Lambda_{\phi_{|\psi\rangle}, \sigma}(|\psi\rangle) | \psi \rangle, \quad (3.74)$$

is independent of the function $\phi_{|\psi\rangle}$. Furthermore, it is equal to the average teleportation fidelity corresponding to the same state σ (equation (3.24)). That is,

$$F_{RSP}(\sigma) = F_{tel}(\sigma) \quad (3.75)$$

Proof: First we rewrite the average teleportation fidelity defined in equation (3.24) as

$$F_{tel}(\sigma) = \sum_{i,j} \int_{\psi} d\psi \left(\langle \psi | \otimes \langle \Phi_{00} | \right) \left(X^i Z^j \otimes X^i Z^j \otimes \mathbf{1} \right) (\sigma \otimes |\psi\rangle\langle\psi|) \left(X^i Z^j \otimes X^i Z^j \otimes \mathbf{1} \right) \left(|\psi\rangle \otimes |\Phi_{00}\rangle \right). \quad (3.76)$$

Then we use the property

$$\langle \Phi_{00} | (\mathbf{1} \otimes |\psi\rangle) = \frac{1}{\sqrt{2}} \langle \psi | \quad (3.77)$$

to find

$$F_{tel}(\sigma) = \frac{1}{2} \sum_{i,j} \int_{\psi} d\psi \left(\langle \psi | \otimes \langle \psi | \right) \left(X^i Z^j \otimes X^i Z^j \right) \left(X^i Z^j \otimes X^i Z^j \right) \left(|\psi\rangle \otimes |\psi\rangle \right). \quad (3.78)$$

Since the Haar measure is invariant under unitaries, the $X^i Z^j$ can be absorbed into the state $|\psi\rangle$, giving

$$F_{\text{tel}}(\sigma) = 2 \int_{\psi} d\psi \left(\langle \psi | \otimes \langle \psi | \right) \sigma \left(|\psi\rangle \otimes |\psi\rangle \right). \quad (3.79)$$

Similarly we can rewrite $F_{\text{RSP}}(\sigma)$ as

$$\begin{aligned} F_{\text{RSP}}(\sigma) &= \int_{\psi} d\psi \left(\langle \psi | \otimes \langle \psi | \right) \sigma \left(|\psi\rangle \otimes |\psi\rangle \right) \\ &\quad + \int_{\psi} d\psi \left(\langle \psi | \otimes \langle \psi | \right) \left(\mathcal{A}_{\phi_{|\psi\rangle}, |\psi\rangle} \otimes \mathcal{A}_{\phi_{|\psi\rangle}, |\psi\rangle} \right) \sigma \left(\mathcal{A}_{\phi_{|\psi\rangle}, |\psi\rangle} \otimes \mathcal{A}_{\phi_{|\psi\rangle}, |\psi\rangle} \right) \left(|\psi\rangle \otimes |\psi\rangle \right). \end{aligned} \quad (3.80)$$

The second term can be rewritten as

$$\begin{aligned} &\int_{\psi} d\psi \left(e^{i\phi_{|\psi\rangle}} (Y(|\psi\rangle))^\dagger \otimes e^{i\phi_{|\psi\rangle}} (Y(|\psi\rangle))^\dagger \right) \sigma \left(e^{-i\phi_{|\psi\rangle}} Y(|\psi\rangle) \otimes e^{-i\phi_{|\psi\rangle}} Y(|\psi\rangle) \right) \\ &= \int_{\psi} d\psi \left((Y(|\psi\rangle))^\dagger \otimes (Y(|\psi\rangle))^\dagger \right) \sigma \left(Y(|\psi\rangle) \otimes Y(|\psi\rangle) \right) \\ &= \int_{\psi} d\psi \left(\langle \psi | \otimes \langle \psi | \right) \sigma \left(|\psi\rangle \otimes |\psi\rangle \right). \end{aligned} \quad (3.81)$$

The last step here follows from the fact that an integral over all antipodal points on the Bloch sphere is itself just an integral over all points on the Bloch sphere. We thus find

$$F_{\text{RSP}}(\sigma) = 2 \int_{\psi} d\psi \left(\langle \psi | \otimes \langle \psi | \right) \sigma \left(|\psi\rangle \otimes |\psi\rangle \right). \quad (3.82)$$

□

Theorem 3.4 *Requirements on entanglement generation for VBQC through remote state preparation. Assume a quantum link generates the two-qubit state σ between a client and a server with average rate R . Furthermore, assume that qubits at the server are stored in a depolarizing memory with coherence time T . Lastly, assume that all local operations are noiseless and instantaneous. Then, a unitary U exists such that Protocol 3.1 can be executed to realize the VBQC protocol [36] for a two-qubit deterministic quantum computation in a way that is composable secure with exponentially small ϵ if*

$$F_{\text{tel}}(\sigma) > \frac{1}{2} \left(1 + \frac{1}{\sqrt{2}} e^{\frac{1}{2RT}} \right). \quad (3.83)$$

Proof: By Theorem 3.3, there exists a function $\phi_{|\psi\rangle}$ such that Protocol 3.1 is equivalent to the VBQC protocol as presented in [36] where qubits are transmitted using the channel $\Lambda_{\phi_{|\psi\rangle}, \sigma, U}$. Therefore, we can simply repeat the proof of Theorem 3.1 but with the channel $\Lambda_{\sigma, U}$ replaced by $\Lambda_{\phi_{|\psi\rangle}, \sigma, U}$. This results then exactly in Eq. (3.83), but with $F_{\text{tel}}(\sigma)$ replaced by the average fidelity over $\Lambda_{\phi_{|\psi\rangle}, \sigma}$, i.e., $F_{\text{RSP}}(\sigma)$. Eq. (3.83) then follows directly from Lemma 3.6.

We note that in order to repeat the proof of Theorem 3.1 two properties of the effective remote-state-preparation channel need to hold. Specifically, they need to hold in order to

reproduce Lemma 3.4. These are properties that hold for any linear CPTP map. $\Lambda_{\phi_{|\psi\rangle}, \sigma, U}$ however is not linear, but the properties can still be shown to hold. First, the average fidelity of the channel is invariant under unitary transformations. That is,

$$\int_{\psi} d\psi \langle \psi | \Lambda_{\phi_{|\psi\rangle}, \sigma, U}(|\psi\rangle) | \psi \rangle = F_{\text{RSP}}(\sigma) \quad (3.84)$$

3

for any unitary U . This follows most evidently from Eq. (3.82), where the effect of including a unitary U would be just to replace $|\psi\rangle \rightarrow U|\psi\rangle$, which leaves the Haar measure invariant.

Second, it needs to be shown that $F_{\text{RSP}}(\sigma)$ can be evaluated by evaluating the fidelity of $\Lambda_{\text{RSP}, \sigma}$ only at six states on the Bloch sphere forming a regular octahedron. To this end, we use the fact that six states forming a regular octahedron are the union of three mutually unbiased bases and hence form a complex projective 2-design [103]. Therefore an integral over the Bloch sphere of which the integrand is a second-order polynomial in $|\psi\rangle\langle\psi|$ can be replaced by an average over those six states. We note that this cannot be applied to Eq. (3.80) directly, as the dependence of $\mathcal{A}_{\phi_{|\psi\rangle}, |\psi\rangle}$ on $|\psi\rangle$ means that the integrand is not necessarily a second-order polynomial. However, it can be applied directly to Eq. (3.82) to express $F_{\text{RSP}}(\sigma)$ as an average over the six states. Below, we show that the resulting expression is the same as taking the average over the six states directly in Eq. (3.80).

An octahedron is made up out of three pairs of antipodal points, so we denote the set of six states $\{|\psi_i\rangle, Y(|\psi_i\rangle)\}$ for $i = 0, 1, 2$. Then, we can write (3.82) as

$$F_{\text{RSP}}(\sigma) = \frac{1}{3} \left(\sum_i \left(\langle \psi_i | \otimes \langle \psi_i | \right) \sigma \left(| \psi_i \rangle \otimes | \psi_i \rangle \right) + \sum_i \left((Y(|\psi_i\rangle))^{\dagger} \otimes (Y(|\psi_i\rangle))^{\dagger} \right) \sigma \left((Y(|\psi_i\rangle)) \otimes (Y(|\psi_i\rangle)) \right) \right). \quad (3.85)$$

It now remains to show that this is the same expression as what one would get from directly averaging the channel fidelity over these six states. This direct average can be

written as

$$\begin{aligned}
& \frac{1}{6} \left(\sum_i \langle \psi_i | \Lambda_{\phi_{|\psi\rangle}, \sigma} (|\psi_i\rangle) | \psi_i \rangle + \sum_i (Y(|\psi_i\rangle))^{\dagger} \Lambda_{\phi_{|\psi\rangle}, \sigma} (Y(|\psi_i\rangle)) Y(|\psi_i\rangle) \right) \\
&= \frac{1}{6} \left(\sum_i \left(\langle \psi_i | \otimes \langle \psi_i | \right) \sigma \left(| \psi_i \rangle \otimes | \psi_i \rangle \right) + \sum_i \left((Y(|\psi_i\rangle))^{\dagger} \otimes (Y(|\psi_i\rangle))^{\dagger} \right) \sigma \left((Y(|\psi_i\rangle)) \otimes (Y(|\psi_i\rangle)) \right) \right) \\
&+ \frac{1}{6} \left(\sum_i \left(\langle \psi_i | \otimes \langle \psi_i | \right) \left(\mathcal{A}_{\phi_{|\psi_i\rangle}, |\psi_i\rangle} \otimes \mathcal{A}_{\phi_{|\psi_i\rangle}, |\psi_i\rangle} \right) \sigma \left(\mathcal{A}_{\phi_{|\psi_i\rangle}, |\psi_i\rangle} \otimes \mathcal{A}_{\phi_{|\psi_i\rangle}, |\psi_i\rangle} \right) \left(| \psi_i \rangle \otimes | \psi_i \rangle \right) \right) \\
&+ \sum_i \left((Y(|\psi_i\rangle))^{\dagger} \otimes (Y(|\psi_i\rangle))^{\dagger} \right) \left(\mathcal{A}_{\phi_{|\psi_i\rangle}, |\psi_i\rangle} \otimes \mathcal{A}_{\phi_{|\psi_i\rangle}, |\psi_i\rangle} \right) \sigma \left(\mathcal{A}_{\phi_{|\psi_i\rangle}, |\psi_i\rangle} \otimes \mathcal{A}_{\phi_{|\psi_i\rangle}, |\psi_i\rangle} \right) \left((Y(|\psi_i\rangle)) \otimes (Y(|\psi_i\rangle)) \right) \\
&= \frac{1}{6} \left(\sum_i \left(\langle \psi_i | \otimes \langle \psi_i | \right) \sigma \left(| \psi_i \rangle \otimes | \psi_i \rangle \right) + \sum_i \left((Y(|\psi_i\rangle))^{\dagger} \otimes (Y(|\psi_i\rangle))^{\dagger} \right) \sigma \left((Y(|\psi_i\rangle)) \otimes (Y(|\psi_i\rangle)) \right) \right) \\
&+ \frac{1}{6} \left(\sum_i \left(e^{-i\phi_{|\psi_i\rangle}} (Y(|\psi_i\rangle))^{\dagger} \otimes e^{-i\phi_{|\psi_i\rangle}} (Y(|\psi_i\rangle))^{\dagger} \right) \sigma \left(e^{i\phi_{|\psi_i\rangle}} Y(|\psi_i\rangle) \otimes e^{i\phi_{|\psi_i\rangle}} Y(|\psi_i\rangle) \right) \right) \\
&+ \sum_i \left(e^{i\phi_{|\psi_i\rangle}} \langle \psi_i | \otimes e^{i\phi_{|\psi_i\rangle}} \langle \psi_i | \right) \sigma \left(e^{-i\phi_{|\psi_i\rangle}} | \psi_i \rangle \otimes e^{-i\phi_{|\psi_i\rangle}} | \psi_i \rangle \right) \\
&= \frac{1}{3} \left(\sum_i \left(\langle \psi_i | \otimes \langle \psi_i | \right) \sigma \left(| \psi_i \rangle \otimes | \psi_i \rangle \right) + \sum_i \left((Y(|\psi_i\rangle))^{\dagger} \otimes (Y(|\psi_i\rangle))^{\dagger} \right) \sigma \left((Y(|\psi_i\rangle)) \otimes (Y(|\psi_i\rangle)) \right) \right). \tag{3.86}
\end{aligned}$$

Therefore, we conclude that taking the average of the fidelity over a regular octahedron of $\Lambda_{\phi_{|\psi\rangle}, \sigma}$ is equivalent to taking the average over the entire Bloch sphere using the Haar measure. We note that the above argument also holds for $\Lambda_{\phi_{|\psi\rangle}, \sigma, U}$ for any unitary U . \square

3.8 Double-click model

In this section, we derive an analytical model for the entangled states created on elementary links when using the double-click protocol, also known as the Barrett-Kok protocol [104]. This model is used as one of the building blocks of our NetSquid simulations, as mentioned in Section 3.13. To the best of our knowledge, the analytical model is a novel result.

3.8.1 Model assumptions

The double-click protocol is a protocol for heralded entanglement generation on an elementary link. First, at each of the two nodes sharing the elementary link (designated A and B), a photon is emitted. This photon can be in one of two different photonic modes. For concreteness, we will here assume these two modes are horizontal and vertical polarization ($|H\rangle$ and $|V\rangle$, respectively), as is the case for the trapped-ion systems we consider in this work. However, depending on the hardware platform that is used, they could just as well be some other modes, e.g., different temporal modes (“early” and “late”), as is the case for the color-center systems we consider. Our model does not incorporate any effects specific to the type of modes that are used, and therefore the assumption that the modes

are polarization modes is made without loss of generality. The photon is emitted such that the mode that it is in is maximally entangled with the state of the emitter, i.e. such that the emitter - photon state after emission is (up to normalization) $|0H\rangle + |1V\rangle$. Then, the photons emitted at both nodes are sent to a midpoint station.

At the midpoint station, the photons from the two different nodes are interfered on a non-polarizing beam splitter. The two output modes are then passed through a polarizing beam splitter, of which each output mode is impinged on a single-photon detector. There are thus four single-photon detectors, two corresponding to horizontal polarization, and two corresponding to vertical polarization. This setup is illustrated in Figure 3.13. If a single photon is detected at one of the “horizontal” detectors and one at the “vertical” detectors, assuming photons in the same polarization emitted at different nodes are indistinguishable, the photons are projected on the state $|HV\rangle \pm |VH\rangle$. This results in the emitters being in the maximally entangled state $|\Psi^\pm\rangle = |01\rangle \pm |10\rangle$. The + state is obtained if the two detectors clicking are located behind the same polarizing beam splitter, while the – state is obtained if they are located behind different polarizing beam splitters. Note: if a different type of modes is used, this setup may look slightly different. For example, in case temporal modes are used, there is no need for polarizing beam splitters and using only two single-photon detectors is sufficient as the different modes can be distinguished based on the time at which they are detected.

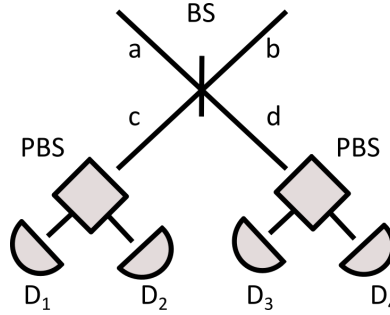


Figure 3.13: Setup of midpoint station in double-click entanglement generation using polarization-encoded photons. Two photonic modes (a and b) are interfered on a non-polarizing 50-50 beam splitter (BS). The output modes (c and d) are then each led into a separate polarizing beam splitter (PBS). Each of the two output modes of each of the two polarizing beam splitters is caught at one of four detectors (D1, D2, D3 and D4).

In our simulations, we use an analytical model to describe the success probability and post-measurement state of the double-click scheme in the presence of several imperfections. The imperfections included in our model are

- Photon loss. Due to nonunit collection efficiency of emitters, attenuation losses in optical fiber and inefficiency of single-photon detectors, there is often only a small probability that an emitted photon is not lost before it partakes in the midpoint measurement. This is captured by the parameters p_A and p_B , where p_A (p_B) denotes the detection probability given that a photon is emitted at node A (B). These account both for attenuation losses and for the photon detection probability excluding attenuation losses.
- Imperfect indistinguishability. We assume photons emitted by the different nodes

with the same polarization are not perfectly indistinguishable. This is captured using the Hong-Ou-Mandel visibility V [75, 76]. We assume the visibility is the same between two horizontally polarized photons as between two vertically polarized photons.

- **Non-photon-number-resolving detectors.** In our model, we distinguish between the case of photon-number-resolving detectors (case NR) and non-photon-number-resolving detectors (case NNR). If the used detectors are NR, when there are two or more photons at the same detector during a single midpoint measurement, all photons are registered individually. However, if detectors are NNR, they cannot distinguish between one or more photons. This model does not account for the case when photons can sometimes, but not always, be distinguished. Such behavior occurs in reality when e.g. two photons can only be resolved if the time between their detections is large enough.
- **Detector dark counts.** Sometimes, single-photon detectors report the presence of a photon when there is none. We model this using a fixed dark-count probability, p_{dc} . During a midpoint measurement, each single-photon detector gives a single dark count with probability p_{dc} , and gives none with probability $1 - p_{dc}$. Note that, in reality, for NR detectors, there is also a nonzero probability for multiple dark counts to occur during a single midpoint measurement in the same detector. Therefore, for NR detectors, treating dark counts this way will only lead to an approximation. The approximation can be expected to be accurate if the probability of multiple dark counts is negligible. For NNR detectors, this way of treating dark counts does not lead to an approximation but is perfectly accurate; multiple dark counts cannot be distinguished from one dark count, and therefore the probability of two or more dark counts and the probability of one dark count can be safely absorbed into one number, which is p_{dc} .
- **Imperfect emission.** It is possible that, directly after emission, the emitter and photon are not in the maximally entangled state $|\phi\rangle = \frac{1}{\sqrt{2}}(|0H\rangle + |1V\rangle)$. To capture this, the state is modelled as a Werner state of the form $\rho_{\text{emit}} = q|\phi\rangle\langle\phi| + (1-q)\frac{1}{4}$. For each node, the parameter q is chosen such that $F_{\text{em } A} (F_{\text{em } B})$ is the emission fidelity $q + (1-q)/4 = \frac{1}{4}(1+3q)$ at node A (B).

3.8.2 POVMs

To derive an analytical model, we notice that the midpoint station effectively implements a single-click midpoint measurement on each of the two different photonic modes (horizontal and vertical) separately. To make use of this, we write the photonic states as Fock states on the two different modes, such that $|H\rangle = |1\rangle_H |0\rangle_V$ and $|V\rangle = |0\rangle_H |1\rangle_V$. Distinguishing also between photons arriving from side A and side B, this allows us to write the pre-measurement state as a state in the Hilbert space that is obtained from taking the tensor product between the Hilbert spaces of the emitters and the horizontally and vertically polarized photons. That is, $\mathcal{H}_{\text{pre-measurement}} = \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{H_A} \otimes \mathcal{H}_{H_B} \otimes \mathcal{H}_{V_A} \otimes \mathcal{H}_{V_B}$. Since we are not interested in the post-measurement state of the photons, we can model

the measurement as a POVM *. The POVM elements of the double-click midpoint station can then be derived from the single-click measurement operators as

$$M_{\text{double click}, ijkl} = \mathbf{1}_A \otimes \mathbf{1}_B \otimes [M_{\text{single click}, ij}]_{H_A H_B} \otimes [M_{\text{single click}, kl}]_{V_A V_B}. \quad (3.87)$$

Here, $M_{\text{single click}, ij}$ is the POVM element corresponding to i clicks in the first detector and j clicks in the second detector of a single-click setup. Thus, keeping in line with the naming of Figure 3.13, $M_{\text{double click}, ijkl}$ is the POVM element corresponding to i clicks in detector 1, j clicks in detector 3, k clicks in detector 2, and l clicks in detector 4, such that detectors 1 and 3, and 2 and 4 correspond to the same polarization, and detector 1 and 2, and 3 and 4, correspond to the same polarizing beam splitter. The single-click POVM elements can be obtained from Section D.5.2 of the supplemental material of [79]. In doing so, we identify the square absolute value of the overlap of the two photon wave functions, $|\mu|^2$ in [79], with the Hong-Ou-Mandel visibility V . The reason for this is that these two are the same when both photons are in a pure state [76] (we note that the photons in our model are only mixed in the polarization degree of freedom, the wave packets themselves are pure and therefore we can safely make the substitution). We modify the single-click POVM elements from [79] to account for dark counts as follows (dropping the “single click” subscript):

$$\begin{aligned} M'_{10} &= M_{10}(1 - p_{\text{dc}})^2 + M_{00}p_{\text{dc}}(1 - p_{\text{dc}}), \\ M'_{20} &= M_{20}(1 - p_{\text{dc}}) + M_{10}p_{\text{dc}}(1 - p_{\text{dc}}), \end{aligned} \quad (3.88)$$

and similarly for M'_{01} and M'_{02} . Note that we have absorbed the POVM element $M'_{30} = M_{20}p_{\text{dc}}(1 - p_{\text{dc}})$ into the POVM element M'_{20} , since for neither NR and NNR detectors will the occurrence of two and the occurrence of three detections be discriminated; for NNR detectors, the different detection events cannot be resolved, while for NR detectors, both the presence of two and of three detections will lead to heralded failure. Other POVM elements (M'_{00} , M'_{11} , M'_{21} , ...) are not needed for our analysis, since having no detection in one of the polarizations, or having two detections at different detectors for one of the modes, is always heralded as a failure.

The double-click protocol heralds two different measurement outcomes as success, namely outcome “detectors behind same polarizing beam splitter” and outcome “detectors behind different polarizing beam splitters”. These two outcomes are henceforth abbreviated “same PBS” and “different PBS”. To determine the probability of each occurring and the corresponding post-measurement states, we need to write down the POVM elements corresponding to these two outcomes. Here, we note that in the case NR, the presence of multiple detections in a single detector is always heralded as a failure, while in the case NNR, multiple detections cannot be distinguished from a single detection. This gives the

*Note that we are interested in the post-measurement state of the emitters. However, as long as the state of the photons is traced out immediately after the measurement, a POVM is sufficient to accurately determine the post-measurement state.

POVM elements (only writing the part acting on $\mathcal{H}_{H_A} \otimes \mathcal{H}_{H_B} \otimes \mathcal{H}_{V_A} \otimes \mathcal{H}_{V_B}$)

$$\begin{aligned}
 M_{\text{same PBS, NR}} &= M'_{01} \otimes M'_{01} + M'_{10} \otimes M'_{10}, \\
 M_{\text{different PBS, NR}} &= M'_{01} \otimes M'_{10} + M'_{10} \otimes M'_{01}, \\
 M_{\text{same PBS, NNR}} &= \sum_{n,m=1,2} \left(M'_{0n} \otimes M'_{0m} + M'_{n0} \otimes M'_{m0} \right), \\
 M_{\text{different PBS, NNR}} &= \sum_{n,m=1,2} \left(M'_{0n} \otimes M'_{m0} + M'_{n0} \otimes M'_{m0} \right).
 \end{aligned} \tag{3.89}$$

3

3.8.3 Results without coincidence window

To derive formulas for the success probability and post-measurement state, we explicitly calculate the probabilities and post-measurement states of the above POVM elements on the six-qubit space using the symbolic-mathematics Python package SymPy [105]. The corresponding code can be found in the repository holding our simulation code [106]. The results are obtained by first initializing Werner states for each node and applying amplitude-damping channels with loss parameter $1 - p_A$ on the \mathcal{H}_{H_A} and \mathcal{H}_{V_A} subspaces and $1 - p_B$ on the \mathcal{H}_{H_B} and \mathcal{H}_{V_B} subspaces. Then the probability and post-measurement state for both the “same PBS” and “different PBS” measurement outcomes are calculated from this pre-measurement state in both the cases NR and NNR. The result can be written as

$$\begin{aligned}
 p_{\text{double click}} &= p_T + p_{F1} + p_{F2} + p_{F3} + p_{F4}, \\
 \rho_{\text{double click}} &= q_{\text{em}} \left(p_T |\Psi^\pm\rangle\langle\Psi^\pm| + p_{F1} \frac{|01\rangle\langle 01| + |10\rangle\langle 10|}{2} + p_{F2} \frac{|00\rangle\langle 00| + |11\rangle\langle 11|}{2} \right) \\
 &\quad + \left((1 - q_{\text{em}})(p_T + p_{F1} + p_{F2}) + p_{F3} + p_{F4} \right) \frac{\mathbb{1}}{4},
 \end{aligned} \tag{3.90}$$

where $p_{\text{double click}}$ is the success probability and $\rho_{\text{double click}}$ is the unnormalized post-measurement state. The different constants are defined as

$$\begin{aligned}
 q_{\text{em}} &= \frac{1}{9}(4F_{\text{em } A} - 1)(4F_{\text{em } B} - 1), \\
 p_T &= \begin{cases} \frac{1}{2}p_A p_B V(1 - p_{\text{dc}})^4 & \text{if NR,} \\ \frac{1}{2}p_A p_B V(1 - p_{\text{dc}})^2 & \text{if NNR,} \end{cases} \\
 p_{F1} &= \begin{cases} \frac{1}{2}p_A p_B (1 - V)(1 - p_{\text{dc}})^4 & \text{if NR,} \\ \frac{1}{2}p_A p_B (1 - V)(1 - p_{\text{dc}})^2 & \text{if NNR,} \end{cases} \\
 p_{F2} &= \begin{cases} 0 & \text{if NR,} \\ \frac{1}{2}p_A p_B (1 + V)p_{\text{dc}}(1 - p_{\text{dc}})^2 & \text{if NNR,} \end{cases} \\
 p_{F3} &= \begin{cases} 2[p_A(1 - p_B) + (1 - p_A)p_B]p_{\text{dc}}(1 - p_{\text{dc}})^3 & \text{if NR,} \\ 2[p_A(1 - p_B) + (1 - p_A)p_B]p_{\text{dc}}(1 - p_{\text{dc}})^2 & \text{if NNR,} \end{cases} \\
 p_{F4} &= 4(1 - p_A)(1 - p_B)p_{\text{dc}}^2(1 - p_{\text{dc}})^2.
 \end{aligned} \tag{3.91}$$

Furthermore, the Bell states are defined by

$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \quad (3.92)$$

The different terms in the equations can be interpreted as corresponding to different possible detection cases, with p_i being the probability of case i occurring, and the density matrix that it multiplies with the state that is created in that case. The different cases are as follows.

- **case T.** This is a “true” heralded success. That is, two photons were detected at the midpoint station (probability $p_A p_B$) in different polarizations (probability $\frac{1}{2}$), and they behaved as indistinguishable photons (i.e. they interfered) (probability V). Finally, there cannot have been dark counts in any of the detectors, except for the detectors at which the photons were detected in the case of non-number-resolving detectors (as this doesn’t change the outcome). The resulting density matrix is one corresponding to the Bell state $|\Psi^\pm\rangle$ (+ for both detections at the same polarizing beam splitter, - for both detections at different polarizing beam splitters).
- **case F1.** This is the first “false” heralded success (i.e. a false positive; a “success” detection pattern is observed without there being a maximally entangled state). Again, two photons arrived at the midpoint station and were detected in different polarizations (probability $\frac{1}{2} p_A p_B$). However, they did not behave as indistinguishable photons (i.e. they did not interfere) (probability $(1 - V)$). Since the photons are in different polarizations, the post-measurement state will be classically anticorrelated $\frac{1}{2}(|01\rangle\langle 01| + |10\rangle\langle 10|)$.
- **case F2.** This is the second “false” heralded success. Two photons arrived at the midpoint station (probability $p_A p_B$) and are detected at the exact same detector. Additionally, a dark count occurs, causing a click pattern that is heralded as a success. For this, both photons need to be detected in the same polarization (probability $\frac{1}{2}$) and end up at the same detector. If they behave as indistinguishable photons (probability V), they will bunch together due to Hong-Ou-Mandel interference and will be guaranteed to go to the same detector. If they do not behave as indistinguishable photons (probability $1 - V$), there is a $\frac{1}{2}$ probability that they happen to go to the same detector. Combining, this gives a factor $V + \frac{1}{2}(1 - V) = \frac{1}{2}(1 + V)$. Since the photons are detected with the same polarization, the post-measurement state will be classically correlated $\frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)$. Note that this case cannot occur when detectors are NR, as detecting both photons at the same detector is then heralded as a failure.
- **case F3.** This is the third “false” heralded success. Only one photon arrives at the midpoint station (probability $p_A(1 - p_B) + (1 - p_A)p_B$), and a dark count makes the detector click pattern look like a success. For this, either of the two detectors corresponding to the polarization the photon is not detected in must undergo a dark count, while the remaining detectors do not undergo dark counts, which occurs with

probability $2p_{\text{dc}}(1 - p_{\text{dc}})^n$, where $n = 3$ in case NR and $n = 2$ in case NNR (because then it doesn't matter whether there is a dark count in the detector that detects the photon). There is no information about correlation between the photons, therefore the post-measurement state is maximally mixed.

- **case F4.** This is the fourth and final “false” heralded success. No photons arrive at the midpoint station (probability $(1 - p_A)(1 - p_B)$), and the detector click pattern is created solely by dark counts. Since there are four distinct click patterns resulting in a heralded success, these dark counts occur with probability $4p_{\text{dc}}^2(1 - p_{\text{dc}})^2$. There is no information about correlation between the photons, therefore the post-measurement state is maximally mixed.

Finally, to understand the role of the parameter q_{em} , note that when either of the initial emitter - photon states is maximally mixed instead of entangled, there is no correlation between the emitter and the photon. Therefore, whatever detection event takes place at the midpoint station, no information about correlation between the emitters is revealed. The post-measurement state is thus a maximally mixed state in this case. The probability that both nodes send an entangled photon instead of a maximally mixed state is exactly q_{em} , and thus the probability that the post-measurement state is maximally mixed regardless which of the above cases takes place is $1 - q_{\text{em}}$.

3.8.4 Results with coincidence window

When performing the double-click protocol, click patterns can be accepted as a success or instead rejected based on the time at which the two detector clicks are registered. A first reason for this is that each round of the double-click protocol only lasts a finite amount of time. That is, there is a detection time window corresponding to each round, and only clicks occurring during the detection time window can result in a heralded success for that specific round. If there is a nonzero probability that photons are detected outside of the detection time window, e.g. because their wave functions are stretched very long, this can be captured in the model by adjusting the detection probabilities appropriately (p_A and p_B).

However, there can also be a second reason. Sometimes, it is desirable to implement a coincidence time window. In this case, when two clicks occur within the correct detectors and within the detection time window, a success is only heralded if the time between the two clicks is smaller than the coincidence time window. While this lowers the success probability of the double-click protocol, it can increase the Hong-Ou-Mandel visibility V (thereby increasing the fidelity of entangled states created using the protocol).

To account for protocols that implement a coincidence time window, we here introduce three new parameters into our model.

- $p_{\text{ph-ph}}$, the probability that two photon detections that occur within the detection time window occur less than one coincidence time window away from each other.
- $p_{\text{ph-dc}}$, the probability that a photon detection and a dark count that occur within the detection time window occur less than one coincidence time window away from each other.
- $p_{\text{dc-dc}}$, the probability that two dark counts that occur within the detection time window occur less than one coincidence time window away from each other.

These parameters will be functions of photon-detection-time probability-density functions and the coincidence time window (we calculate them for a simplified model of the photon state in Section 3.9) Then, we make the following adjustments to the above results to account for the coincidence time window:

$$\begin{aligned}
 p_T &\rightarrow p_{\text{ph-ph}} p_T, \\
 p_{F1} &\rightarrow p_{\text{ph-ph}} p_{F1}, \\
 p_{F2} &\rightarrow p_{\text{ph-dc}} p_{F2}, \\
 p_{F3} &\rightarrow p_{\text{ph-dc}} p_{F3}, \\
 p_{F4} &\rightarrow p_{\text{dc-dc}} p_{F4}.
 \end{aligned} \tag{3.93}$$

The reason for this is as follows. p_T corresponds to an event where two photons are detected, leading to a heralded success. When using a coincidence time window, the two photons are only close enough in time to lead to a heralded success with probability $p_{\text{ph-ph}}$. The same logic holds for p_{F1} . Probability p_{F3} corresponds to a photon detection and a dark count leading to a heralded success; that now only happens if the photon detection and dark count are within one coincidence time window, which is exactly $p_{\text{ph-dc}}$. And probability p_{F4} corresponds to a heralded success due to two dark counts. These dark counts also should not be separated by too much time, giving a factor $p_{\text{dc-dc}}$. Less straightforward to adjust is p_{F2} in the NNR case. It corresponds to an event where two photons are detected within the same detector, but they are not independently resolved. The probability that the time stamp assigned to this detection is within a coincidence window from a dark count occurring in another detector, may not be exactly $p_{\text{ph-dc}}$. However, we do expect it to be a reasonable approximation, and therefore we use $p_{\text{ph-dc}}$ to avoid introducing a fourth new parameter to the model.

3.9 Effect of detection and coincidence time windows

In the double-click protocol, success is declared only if there are clicks in two detectors that measure different polarization modes. These clicks typically occur at random times, and a prerequisite for success is that certain conditions on the detection times are met. First, in any practical experiment, detection time windows have to be of finite duration. If a click only occurs after the detection time window closes, it is effectively not detected. Thus, success is only declared if two clicks occur within the detection time window. Second, it is sometimes beneficial to also condition success on the time difference between the two clicks. In that case, a success is only declared if the time between the clicks does not exceed the coincidence time window. This can help boost the Hong-Ou-Mandel visibility of the photon interference and thereby increase the fidelity of entangled states.

In Section 3.8, we present a model that allows for the calculation of the success probability of the double-click protocol and the two-qubit state that it creates. The coincidence probabilities between two photons, two dark counts and a photon and a dark count are free parameters in this model, just as the visibility and the photon detection probability. To accurately account for the detection time window and coincidence time window in this model, these parameters need to be given appropriate values. In this section, we introduce a simplified model for the photon state that allows us to calculate the required values. We use this simplified model to simulate double-click entanglement generation with trapped-

ion devices, as described in Section 3.6.6. To the best of our knowledge, this is a novel result.

Definition 3.7 *Detection time window.* If a detection time window of duration $T > 0$ is used in the double-click protocol, success is only heralded if both detector clicks occur within the time interval $[0, T]$.

Definition 3.8 *Coincidence time window.* If a coincidence time window of duration $\tau > 0$ is used in the double-click protocol, success is only heralded if the time between both detector clicks does not exceed τ .

Definition 3.9 *Photon state described by $(p_{em}(t), \psi_{t_0}(t))$.* Let $p_{em}(t)$ be a function such that

$$\int_0^\infty dt p_{em}(t) = 1 \quad (3.94)$$

and let $\psi_{t_0}(t)$ be a function such that

$$\int_{t_0}^\infty dt |\psi_{t_0}(t)|^2 = 1. \quad (3.95)$$

Then, $p_{em}(t)$ can be interpreted as a probability density function for the photon emission time, and $\psi(t)$ can be interpreted as the temporal wave function of a photon emitted at $t = 0$. The tuple $(p_{em}(t), \psi(t))$ then describes a mixed photon state

$$\rho = \int_0^\infty dt_0 p_{em}(t_0) |\psi_{t_0}\rangle\langle\psi_{t_0}| \quad (3.96)$$

where

$$|\psi_{t_0}\rangle = \int_{t_0}^\infty dt \psi_{t_0}(t) a_t^\dagger |0\rangle \quad (3.97)$$

with a_t^\dagger the photon's creation operator at time t .

The temporal impurity of a state described by $(p_{em}(t), \psi_{t_0}(t))$ (if $p_{em}(t)$ is not a delta function) can reduce the Hong-Ou-Mandel visibility of photons. The reason for this is that photons that are emitted at very different times have small overlap. If two photons are detected close together, they were probably not emitted at very different times (depending on their distributions). Using a coincidence time window is then effectively applying a temporal purification to the photons, allowing for an increase in visibility.

Definition 3.10 *Double-exponential photon state (a, b) .* The double-exponential photon state described by (a, b) , where both a and b are constants with dimension time^{-1} , is the photon state described by $(p_{em}(t), \psi_{t_0}(t))$ where

$$p_{em}(t) = ae^{-at}\Theta(t) \quad (3.98)$$

and

$$\psi_{t_0}(t) = \sqrt{2b}e^{-b(t-t_0)}\Theta(t-t_0). \quad (3.99)$$

Here, $\Theta(t)$ is the Heaviside step function. That is, both the emission-time probability density function and the pure photon wavefunctions are one-sided exponentials.

In this section, we model all photons emitted by processing nodes as having a double-exponential state. The pure wave functions of photons emitted by spontaneous decay of an excited state to a ground state in a two-level system are described well as one-sided exponentials [107]. An example of a system where photons are emitted this way is NV centers [49]. Similarly, pure wave functions of photons emitted using cavity-enhanced Raman transitions (using a constant Rabi pulse), as is the case for the trapped-ion systems we study in this chapter, also look approximately exponential [108]. We note that such trapped-ion systems are exactly the use case in this chapter for the simplified model presented here. For solid-state sources such as color centers, temporal impurity of photons is not a limiting factor [107]. However, for cavity-enhanced Raman transitions, off-resonant scattering causes the photon to only be emitted at a random time after a trajectory through the ion-state manifold [87, 108]. We model the resulting temporal impurity using the function $p_{\text{em}}(t)$. We note that we do not expect this function to be exponential for cavity-enhanced Raman transitions. For instance, the function should include a $\delta(0)$ delta-function contribution to account for the probability that not a single off-resonant scattering takes place. However, in the toy model presented here, we will assume $p_{\text{em}}(t)$ is a one-sided exponential so that we have a model with a small number of parameters in which exact closed-form expressions can be obtained for the relevant quantities. As shown in Section 3.6.6, this model can be fitted well to experimental data for interference between photons emitted by ion-cavity systems.

Lemma 3.7 *Detection-time probability density function. Consider the case where a photon with double-exponential state (a, b) is emitted directly on a photon detector. Assume this photon detector is perfect except that it has a possibly nonunit detection efficiency η (with a flat response). The probability density function for the photon being detected at time t is given by*

$$p(t) = \frac{2ab\eta}{a-2b} (e^{-2bt} - e^{-at}) \Theta(t). \quad (3.100)$$

This probability density function may be subnormalized, as it is also possible that no photon is detected.

Proof: A perfect detector implements a POVM with operators $E_t = a_t^\dagger |0\rangle\langle 0| a_t$. Instead, a detector with efficiency factor η implements a POVM with operators $E'_t = \eta E_t$ and $F = 1 - \eta$, where F corresponds to no photon detection taking place. The probability density that the photon is detected at time t is then the probability density corresponding to the POVM operator E'_t , given by

$$p(t) = \text{Tr}(E'_t \rho). \quad (3.101)$$

For a photon state described by $(p_{\text{em}}(t), \psi_{t_0}(t))$, the density matrix is

$$\rho = \int_0^\infty dt_0 \int_{t_0}^\infty dt_1 \int_{t_0}^\infty dt_2 p_{\text{em}}(t_0) \psi_{t_0}(t_1) \psi_{t_0}^*(t_1) a_{t_1}^\dagger |0\rangle\langle 0| a_{t_2} \quad (3.102)$$

This can be evaluated using the cyclic property of the trace to give

$$\begin{aligned}
 p(t) &= \eta \int_0^\infty dt_0 \int_{t_0}^\infty dt_1 \int_{t_0}^\infty dt_2 p_{\text{em}}(t_0) \psi_{t_0}(t_1) \psi_{t_0}^*(t_1) \langle 0 | a_t a_{t_1}^\dagger | 0 \rangle \langle 0 | a_{t_2} a_t^\dagger | 0 \rangle \\
 &= \eta \int_0^\infty dt_0 \int_{t_0}^\infty dt_1 \int_{t_0}^\infty dt_2 p_{\text{em}}(t_0) \psi_{t_0}(t_1) \psi_{t_0}^*(t_1) \delta(t - t_1) \delta(t - t_2) \\
 &= \eta \int_0^\infty dt_0 p_{\text{em}}(t_0) |\psi_{t_0}(t)|^2.
 \end{aligned} \tag{3.103}$$

For a double-exponential photon state (a, b) , this becomes

$$\begin{aligned}
 p(t) &= 2ab\eta e^{-2bt} \int_0^\infty dt_0 e^{-(a-2b)t_0} \Theta(t - t_0) \\
 &= 2ab\eta e^{-2bt} \Theta(t) \int_0^t dt_0 e^{-(a-2b)t_0} \\
 &= 2ab\eta e^{-2b} \Theta(t) \frac{1}{a-2b} (1 - e^{-(a-2b)t}) \\
 &= \frac{2ab\eta}{a-2b} (e^{-2bt} - e^{-at}) \Theta(t).
 \end{aligned} \tag{3.104}$$

□

Definition 3.11 *Coincidence probability.* When using a detection time window T and coincidence time window of τ in the double-click protocol, the coincidence probability is the probability that given that there are two clicks within the detection time window, the clicks are also within one coincidence time window.

Our goal now is to find the coincidence probability for two double-exponential photons. This requires us to calculate the probability that two photons arrive within a time τ of one another, conditioned on each of the photons being successfully detected within the time interval $[0, T]$. To this end, we calculate the probability density function for the detection time of a double-exponential photon conditioned on the photon being successfully detected. This requires us to calculate the detection probability of the photon, i.e., the probability that it is successfully detected within the detection time window. The detection probability is also an important result in itself, as it is required by the model presented in Section 3.8 (it takes the role of p_A and p_B in this model).

Theorem 3.5 *Detection probability.* If a detection time window of duration T is used, then the probability that a photon with double-exponential state (a, b) is detected within the time window is given by

$$p_{\text{det}}(T) = \eta \left[1 - \frac{a}{a-2b} e^{-2bT} + \frac{2b}{a-2b} e^{-aT} \right]. \tag{3.105}$$

Proof: $p_{\text{det}}(T)$ is given by the probability that the photon is detected in the time interval $[0, T]$. This probability can be calculated from the probability density function

$$\begin{aligned}
 p_{\text{det}}(T) &= \int_0^T dt p(t) \\
 &= \frac{2ab\eta}{a-2b} \int_0^T dt (e^{-2bt} - e^{-at}) \\
 &= \frac{2ab\eta}{a-2b} \left[\frac{1}{2b} (1 - e^{-2bT}) - \frac{1}{a} (1 - e^{-aT}) \right] \\
 &= \frac{\eta}{a-2b} \left[a(1 - e^{-2bT}) - 2b(1 - e^{-aT}) \right] \\
 &= \eta \left[1 - \frac{a}{a-2b} e^{-2bT} + \frac{2b}{a-2b} e^{-aT} \right].
 \end{aligned} \tag{3.106}$$

□

Corollary 3.1 *When no detection time window is used, i.e., when the duration of the detection time window $T \rightarrow \infty$, then the photon detection probability is equal to the detector's detection efficiency η .*

Proof: When we take $T \rightarrow \infty$ in equation (3.105), we find $p_{\text{det}}(T) \rightarrow \eta$. □ This corresponds to the situation when the entire photon is within the detection time window and the only reason why the photon would not be detected is detector inefficiency. One can think of $p_{\text{det}}(T)/\eta$ as the “additional efficiency factor” due to not capturing the entire photon in the detection time window.

Lemma 3.8 *Conditional detection-time probability density function. Consider the case where a photon with double-exponential state (a, b) is emitted directly on a photon detector. Assume this photon detector is perfect except that it has a possibly nonunit detection efficiency η (with a flat response). The probability density function for the photon being detected at time t , if the photon is in the double-exponential state (a, b) , is given by*

$$p_T(t) = \Theta(t)\Theta(T-t) \frac{p(t)}{p_{\text{det}}(T)}. \tag{3.107}$$

Unlike $p(t)$, this probability density function is always normalized.

Proof: Let X be the continuous random variable corresponding to the detection time of the photon. Let it take the value -1 if no photon is detected, such that the corresponding probability density function $f_X(x)$ is normalized and X is well-defined as a random variable. It follows from Corollary 3.1 that the probability that this happens is $1 - \eta$. Therefore, the probability density function can then be written as

$$f_X(x) = (1 - \eta)\delta(x + 1) + \Theta(x)p(x). \tag{3.108}$$

Additionally, we define a discrete random variable Y_T which takes the value 1 if the photon is detected within the detection time window T and 0 if not. By Theorem 3.5, the

probability distribution of Y_T is given by

$$f_{Y_T}(y) = \begin{cases} p_{\text{det}}(T) & \text{if } y = 1 \\ 1 - p_{\text{det}}(T) & \text{if } y = 0. \end{cases} \quad (3.109)$$

Note that X and Y_T are not independent random variables. Now, the conditional probability density function that we are interested in is

$$p_T(x) \equiv f_{X|Y_T}(x, 1) = \frac{f_{X,Y_T}(x, 1)}{f_{Y_T}(1)} = \frac{f_{X,Y_T}(x, 1)}{p_{\text{det}}(T)}. \quad (3.110)$$

Here, $f_{X,Y_T}(x, y)$ is the mixed joint density of the continuous random variable X and the discrete random variable Y_T . When X takes a value between 0 and T , then Y_T takes the value 1 with unit probability. Otherwise, Y_T takes the value 0 with unit probability. Therefore,

$$f_{X,Y_T}(x, 1) = \Theta(x)\Theta(T-x)f_X(x) = \Theta(x)\Theta(T-x)p(x). \quad (3.111)$$

Substituting this into equation (3.110) allows us then finally to write

$$p_T(t) = \Theta(t)\Theta(T-t) \frac{p(t)}{p_{\text{det}}(T)}. \quad (3.112)$$

□

Theorem 3.6 *Coincidence probability of two photons. The coincidence probability for two photon detections, if both photons are in the double-exponential state (a, b) , a detection time window of duration T is used and the coincidence time window of duration τ is used, is given by*

$$\begin{aligned} p_{\text{ph-ph}}(T, \tau) \left(\frac{p_{\text{det}}(T)}{\eta} \right)^2 &= \frac{a^2}{a^2 - 4b^2} (1 - e^{-2b\tau}) - \frac{4b^2}{a^2 - 4b^2} (1 - e^{-a\tau}) \\ &\quad + \frac{a^2}{(a-2b)^2} (1 - e^{2b\tau}) e^{-4bT} + \frac{4b^2}{(a-2b)^2} (1 - e^{a\tau}) e^{-2aT} \\ &\quad - \frac{4ab}{(a-2b)^2} \left(1 - \frac{ae^{2b\tau} + 2be^{a\tau}}{a+2b} \right) e^{-(a+2b)T}. \end{aligned} \quad (3.113)$$

Proof: By definition, the coincidence probability is given by

$$p_{\text{ph-ph}}(T, \tau) = \iint_{|t_1 - t_2| \leq \tau} dt_1 dt_2 p_T(t_1) p_T(t_2). \quad (3.114)$$

By Lemma 3.8, this implies

$$p_{\text{ph-ph}}(T, \tau) \left(\frac{p_{\text{det}}(T)}{\eta} \right)^2 = \frac{1}{\eta^2} \iint_{|t_1 - t_2| \leq \tau} dt_1 dt_2 p(t_1) p(t_2). \quad (3.115)$$

The region of integration is $|t_1 - t_2| \leq \tau$, i.e., $-\tau \leq t_1 - t_2 \leq \tau$. The integrand is symmetric under the interchange of t_1 and t_2 . Therefore, the region $0 \leq t_1 - t_2 \leq \tau$ will give exactly the

same contribution as $-\tau \leq t_1 - t_2 \leq 0$. This has the following physical interpretation: the probability of photon 2 arriving a time Δt after photon 1 is the same as the probability of photon 1 arriving Δt after photon 2. This can be used to simplify the integral somewhat, giving

$$p_{\text{ph-ph}}(T, \tau) \left(\frac{p_{\text{det}}(T)}{\eta} \right)^2 = \frac{2}{\eta^2} \iint_{0 \leq t_1 - t_2 \leq \tau} dt_1 dt_2 p(t_1) p(t_2). \quad (3.116)$$

It follows from Lemma 3.7 that each $p(t)$ carries an overall factor $\Theta(t)\Theta(T)$. This can be absorbed into the integration limits to give

$$\begin{aligned} p_{\text{ph-ph}}(T, \tau) \left(\frac{p_{\text{det}}(T)}{\eta} \right)^2 &= \frac{2}{\eta^2} \int_0^T dt_1 \int_{t_1}^{\min(t_1 + \tau, T)} dt_2 p(t_1) p(t_2) \\ &= 2 \left(\frac{1}{\eta^2} \int_0^{T-\tau} dt_1 \int_{t_1}^{t_1 + \tau} dt_2 p(t_1) p(t_2) + \frac{1}{\eta^2} \int_{T-\tau}^T dt_1 \int_{t_1}^T dt_2 p(t_1) p(t_2) \right). \end{aligned} \quad (3.117)$$

We calculate these two integrals one by one, using Lemma 3.7. The first is

$$\begin{aligned} &\left(\frac{a-2b}{2ab} \right)^2 \left(\frac{1}{\eta^2} \int_0^{T-\tau} dt_1 \int_{t_1}^{t_1 + \tau} dt_2 p(t_1) p(t_2) \right) \\ &= \int_0^{T-\tau} dt_1 (e^{-2bt_1} - e^{-at_1}) \int_{t_1}^{t_1 + \tau} (e^{-2bt_2} - e^{-at_2}) \\ &= \int_0^{T-\tau} dt_1 (e^{-2bt_1} - e^{-at_1}) \left(\frac{1}{2b} e^{-2bt_1} (1 - e^{-2b\tau}) - \frac{1}{a} e^{-at_1} (1 - e^{-a\tau}) \right) \\ &= \frac{1 - e^{-2b\tau}}{2b} \int_0^{T-\tau} dt_1 (e^{-4bt_1} - e^{-(a+2b)t_2}) - \frac{1 - e^{-a\tau}}{a} \int_0^{T-\tau} dt_1 (e^{-(a+2b)t_1} - e^{-2at_1}) \\ &= \frac{1 - e^{-2b\tau}}{2b} \left(\frac{1 - e^{4b\tau} e^{-4bT}}{4b} - \frac{1 - e^{(a+2b)\tau} e^{-(a+2b)T}}{a+2b} \right) \\ &\quad - \frac{1 - e^{-a\tau}}{a} \left(\frac{1 - e^{(a+2b)\tau} e^{-(a+2b)T}}{a+2b} - \frac{1 - e^{2a\tau} e^{-2aT}}{2a} \right) \\ &= \frac{a-2b}{a+2b} \left(\frac{1 - e^{-2b\tau}}{8b^2} - \frac{1 - e^{-a\tau}}{2a^2} \right) + \frac{-e^{2a\tau} + e^{a\tau}}{2a^2} e^{-2aT} \\ &\quad + \frac{e^{2b\tau} - e^{4b\tau}}{8b^2} e^{-4bT} + \frac{1}{a+2b} \left(\frac{e^{(a+2b)\tau} - e^{a\tau}}{2b} + \frac{e^{(a+2b)\tau} - e^{2b\tau}}{a} \right) e^{-(a+2b)T}. \end{aligned} \quad (3.118)$$

In the last step, terms with the same exponents of T were collected. Resolving the prefactor

gives

$$\begin{aligned}
 & \frac{1}{\eta^2} \int_0^{T-\tau} dt_1 \int_{t_1}^{t_1+\tau} dt_2 p(t_1) p(t_2) \\
 &= \frac{a^2}{2(a^2-4b^2)} (1-e^{-2b\tau}) - \frac{2b^2}{2(a^2-4b^2)} (1-e^{-a\tau}) + \frac{2b^2}{(a-2b)^2} (-e^{2a\tau} + e^{a\tau}) e^{-2aT} \\
 & \quad + \frac{a^2}{2(a-2b)^2} (e^{2b\tau} - e^{4b\tau}) e^{-4bT} \\
 & \quad + \frac{2ab}{(a-2b)^2(a+2b)} \left(a(e^{(a+2b)\tau} - e^{a\tau}) + 2b(e^{(a+2b)\tau} - e^{2b\tau}) \right) e^{-(a+2b)T}.
 \end{aligned} \tag{3.119}$$

The second term is

$$\begin{aligned}
 & \left(\frac{a-2b}{2ab} \right)^2 \left(\frac{1}{\eta^2} \int_{T-\tau}^T dt_1 \int_{t_1}^T dt_2 p(t_1) p(t_2) \right) \\
 &= \int_{T-\tau}^T dt_1 (e^{-2bt_1} - e^{-at_1}) \int_{t_1}^T (e^{-2bt_2} - e^{-at_2}) \\
 &= \int_{T-\tau}^T dt_1 (e^{-2bt_1} - e^{-at_1}) \left(\frac{1}{2b} (e^{-2bt_1} - e^{-2bT}) - \frac{1}{a} (e^{-at_1} - e^{-aT}) \right) \\
 &= \frac{1}{2ab} (2be^{-aT} - ae^{-2bT}) \int_{T-\tau}^T dt_1 (e^{-2bt_1} - e^{-at_1}) + \frac{1}{2b} \int_{T-\tau}^T dt_1 e^{-4bt_1} \\
 & \quad + \frac{1}{a} \int_{T-\tau}^T dt_1 e^{-2at_1} - \frac{a+2b}{2ab} \int_{T-\tau}^T dt_1 e^{-(a+2b)t_1} \\
 &= \frac{1}{2ab} (2be^{-aT} - ae^{-2bT}) \left[\frac{e^{-2bT}}{2b} (e^{2b\tau} - 1) - \frac{e^{-aT}}{a} (e^{a\tau} - 1) \right] + \frac{e^{-4bT}}{8b^2} (e^{4b\tau} - 1) \\
 & \quad + \frac{e^{-2aT}}{2a^2} (e^{2a\tau} - 1) - \frac{e^{-(a+2b)T}}{2ab} (e^{(a+2b)\tau} - 1) \\
 &= \frac{1}{2a^2} (e^{2a\tau} - 2e^{a\tau} + 1) e^{-2aT} + \frac{1}{8b^2} (e^{4b\tau} - 2e^{2b\tau} + 1) e^{-4bT} \\
 & \quad + \frac{1}{2ab} (e^{a\tau} + e^{2b\tau} - e^{(a+2b)\tau} - 1) e^{-(a+2b)T}.
 \end{aligned} \tag{3.120}$$

Again resolving the prefactor, we find

$$\begin{aligned}
 & \frac{1}{\eta^2} \int_{T-\tau}^T dt_1 \int_{t_1}^T dt_2 p(t_1) p(t_2) \\
 &= \frac{2b^2}{(a-2b)^2} (e^{2a\tau} - 2e^{a\tau} + 1) e^{-2aT} + \frac{a^2}{2(a-2b)^2} (e^{4b\tau} - 2e^{2b\tau} + 1) e^{-4bT} \\
 & \quad + \frac{2ab}{(a-2b)^2} (e^{a\tau} + e^{2b\tau} - e^{(a+2b)\tau} - 1) e^{-(a+2b)T}.
 \end{aligned} \tag{3.121}$$

Finally, substituting equations (3.119) and (3.121) into equation (3.117) yields equation (3.113). \square

Theorem 3.7 *Coincidence probability of two dark counts. The coincidence probability for two detector dark counts if the detection time window is T and the coincidence time window is τ is given by*

$$p_{dc-dc}(T, \tau) = 1 - \left(\frac{T - \tau}{T} \right)^2, \quad (3.122)$$

assuming that dark counts occur uniformly throughout the detection time window.

Proof: Given that there is a dark count within the detection time window T , the probability density function for the time at which it occurs is given by

$$d_T(t) = \frac{1}{T} \Theta(t) \Theta(T - t) \quad (3.123)$$

because we assume the dark counts are uniformly distributed. The coincidence probability is then given by

$$\begin{aligned} p_{dc-dc}(T, \tau) &= \iint_{|t_1 - t_2| \leq \tau} dt_1 dt_2 d_T(t_1) d_T(t_2) \\ &= \frac{2}{T^2} \int_0^T dt_1 \int_{t_1}^{\min(t_1 + \tau, T)} dt_2 \\ &= \frac{2}{T^2} \left(\int_0^{T-\tau} dt_1 \int_{t_1}^{t_1 + \tau} dt_2 + \int_{T-\tau}^T dt_1 \int_{t_1}^T dt_2 \right) \\ &= \frac{2}{T^2} \left(\int_0^{T-\tau} dt_1 \tau + \int_{T-\tau}^T dt_1 (T - t_1) \right) \\ &= \frac{2}{T^2} \left((T - \tau)\tau + T\tau - \frac{1}{2}T^2 + \frac{1}{2}(T - \tau)^2 \right) \\ &= \frac{1}{T^2} (2T\tau - \tau^2) \\ &= 1 - \left(\frac{T - \tau}{T} \right)^2. \end{aligned} \quad (3.124)$$

□

Theorem 3.8 *Coincidence probability of a photon and a dark count. The coincidence probability for one photon detection and one dark count, if the photon is in the double-exponential state (a, b) , the detection time window is T and the coincidence time window is τ is given by*

$$\begin{aligned} p_{ph-dc}(T, \tau) \frac{p_{det}(T)}{\eta} &= \frac{a}{2b(a - 2b)T} \left[1 + 2b\tau - e^{-2b\tau} + e^{-2bT} (1 - 2b\tau - e^{2b\tau}) \right] \\ &\quad - \frac{2b}{a(a - 2b)T} \left[1 + a\tau - e^{-a\tau} + e^{-aT} (1 - a\tau - e^{a\tau}) \right]. \end{aligned} \quad (3.125)$$

assuming that dark counts occur uniformly throughout the detection time window.

Proof: For the photon, we again have the probability density function $p_T(t)$ as given by Lemma 3.8, while for the dark count we have the probability density function $d_T(t)$ as given by equation (3.123). The coincidence probability is then given by

$$p_{\text{ph-dc}}(T, \tau) = \iint_{|t_1 - t_2| \leq \tau} dt_1 dt_2 p_T(t_1) d_T(t_2). \quad (3.126)$$

3

When calculating the other coincidence probabilities, we were able to use a symmetry argument to simplify the integral. However, because $p_T(t) \neq d_T(t)$, we are unable to do so here. Assuming for the moment that $\tau \leq \frac{1}{2}T$ and the fact that both probability density functions are proportional to $\Theta(t)\Theta(T-t)$, we can write

$$p_{\text{ph-dc}}(T, \tau) = \left(\int_0^\tau dt_1 \int_0^{t_1+\tau} dt_2 + \int_\tau^{T-\tau} dt_1 \int_{t_1-\tau}^{t_1+\tau} dt_2 + \int_{T-\tau}^T dt_1 \int_{t_1-\tau}^T dt_2 \right) p_T(t_1) d_T(t_2). \quad (3.127)$$

This becomes

$$\begin{aligned} & p_{\text{ph-dc}}(T, \tau) \frac{p_{\text{det}}(T)T}{\eta} \frac{a-2b}{2ab} \\ &= \left(\int_0^\tau dt_1 \int_0^{t_1+\tau} dt_2 + \int_\tau^{T-\tau} dt_1 \int_{t_1-\tau}^{t_1+\tau} dt_2 + \int_{T-\tau}^T dt_1 \int_{t_1-\tau}^T dt_2 \right) (e^{-2bt_1} - e^{-at_1}) \\ &= \left(\int_0^\tau dt_1 (t_1 + \tau) + \int_\tau^{T-\tau} dt_1 2\tau + \int_{T-\tau}^T dt_1 (T + \tau - t_1) \right) (e^{-2bt_1} - e^{-at_1}). \end{aligned} \quad (3.128)$$

We calculate these three terms individually. Before doing this, we note that we can use integration by parts to calculate

$$\int_x^y dt e^{-zt} t = -\frac{1}{z} [te^{-zt}]_{t=x}^{t=y} + \frac{1}{z} \int_x^y e^{-zt} dt = \left[\frac{e^{-zt}}{z} \left(t + \frac{1}{z} \right) \right]_{t=x}^{t=y}. \quad (3.129)$$

Then, the first term becomes

$$\begin{aligned} \int_0^\tau dt_1 (t_1 + \tau) (e^{-2bt_1} - e^{-at_1}) &= \left[\left(\tau + \frac{1}{2b} + t_1 \right) \frac{e^{-2bt_1}}{2b} \right]_0^\tau - \left[\left(\tau + \frac{1}{a} + t_1 \right) \frac{e^{-at_1}}{a} \right]_0^\tau \\ &= \frac{1}{4b^2} + \frac{\tau}{2b} - \frac{1}{a^2} - \frac{\tau}{a} - \left(\frac{1}{2b} + 2\tau \right) \frac{e^{-2b\tau}}{2b} + \left(\frac{1}{a} + 2\tau \right) \frac{e^{-a\tau}}{a}. \end{aligned} \quad (3.130)$$

The second yields

$$2\tau \int_\tau^{T-\tau} dt_1 (e^{-2bt_1} - e^{-at_1}) = 2\tau \frac{e^{-2b\tau}}{2b} - 2\tau \frac{e^{2b(\tau-T)}}{2b} - 2\tau \frac{e^{-a\tau}}{a} + 2\tau \frac{e^{a(\tau-T)}}{a}. \quad (3.131)$$

The final one yields

$$\begin{aligned}
 \int_{T-\tau}^T dt_1 (T + \tau - t_1) (e^{-2bt_1} - e^{-at_1}) &= \left[\left(T + \tau - \frac{1}{2b} - t_1 \right) \frac{e^{-2bt_1}}{2b} \right]_T^{T-\tau} \\
 &\quad - \left[\left(T + \tau - \frac{1}{a} - t_1 \right) \frac{e^{-at_1}}{a} \right]_T^{T-\tau} \\
 &= \left[\frac{1}{2b} - \tau + e^{2b\tau} \left(2\tau - \frac{1}{2b} \right) \right] \frac{e^{-2bT}}{2b} \\
 &\quad - \left[\frac{1}{a} - \tau + e^{a\tau} \left(2\tau - \frac{1}{a} \right) \right] \frac{e^{-aT}}{a}.
 \end{aligned} \tag{3.132}$$

We note that the second term cancels fully against the first and the third. When adding all together, we find

$$\begin{aligned}
 p_{\text{ph-dc}}(T, \tau) \frac{p_{\text{det}}(T)T}{\eta} \frac{a-2b}{2ab} &= \frac{1}{2b} \left[\frac{1}{2b} + \tau - \frac{e^{-2b\tau}}{2b} + e^{-2bT} \left(\frac{1}{2b} - \tau - \frac{e^{2b\tau}}{2b} \right) \right] \\
 &\quad - \frac{1}{a} \left[\frac{1}{a} + \tau - \frac{e^{-a\tau}}{a} + e^{-aT} \left(\frac{1}{a} - \tau - \frac{e^{a\tau}}{a} \right) \right]
 \end{aligned} \tag{3.133}$$

and thus

$$\begin{aligned}
 p_{\text{ph-dc}}(T, \tau) \frac{p_{\text{det}}(T)}{\eta} &= \frac{a}{2b(a-2b)T} \left[1 + 2b\tau - e^{-2b\tau} + e^{-2bT} (1 - 2b\tau - e^{2b\tau}) \right] \\
 &\quad - \frac{2b}{a(a-2b)T} \left[1 + a\tau - e^{-a\tau} + e^{-aT} (1 - a\tau - e^{a\tau}) \right].
 \end{aligned} \tag{3.134}$$

This procedure can be repeated when making the assumption $\tau \geq \frac{T}{2}$. In that case, the exact same formula is found. Therefore, equation (3.125) is valid for any $0 \leq \tau \leq T$. \square

Definition 3.12 *Visibility.* When using a detection time window T and coincidence time window of τ in the double-click protocol, the Hong-Ou-Mandel visibility is defined as

$$V(T, \tau) = 1 - \frac{P(\text{two photons detected at different detectors} \mid \text{same mode})}{P(\text{two photons detected at different detectors} \mid \text{different modes})}. \tag{3.135}$$

Here, $P(\text{two photons detected at different detectors} \mid \text{same mode})$ is the probability that if both incoming photons are in the same mode, they will be both be detected, and these detection events occur at different detectors. On the other hand,

$P(\text{two photons detected at different detectors} \mid \text{different modes})$ is the probability that if both incoming photons are in different modes (e.g., different polarizations), they will both be detected, and these detection events occur at different detectors. Dark counts are not considered photon detections for the definitions of these probabilities.

Note that when the two photons are in the same mode, they are able to interfere. Then, if the two photons are pure and have the same temporal profile, they are perfectly indistinguishable and will never be detected at different detectors because of the Hong-Ou-Mandel

effect [75]. On the other hand, if the two photons are in different modes (e.g., different polarizations), they are not able to interfere. We note that the definition here given is in line with the definition given for the Hong-Ou-Mandel visibility in the main text.

Theorem 3.9 *Visibility. The Hong-Ou-Mandel visibility for a double-click protocol with two photons that are both in the double-exponential state (a, b) is given by*

$$\begin{aligned}
 V(T, \tau) \left(\frac{p_{\text{det}}(T)}{\eta} \right)^2 p_{\text{ph-ph}}(T, \tau) = & \frac{a}{a+2b} (1 - e^{-2b\tau}) + \frac{2ab^2}{(a-2b)^2(a-b)} (1 - e^{2(a-b)\tau}) e^{-2aT} \\
 & + \frac{a^2}{(a-2b)^2} (1 - e^{2b\tau}) e^{-4bT} \\
 & - \frac{16ab^2}{(a-2b)^2(a+2b)} (1 - e^{a\tau}) e^{-(a+2b)T}.
 \end{aligned} \tag{3.136}$$

Proof:

First, we evaluate $P(\text{two photons detected at different detectors} \mid \text{different modes})$. Because the photons do not interfere, this probability is just the probability that both photons are detected within the detection time window and within one coincidence time window, multiplied by a factor of $\frac{1}{2}$ as the probability for both photons going to different detectors is the same as the probability for both photons going to the same detector. The probability for a single photon falling within the detection time window is the detection probability (Theorem 3.5), and the probability of both photons being detected within a single coincidence time window is the photon-photon coincidence probability (Theorem 3.6). Thus,

$$P(\text{two photons detected at different detectors} \mid \text{different modes}) = \frac{1}{2} p_{\text{det}}(T)^2 p_{\text{ph-ph}}(T, \tau). \tag{3.137}$$

The second probability can be evaluated as [87]

$$\begin{aligned}
 & P(\text{two photons detected at different detectors} \mid \text{same mode}) \\
 &= \frac{\eta^2}{4} \int_0^\infty dt_1 \int_0^\infty dt_2 \iint_{|t'_1 - t'_2| \leq \tau} dt'_1 dt'_2 p_{\text{em}}(t_1) p_{\text{em}}(t_2) \left| \psi_{t_1}(t'_1) \psi_{t_2}(t'_2) - \psi_{t_1}(t'_2) \psi_{t_2}(t'_1) \right|^2.
 \end{aligned} \tag{3.138}$$

From combining equations (3.103), (3.107) and (3.114), we see that

$$\eta^2 \int_0^\infty dt_1 \int_0^\infty dt_2 \iint_{|t'_1 - t'_2| \leq \tau} p_{\text{em}}(t_1) p_{\text{em}}(t_2) |\psi_{t_1}(t'_1)|^2 |\psi_{t_2}(t'_2)|^2 = p_{\text{det}}(T)^2 p_{\text{ph-ph}}(T, \tau). \tag{3.139}$$

We use this, together with the fact that for double-exponential photons it holds that $\psi_{t_0}^*(t) = \psi_{t_0}(t)$, to find

$$\begin{aligned}
 & P(\text{two photons detected at different detectors} \mid \text{same mode}) = \frac{1}{2} p_{\text{det}}(T)^2 p_{\text{ph-ph}}(T, \tau) \\
 & - \frac{\eta^2}{2} \int_0^\infty dt_1 \int_0^\infty dt_2 \iint_{|t'_1 - t'_2| \leq \tau} dt'_1 dt'_2 p_{\text{em}}(t_1) p_{\text{em}}(t_2) \psi_{t_1}(t'_1) \psi_{t_1}(t'_2) \psi_{t_2}(t'_2) \psi_{t_2}(t'_1).
 \end{aligned} \tag{3.140}$$

We can then work out equation (3.135) to find

$$\begin{aligned}
 & V(T, \tau) \left(\frac{p_{\text{det}}(T)}{\eta} \right)^2 p_{\text{ph-ph}}(T, \tau) \\
 &= \int_0^\infty dt_1 \int_0^\infty dt_2 \int_0^T dt'_1 \int_0^T dt'_2 \Theta(|t'_1 - t'_2| - \tau) p_{\text{em}}(t_1) p_{\text{em}}(t_2) \psi_{t_1}(t'_1) \psi_{t_1}(t'_2) \psi_{t_2}(t'_2) \psi_{t_2}(t'_1).
 \end{aligned} \tag{3.141}$$

The integrand is symmetric under interchange of t'_1 and t'_2 . This allows us to consider only the region $0 \leq t'_2 - t'_1 \leq \tau$, giving

$$\begin{aligned}
 & V(T, \tau) \left(\frac{p_{\text{det}}(T)}{\eta} \right)^2 p_{\text{ph-ph}}(T, \tau) \\
 &= 2 \int_0^\infty dt_1 \int_0^\infty dt_2 \int_0^T dt'_1 \int_{t'_1}^{\min(t'_1 + \tau, T)} dt'_2 p_{\text{em}}(t_1) p_{\text{em}}(t_2) \psi_{t_1}(t'_1) \psi_{t_1}(t'_2) \psi_{t_2}(t'_2) \psi_{t_2}(t'_1).
 \end{aligned} \tag{3.142}$$

Now, we notice that each $\psi_{t_0}(t)$ is proportional to $\Theta(t - t_0)$. This can be absorbed into the limit of integration for t_1 and t_2 , yielding

$$\begin{aligned}
 & V(T, \tau) \left(\frac{p_{\text{det}}(T)}{\eta} \right)^2 p_{\text{ph-ph}}(T, \tau) \\
 &= 2 \int_0^T dt'_1 \int_0^{t'_1} dt_1 \int_0^{t'_1} dt_2 \int_{t'_1}^{\min(t'_1 + \tau, T)} dt'_2 p_{\text{em}}(t_1) p_{\text{em}}(t_2) \psi_{t_1}(t'_1) \psi_{t_1}(t'_2) \psi_{t_2}(t'_2) \psi_{t_2}(t'_1) \\
 &= 8a^2 b^2 \int_0^T dt'_1 e^{-2bt'_1} \int_0^{t'_1} dt_1 e^{-(a-2b)t_1} \int_0^{t'_1} dt_2 e^{-(a-2b)t_2} \int_{t'_1}^{\min(t'_1 + \tau, T)} dt'_2 e^{-2bt'_2} \\
 &= \frac{4a^2 b}{(a-2b)^2} \int_0^T dt'_1 e^{-2bt'_1} (e^{-2bt'_1} - e^{-2b\min(t'_1 + \tau, T)}) (1 - e^{-(a-2b)t'_1})^2 \\
 &= \frac{4a^2 b}{(a-2b)^2} \left[\int_0^T e^{-2bt} - e^{-2b\tau} \int_0^{T-\tau} e^{-2bt} - e^{-2bT} \int_{T-\tau}^T \right] (e^{-2bt} - 2e^{-at} + e^{-2(a-b)t}) dt.
 \end{aligned} \tag{3.143}$$

In the last step, we split up the integration region into a part where $t'_1 + \tau$ is smaller and a part where T is smaller. Furthermore, for brevity, we renamed t'_1 to t . We first calculate the first integral to find

$$\begin{aligned}
 \int_0^T dt (e^{-4bt} - 2e^{-(a+2b)t} + e^{-2at}) &= \frac{1}{4b} (1 - e^{-4bT}) - \frac{2}{a+2b} (1 - e^{-(a+2b)T}) + \frac{1}{2a} (1 - e^{-2aT}) \\
 &= \frac{1}{4b} - \frac{2}{a+2b} + \frac{1}{2a} - \frac{1}{2a} e^{-2aT} - \frac{1}{4b} e^{-4bT} + \frac{2}{a+2b} e^{-(a+2b)T}.
 \end{aligned} \tag{3.144}$$

The second yields

$$\begin{aligned}
 & e^{-2b\tau} \int_0^{T-\tau} dt \left(-e^{-4bt} + 2e^{-(a+2b)t} - e^{-2at} \right) \\
 &= e^{-2b\tau} \left(-\frac{1}{4b}(1 - e^{-4b(T-\tau)}) + \frac{2}{a+2b}(1 - e^{-(a+2b)(T-\tau)}) - \frac{1}{2a}(1 - e^{-2a(T-\tau)}) \right) \quad (3.145) \\
 &= \left(-\frac{1}{4b} + \frac{2}{a+2b} - \frac{1}{2a} \right) e^{-2b\tau} + \frac{e^{2(a-b)\tau}}{2a} e^{-2aT} + \frac{e^{2b\tau}}{4b} e^{-4bT} - \frac{2e^{a\tau}}{a+2b} e^{-(a+2b)T}.
 \end{aligned}$$

The final one yields

$$\begin{aligned}
 & e^{-2bT} \int_{T-\tau}^T dt \left(-e^{-2bt} + 2e^{-at} - e^{-2(a-b)t} \right) \\
 &= -\frac{e^{2b\tau} - 1}{2b} e^{-4bT} + \frac{2(e^{a\tau} - 1)}{a} e^{-(a+2b)T} - \frac{e^{2(a-b)\tau} - 1}{2(a-b)} e^{-2aT}. \quad (3.146)
 \end{aligned}$$

Now, it is just a matter of adding these three terms together and taking the prefactor into account. We collect terms separately for each different exponent with a T . The part of the expression that is independent of T yields

$$\begin{aligned}
 & (1 - e^{-2b\tau}) \frac{4a^2b}{(a-2b)^2} \left(\frac{1}{4b} - \frac{2}{a+2b} + \frac{1}{2a} \right) \\
 &= \frac{a}{(a-2b)^2} \left(a - \frac{8ab}{a+2b} + 2b \right) \quad (3.147) \\
 &= (1 - e^{-2b\tau}) \frac{a}{(a-2b)^2(a+2b)} (a(a+2b) - 8ab + 2b(a+2b)) \\
 &= (1 - e^{-2b\tau}) \frac{a}{a+2b}.
 \end{aligned}$$

For the terms proportional to e^{-2aT} we find

$$\begin{aligned}
 & \frac{4a^2b}{(a-2b)^2} (1 - e^{2(a-b)\tau}) \left(\frac{1}{2a} - \frac{1}{2(a-b)} \right) e^{-2aT} = \frac{2ab}{(a-2b)^2} (1 - e^{2(a-b)\tau}) \left(\frac{a}{a-b} - 1 \right) e^{-2aT} \\
 &= \frac{2ab}{(a-2b)^2} (1 - e^{2(a-b)\tau}) \frac{b}{a-b} e^{-2aT} \\
 &= \frac{2ab^2}{(a-2b)^2(a-b)} (1 - e^{2(a-b)\tau}) \frac{b}{a-b} e^{-2aT}. \quad (3.148)
 \end{aligned}$$

For the terms proportional to e^{-4bT} we find

$$\frac{4a^2b}{(a-2b)^2} (1 - e^{2b\tau}) \left(\frac{1}{4b} - \frac{1}{2b} \right) e^{-4bT} = \frac{a^2}{2(a-2b)^2} (1 - e^{2b\tau}) e^{-4bT}. \quad (3.149)$$

Finally, for the terms proportional to $e^{-(a+2b)T}$ we find

$$\begin{aligned} \frac{4a^2b}{(a-2b)^2}(1-e^{a\tau})\left(\frac{2}{a+2b}-\frac{2}{a}\right)e^{-(a+2b)T} &= \frac{8ab}{(a-2b)^2(a+2b)}(1-e^{a\tau})(a-(a+2b))e^{-(a+2b)T} \\ &= \frac{-16ab^2}{(a-2b)^2(a+2b)}(1-e^{a\tau})e^{-(a+2b)T} \end{aligned} \quad (3.150)$$

Adding these four different contributions together then yields equation (3.136). \square

We note that Lemma 3.8 and Theorems 3.6 and 3.9 are compared to experimental results obtained with a trapped-ion device in Figure 3.10.

3

3.10 Single-click model

In this section, we present an analytical model for the entangled states created on elementary links when using a single-click entanglement generation protocol [67]. This model is used as one of the building blocks of our NetSquid simulations, as mentioned in Section 3.13, and based on the models previously introduced in [47–49]. The novelty of the model presented here lies in combining features of the three previous models [47–49] and in additionally considering the possibility that non-number-resolving detectors may be used (the three cited papers assume the use of number-resolving detectors).

3.10.1 Model assumptions

We model a single-click protocol for entanglement generation on an elementary link between two nodes, which we designate A and B. The protocol starts with the preparation of an optically-active matter qubit at each of the nodes in the following state:

$$|\psi_m\rangle = \sqrt{\alpha}|\uparrow\rangle + \sqrt{1-\alpha}|\downarrow\rangle, \quad (3.151)$$

where the subscript m stands for matter, $|\uparrow\rangle$ is a bright state, i.e., a state that rapidly decays via photon emission after being excited, and α is the bright-state parameter, i.e. the fraction of the matter qubit's state that is in $|\uparrow\rangle$. Excitation and subsequent radiative decay of $|\uparrow\rangle$ entangles the state of the matter qubit with the presence $|1\rangle$ or absence $|0\rangle$ of a photon (subscript p):

$$|\psi_m, \psi_p\rangle = \sqrt{\alpha}|\uparrow\rangle|1\rangle + \sqrt{1-\alpha}|\downarrow\rangle|0\rangle \quad (3.152)$$

The photons are then sent to a heralding station where they are interfered. Detection of a single photon heralds the generation of a matter-matter entangled state.

In our analytical model, we account for the following imperfections when computing the success probability and entangled state generated with the protocol:

- Double excitation of the matter qubit. Resonant laser light incident on the optically-active matter qubit triggers its excitation. It is possible that this excitation happens two times as the laser shines on the matter qubit, leading to the emission of two photons. This happens with probability p_{dex} . We note that the excitation could in theory also happen multiple times, but, as detailed in Section 3.10.2, the effect this would have on the state would be the same as if two photons were emitted, so we can absorb the probability of more than one excitation into one quantity.

- Photon phase uncertainty. The photons interfering at the midpoint acquire a phase during transmission over the fiber, and the difference between the phases of the two interfering photons influences the entangled state that is generated [47]. The dephasing probability of the state p_{phase} can be computed from the standard deviation of the difference between the acquired phases σ_{phase} [48]:

$$p_{\text{phase}} = \frac{1}{2} \left(1 - e^{-\sigma_{\text{phase}}^2/2} \right). \quad (3.153)$$

3

Furthermore, we also account for photon loss, imperfect indistinguishability, non-photon-number-resolving detectors and detector dark counts, as described in 3.8. Finally, we account for the possibility of asymmetry in the placement of the heralding station, the attenuation of the fibers connecting the nodes to the heralding station and the bright-state parameters of the nodes.

3.10.2 Results

Here we present the derivation of the entangled matter-matter state generated in our model of the single-click protocol. We split this derivation into four situations, as done in [47–49]. Each of them corresponds to one of the different configurations of the states of the matter qubits that can result in a heralded success.

1. Both matter qubits are in the bright state. In this case, both matter qubits emit a photon, so this situation is heralded as a success if:

- (a) Only one of the emitted photons survives. For NR detectors, there cannot be dark counts in either of the detectors (as otherwise two photons would be detected in the detector which also saw the actual emitted photon, and the event would be heralded as a failure). For NNR detectors, the requirement is just that there is no dark count in the detector that did not detect the emitted photon. The probability of this case happening is:

$$p_{1a} = \begin{cases} \alpha_A \alpha_B (1 - p_{\text{dc}})^2 (p_A(1 - p_B) + p_B(1 - p_A)) & \text{if NR,} \\ \alpha_A \alpha_B (1 - p_{\text{dc}}) (p_A(1 - p_B) + p_B(1 - p_A)) & \text{if NNR.} \end{cases} \quad (3.154)$$

- (b) No emitted photon is detected, and there is a dark count in one of the detectors. This case is the same irrespective of whether or not the detectors are NR. There is a factor of two because this can happen in either detector. The probability of this case happening is:

$$p_{1b} = 2\alpha_A \alpha_B (1 - p_A)(1 - p_B)(1 - p_{\text{dc}})p_{\text{dc}}. \quad (3.155)$$

- (c) Both emitted photons make it to the midpoint and are detected, but they bunch and go into the same detector. Furthermore, there is no dark count in the other detector. There is a factor of two because this can happen in either detector. This is heralded as a failure if the detectors are NR. The probability of this case happening is:

$$p_{1c} = \begin{cases} 0 & \text{if NR,} \\ \alpha_A \alpha_B p_A p_B p_{\text{same dets}} (1 - p_{\text{dc}}) & \text{if NNR,} \end{cases} \quad (3.156)$$

where $p_{\text{same dets}}$ is the probability that the two photons go to the same detector, as derived in case F2 of Section 3.8:

$$p_{\text{same dets}} = 1 - \frac{1 - V}{2}. \quad (3.157)$$

2. Matter qubit A is in the bright state, matter qubit B is not. In this case, only matter qubit A emits a photon, so this situation is heralded as a success if:

- (a) The emitted photon survives. For NR detectors, there cannot be dark counts in either of the detectors (as otherwise two photons would be detected in the detector which also saw the actual emitted photon, and the event would be heralded as a failure). For NNR detectors, the requirement is just that there is no dark count in the detector that did not detect the emitted photon.

$$p_{2a} = \begin{cases} \alpha_A(1 - \alpha_B)(1 - p_{\text{dc}})^2 p_A & \text{if NR,} \\ \alpha_A(1 - \alpha_B)(1 - p_{\text{dc}}) p_A & \text{if NNR.} \end{cases} \quad (3.158)$$

- (b) The emitted photon does not survive, and there is a dark count in one of the detectors. This case is the same irrespective of whether the detectors are NR. There is a factor of two because this can happen in either detector.

$$p_{2b} = 2\alpha_A(1 - \alpha_B)(1 - p_A)(1 - p_{\text{dc}})p_{\text{dc}}. \quad (3.159)$$

3. Matter qubit B is in the bright state, matter qubit A is not. In this case, only matter qubit B emits a photon. This identical to case 2, interchanging A and B.
4. Neither of the matter qubits are in the bright state. No photon is emitted. In this case, we only get a success if there is a dark count in one of the detectors, but not the other. This case is the same irrespective of whether the detectors are NR. There is a factor of two because this can happen in either detector.

$$p_4 = 2(1 - \alpha_A)(1 - \alpha_B)(1 - p_{\text{dc}})p_{\text{dc}}. \quad (3.160)$$

The overall success probability of the protocol p_{suc} is then given by adding up the probability that each of the cases above happens, $p_{\text{suc}} = p_1 + p_2 + p_3 + p_4$, with $p_1 = p_{1a} + p_{1b} + p_{1c}$, $p_2 = p_{2a} + p_{2b}$ and $p_3 = p_{3a} + p_{3b}$.

The unnormalized density matrix of the generated state ρ can then be obtained by taking the model introduced in [48] and replacing the probabilities appropriately. The result is the following:

$$\rho = \begin{pmatrix} p_1 & 0 & 0 & 0 \\ 0 & p_2 & \pm\sqrt{V}p_2p_3 & 0 \\ 0 & \pm\sqrt{V}p_2p_3 & p_3 & 0 \\ 0 & 0 & 0 & p_4 \end{pmatrix}, \quad (3.161)$$

where the sign depends on which detector clicked.

Two more dephasing channels are then applied in succession to the state in order to account for the effect of double photon excitation and photonic phase drift.

The first channel, corresponding to double excitation, is applied to both matter qubits, with probability $p_{\text{dexc}}/2$. The light pulse used to excite the bright state to a short-lived excited state is not instantaneous, so there is a chance that the matter qubit decays back down to the original state and be re-excited before the pulse is complete. The first emitted photon will be lost to the environment because it is impossible to distinguish it from the laser light used to excite the matter qubit [48]. It must then be traced out, resulting in a loss of coherence between the two matter qubit states. However, detection of the second emitted photon will falsely herald entanglement, so we apply a dephasing channel with probability $p_{\text{dexc}}/2$ to account for the possibility that more than one photon is emitted.

The second one, corresponding to the photonic phase drift, is applied to only one of them, with probability p_{phase} . The difference in the phases acquired by the two interfering photons results in a phase difference between the two components of the resulting Bell state [48]. Applying a dephasing channel to only one of the matter qubits, with the correct probability given by p_{phase} , has the same effect.

3.11 Optimization method

In this section we provide more details regarding our optimization methodology. As mentioned in the main text, this methodology is based on genetic algorithms, which come in several different flavors. Our particular implementation is heavily based on the one introduced in [80], to which we refer the interested reader. The only novelty introduced here is the use of a different termination criterion, which is explained in detail in the following section. We note also that the code for our implementation, together with the tools required for integration with NetSquid simulations, is publicly accessible at [109].

3.11.1 Termination criteria for genetic algorithms

The matter of choosing termination criteria for genetic algorithms (and, more generally, evolutionary algorithms) has been the object of some study (see, e.g., [110] for a review). If the algorithm is terminated too soon, good solutions might remain undiscovered. On the other hand, running the algorithm for too long in case good solutions have already been found leads to wasting computational resources. Typically-used termination criteria can be split into two groups [110]:

1. Direct termination criteria: these can be obtained directly from the optimization, without any extra data analysis. Examples include setting a maximum number of generations for the optimization or imposing a threshold value on the value of the best solution's cost;
2. Derived termination criteria: these are *a posteriori* criteria, requiring that some data analysis be performed on the outcome of the optimization. Examples include setting a threshold on the standard deviation of the costs of the individuals in the population or on the gap between the best and worst individuals in a given generation.

The authors of [110] applied an evolutionary algorithm to a particular cost function with different termination criteria. They found that the only reliable termination criteria fitting

into the groups above were one in which the algorithm terminated after a fixed, predetermined number of generations, which we name GEN, and one in which the best solution had not varied by more than a predetermined value after a predetermined number of generations, which we name VAR. For all the other criteria tested, the algorithm did not terminate even though the optimal solution had already been found. GEN and VAR both have the drawback of depending on hyperparameters for which a good choice can only be made with knowledge of the problem at hand. By this we mean that the number of generations or accepted variation in the best solution per generation that guarantee termination are problem-dependent.

With this in mind, we opted to employ VAR as the termination criterion for our optimization runs. We made this choice as using VAR results in a more systematic, performance-dependent process for the decision of terminating the optimization. By this we mean that even though GEN guarantees termination (by definition) it does so in an arbitrary way by deciding to stop the optimization without any regard for its evolution. As suggested in [110] we terminated the algorithm if the best solution's cost averaged over the past fifteen generations had not varied by more than a given value. In contrast with the work of [110], we measured the variation in percentual terms. For each setup, we ran the optimization process ten times, each for two hundred generations. Then, to determine what the tolerance for the variation should be, we swept across its values, starting at 1% and with a step of 1%. The chosen tolerance was the one that guaranteed termination for all ten of the optimization runs, and the best solution (i.e., the ones showed in this work), was then the best cost found across the ten different runs, up until termination. We note that the tolerance can be different for different setups. We further note that this offline implementation of VAR is not good for saving computational resources, as the optimization must anyway be run for a large number of generations, with some of them being discarded. It was however simpler to integrate into our workflow, which weighed heavily since we were more constrained in working hours than in computing hours.

3.11.2 Cost function

Our goal with this work was to find the minimal requirements for a quantum repeater enabling Verifiable Blind Quantum Computation between two nodes separated by fiber of length 226.5 km. This implies solving a multi-objective optimization problem, as we want to minimize hardware-parameter improvement while simultaneously ensuring that performance targets are met. There are various ways of approaching such problems, one of them being scalarization. This consists of adding the cost functions corresponding to different objectives together, so that effectively only one scalar quantity has to be optimized. Through this process, we arrive at the cost function C introduced in the Methods, which we reproduce in equation (3.162).

$$C = w_1 \left(1 + (F_{min} - F)^2 \right) \Theta(F_{min} - F) + w_2 \left(1 + (R_{min} - R)^2 \right) \Theta(R_{min} - R) + w_3 H_C(x_1, \dots, x_{N_c}) \quad (3.162)$$

We recall that H_C is the hardware cost, w_i are the weights of the objectives, Θ is the Heaviside function and F and R are the average teleportation fidelity and entanglement generation rate achieved by the parameter set, respectively. F_{min} and R_{min} are the minimal performance requirements. Scalarization conveniently transforms multi-objective optimization into their much simpler single-objective counterparts, but it does so by stowing

away the problem in defining the weights w_1 , w_2 and w_3 assigned to each of the objectives. Different choices in the weights can lead to different outcomes from the optimization procedure. In this work, just as in [80], we wanted the performance targets to be hard requirements, i.e. a set of hardware parameters that did not fulfill them should not be assigned a low cost. To ensure this, we picked $w_1, w_2 \gg w_3$, such that $w_1 \left(1 + (F_{\min} - F)^2\right) \Theta(F_{\min} - F)$, $w_2 \left(1 + (R_{\min} - R)^2\right) \Theta(R_{\min} - R) \gg w_3 H_C(x_{1_c}, \dots, x_{N_c})$. We set $w_1 = w_2 = 1 \times 10^{20}$ and $w_3 = 1$. No particular heuristic was used to select these numbers. They were picked because they ensure that the cost assigned to not meeting the performance targets is much higher than the hardware cost, effectively making the performance targets hard requirements.

As mentioned in the main text, we picked the hardware cost function because it reflects the concept of progressive hardness, i.e. that parameters become harder to improve as they approach their perfect value. Furthermore, it satisfies a composability property regarding the probability of no-imperfection. To see this, consider a parameter's probability of no-imperfection p that can be expressed as the product of two other parameters' probabilities of no-imperfection, $p = p_a p_b$. p could for example be the probability that a photon emitted in the correct mode is collected into a fiber, while p_a and p_b are the probabilities that the photon is emitted with the right wavelength and collected into the fiber, respectively. Improving p by a factor of k takes it to $\sqrt[k]{p} = \sqrt[k]{p_a p_b} = \sqrt[k]{p_a} \sqrt[k]{p_b}$, which is equivalent to improving p_a and p_b separately by the same factor k . Therefore, hardware improvement as measured by this function is invariant to the granularity at which parameters are considered.

The last aspect we would like to highlight regarding the cost function is its squared difference terms, i.e. $1 + (F_{\min} - F)^2$ and $1 + (R_{\min} - R)^2$. These were introduced in [111] and are used to steer the algorithm towards sets of hardware parameters that are more likely to meet the performance targets. They do this by ensuring that parameter sets which fail to meet the targets by a large margin are assigned a higher cost, being therefore less likely to progress into further generations.

3.11.3 Probabilities of no-imperfection

For some parameters, such as the probability that a photon is not lost when coupling to a fiber, the conversion to probability of no-imperfection is obvious. For others, such as coherence times, this is not so. Therefore, we show in Table 5.5 the probability of no-imperfection for all parameters considered in our hardware models. We proceed with the derivation of the probability of no-imperfection for some of the less obvious cases.

As mentioned in the main text, and explained in detail in Supplementary Note 4c of [61], the initialization of an color center's electron spin state induces dephasing of its carbon spin states through their hyperfine coupling. This is typically modelled as the carbon spin states dephasing with some probability each time entanglement generation is attempted [34]. This probability can be related to $N_{1/e}$ as $p = 1/2 (1 - e^{-1/N_{1/e}})$. The corresponding probability of no-imperfection is then $p_{ne} = 1 - p = (1 + e^{-1/N_{1/e}})/2$.

T_1 represents the timescale over which qubit relaxation occurs, with the probability of amplitude damping occurring over a period of time t being given by $p_{ad} = 1 - e^{-t/T_1}$. The associated probability of no-imperfection is e^{-t/T_1} . Improving T_1 by a factor of k then corresponds to improving the probability of no-imperfection to $\sqrt[k]{e^{-t/T_1}}$. Some algebra reveals that this is equivalent to multiplying T_1 by a factor of k , and that this holds irrespective

Parameter	Probability of no-imperfection
Photon detection probability excluding attenuation losses p_{det}	p_{det}
Probability of double excitation p_{dexc}	$1 - p_{\text{dexc}}$
Gate depolarizing probability p_{dep}	$1 - p_{\text{dep}}$
Number of entanglement generation attempts before dephasing $N_{1/e}$	$(1 + e^{-1/N_{1/e}})/2$
T_1	e^{-t/T_1}
T_2	e^{-t/T_2}
Ion coherence time T_c	e^{-t/T_c^2}
Emission fidelity F_{em}	$1/3(4F_{\text{em}} - 1)$
Swap quality s_q	s_q
Visibility V	V
Dark count probability p_{dc}	$1 - p_{dc}$

Table 3.6: Probabilities of no-imperfection for parameters we optimized over in this work. Some parameters were merged for brevity, e.g. the probability of no-imperfection presented for T_2 holds for the abstract model T_2 , the carbon spin T_2 and the electron spin T_2 . In the probability of no-imperfection for each of the coherence times, t is the time spent in memory.

of the chosen timescale.

T_2 represents the timescale over which qubit dephasing occurs, with the probability of a Z error occurring over a period of time t being given by $p_z = (1 - e^{-t/T_2})/2$. The associated probability of no-imperfection is $p_{ne} = \frac{1+e^{-t/T_2}}{2}$. To first order, this can be written as $p_{ne} = e^{-t/2T_2}$, and some algebra again reveals that with this approximation improving T_2 by a factor of k is equivalent to multiplying it by the same factor.

The ion coherence time T_c also represents a timescale for dephasing, but in this case the probability of a Z error occurring is given by $1 - \frac{1}{2}(1 + e^{-2t^2/T_c^2})$. To first order, the probability of no-imperfection can thus be written as $p_{ne} = e^{-t^2/T_c^2}$. In this case, improving T_c by a factor of k is equivalent to multiplying it by \sqrt{k} .

We model noise in photon emission as a depolarizing channel of fidelity F_{em} . The action of the depolarizing channel on a perfect Bell state $|\Phi^+\rangle$ can be written as follows:

$$|\Phi^+\rangle\langle\Phi^+| \rightarrow (1 - p_{\text{dep}})|\Phi^+\rangle\langle\Phi^+| + p_{\text{dep}}\frac{\mathbb{I}}{4},$$

where p_{dep} is the associated depolarizing probability and \mathbb{I} is the identity matrix. This can be rewritten as:

$$|\Phi^+\rangle\langle\Phi^+| \rightarrow (1 - p_{\text{dep}})|\Phi^+\rangle\langle\Phi^+| + p_{\text{dep}}\frac{1}{4}(|\Phi^+\rangle\langle\Phi^+| + |\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-|).$$

Since the Bell states are orthogonal to each other, it follows that $p = \frac{4}{3}(1 - F_{\text{em}})$ and that the corresponding probability of no-imperfection is $\frac{1}{3}(4F_{\text{em}} - 1)$.

The derivation of the probability of no-imperfection for the remaining parameters should be self-evident and is therefore omitted here.

3.11.4 Optimizing over tunable parameters

As discussed in the Methods, the entanglement generation and distribution protocols employed in our simulations include parameters that can be freely varied. We name these *tunable* parameters. They affect the behavior and performance of the setups we investigated, and as a consequence also the minimal hardware requirements. The tunable parameters should thus be chosen such that the best possible performance is extracted from a given set of hardware parameters, minimizing the cost function. The values of the tunable parameters that allow for this are the optimal values. This is however not trivial, as different sets of hardware parameters perform best with different tunable parameters. To illustrate this, we again go over the tunable parameters considered in our simulations.

We start with the *cut-off time*. This is the maximum duration for which a state can be held in memory before being discarded. For details on the implementation of a cut-off timer in our simulations, see Section 3.13. If the cut-off time is very short, states will not be held in memory for long, and therefore the end-to-end fidelity will be high. On the other hand, states will also be frequently discarded and regenerated, which means that establishment of end-to-end entanglement will take longer. In contrast, a very long cut-off is equivalent to no cut-off, in the sense that states are never discarded. This maximizes the entanglement generation rate at the expense of lower state fidelity.

The second tunable parameter is the *bright-state parameter*, which is relevant in the single-click entanglement generation protocol. This is the fraction of the superposition that is in the optically-active state, and therefore corresponds to the probability that a photon is emitted. A larger bright-state parameter corresponds to a higher probability of entanglement generation, but at the expense of a lower fidelity, as it also introduces a component orthogonal to the Bell basis in the generated entangled state. For more details on single-click entanglement generation see Section 3.10.

The final tunable parameter is the *coincidence time window*, which is part of our trapped ion double-click entanglement generation model. Two detection events arising from the correct detectors are only heralded as a success if the time elapsed between the events is smaller than the coincidence time window. It acts as a temporal filter, lowering the protocol's success probability but increasing the visibility and hence the fidelity of the generated entangled states. For more details on our modeling of a coincidence time window, see Section 3.9.

These three parameters can be used to trade-off rate against fidelity, and their optimal values are different for different sets of hardware parameters. For example, if the coherence time is short and the detection probability is high, it will likely be beneficial to have a short cut-off time. The opposite is true if the coherence time is long and the detection probability is low.

In order to find good values for the tunable parameters, we included them as parameters to be optimized by the genetic-algorithm-based optimization machinery. We imposed that the values the cut-off time can take are in the interval between $0.1 T_C$ and T_C , where T_C is the coherence time (collective dephasing coherence time for trapped ions, T_2 for abstract nodes and carbon T_2 for NV centers). The expected entanglement generation time grows exponentially as the cut-off time is reduced, so the lower bound was imposed to prevent the simulation taking unreasonably long to run. Furthermore, we anyway expect that a too low cut-off time would not allow the rate target to be met, so we can be reasonably sure that no cheap hardware requirements are missed by imposing this constraint. The up-

per bound is imposed as we observed that not imposing it made it hard for the algorithm to converge, due to the reduced sensitivity of the target metrics to high values of the cut-off time. As discussed above, employing a very long cut-off time is effectively equivalent to not employing one at all. Therefore, in that regime the choice of cut-off time becomes irrelevant, and the set of parameters minimizing the cost function is chosen independently of it. We have empirically observed that the cut-off time tends to converge to around 65% of the relevant coherence time, which is fairly distant from both bounds we imposed. A back-of-the-envelope calculation can also be performed to argue that it is unlikely that allowing for cut-off times which are larger than the memory's coherence time would be useful. We do this by computing the end-to-end fidelity in a single sequential-repeater setup under the following assumptions:

- The cut-off time is equal to the memory dephasing time;
- There are no other noise sources.

The worst case scenario in this setup in terms of fidelity occurs when the second entangled state takes exactly cut-off time seconds to be generated, resulting in both qubits of the first entangled pair to dephase for a time equal to their dephasing time. The dephasing probability is in this case given by $p_Z = \frac{1-e^{-2}}{2}$. Assuming that the state that had been generated was $|\Phi^+\rangle$, the post-dephasing state is a mixture of $|\Phi^+\rangle$ and $|\Phi^-\rangle$:

$$\rho = (1 - p_Z)|\Phi^+\rangle\langle\Phi^+| + p_Z|\Phi^-\rangle\langle\Phi^-|. \quad (3.163)$$

This has a fidelity of 0.57 with the target Bell state $|\Phi^+\rangle$, corresponding to a teleportation fidelity of 0.71. This value is much lower than our lowest teleportation fidelity target, 0.8571, even with no noise sources besides dephasing noise on the memory. It is then unlikely that picking even higher cut-off times would lead to finding better solutions to our optimization problem.

In the single-repeater setup we investigated, there are four bright-state parameters to be chosen, corresponding to the four different fiber segments between processing nodes and heralding stations. We imposed that αp_{det} had to be equal for all of them, with α is the bright-state parameter and p_{det} the probability that a photon is not lost in the fiber connecting the node to the midpoint station. This condition guarantees balanced entanglement-generation success probabilities across all segments, which is a good heuristic for segments connecting to the same heralding station, as it maximizes the fidelity of the generated states [49]. Imposing it also for segments connecting to different heralding stations was done in order to reduce the size of the search space.

There are also two coincidence time window parameters to be chosen, corresponding to the two elementary links. We imposed that they must have the same value in order to make the search space smaller.

3.12 Simulation performance

Each execution of our quantum-network simulations simulates the delivery of n end-to-end entangled states. When the protocols running on the end nodes learn through classical communication between nodes that n states were successfully distributed, they abort and the simulation terminates. In Figure 3.14, we show how the runtime of our simulation of

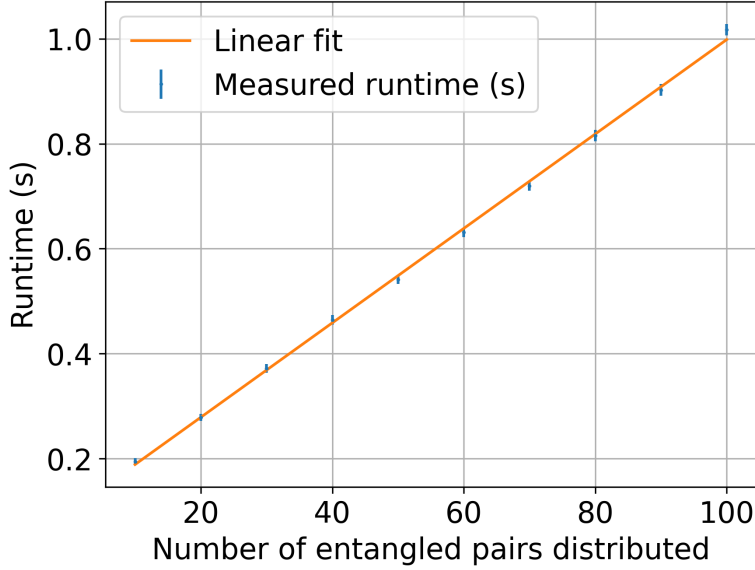


Figure 3.14: Performance of our simulation of the Delft - Eindhoven setup with abstract model nodes and a cut-off timer using a machine running 40 Intel Xeon Gold cores at 2.1 GHz and 192 GB of RAM. The runtime scales linearly with the number of entangled pairs being distributed. Distributing 100 times, which we have empirically determined is enough to evaluate the performance of a given parameter set with reasonable accuracy, takes roughly one second. The data point corresponding to n pairs was obtained by running the corresponding simulation 500 times. The error bars represent the standard error of the mean.

the Delft - Eindhoven setup scales with the number n . As expected, the scaling is linear. A simulation with $n = 100$, which we have empirically determined is enough to evaluate the performance of a given parameter set with reasonable accuracy, takes roughly 1 s. To be more concrete, when running a color-center double-click simulation using the minimal hardware parameters presented in Section 6.2, we find that after distributing 100 pairs a teleportation fidelity F_{tel} of 0.8774 ± 0.0035 and a rate of $0.106 \text{ Hz} \pm 0.003$ are obtained.

We note that Figure 3.14 was obtained by running the simulation without a cut-off. Although the runtime still grows linearly with the number of distributed entangled pairs with a cut-off, its inclusion does mean that the simulation runtime grows exponentially as the the cut-off time becomes shorter. This is because the expected number of necessary entanglement generation attempts also grows exponentially, as seen in Figure 3.15.

As discussed in Section 6.3 and in Section 3.11, the optimization methodology we employ requires running our simulation for many different sets of parameters. We now estimate a lower bound on the time required to perform optimization in one setup. We run the optimization algorithm for 200 iterations. In each of these, there are 200 different parameter sets, and the distribution of 100 entangled pairs is simulated for each. The computing nodes in the high-performance-computing cluster we use have 128 cores, which means that the simulation for 128 of the 200 parameter sets can be executed in parallel. Assuming that there is no cut-off, or that it is large enough not to significantly impact the simulation runtime, this means that we can expect 1 generation to be run in roughly 2.5 seconds. The data processing and file input and output required to generate new sets of

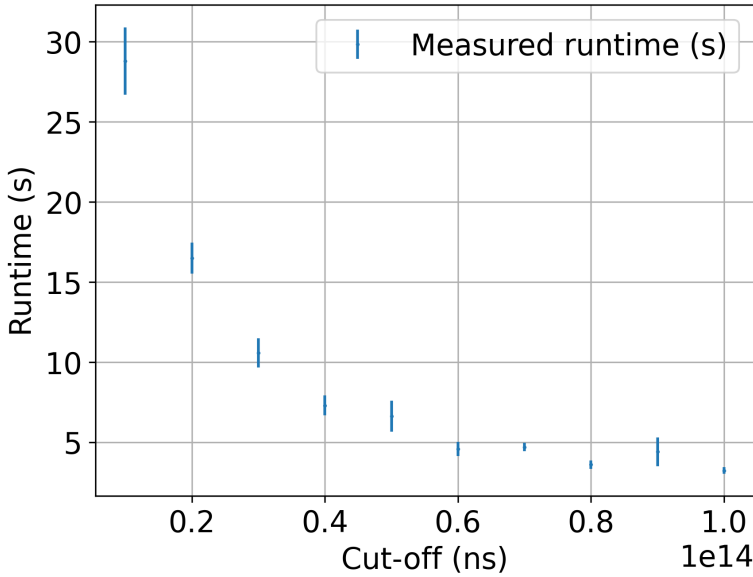


Figure 3.15: Performance of our simulation of the Delft - Eindhoven setup with abstract model nodes and a cut-off timer using a laptop running a quad-core Intel i7-8665U processor at 1.9 GHz and 8 GB of RAM. The runtime scales exponentially as the cut-off time is reduced. The data point corresponding to n pairs was obtained by running the corresponding simulation 20 times. The error bars represent the standard error of the mean.

parameters take a comparable amount of time, making $T = 200 \times 5$ s, roughly seventeen minutes, a good estimate for the time required to perform optimization for one setup. We must however stress that this is a very optimistic lower bound, because as Figure 3.15 makes clear, the use of a cut-off has a huge impact on the runtime of the simulation. We have observed that optimization of most of the setups we studied required 10 to 20 hours to terminate.

3.13 Framework for simulating quantum repeaters

In this section, we discuss the framework that we use to evaluate the performance of quantum repeaters. This framework is presented in this work for the first time.

The code that we have used to simulate all the quantum networks in this chapter is publicly available [106]. The repository contains code that has a much broader applicability than simulating the networks of up to three nodes presented here. In fact, the simulations can be used to assess the performance of quantum-repeater chains with any number of nodes, and any spacing between nodes. The currently supported types of nodes are those containing NV centers, ion traps or abstract quantum processors, and the currently supported types of entanglement generation between neighboring nodes are the single-click and double-click protocols. The simulation code depends on a number of other public repositories [96, 112–116], all of which were developed in tandem with the code for this chapter and will be explained in more detail below.

3.13.1 Services

The primary functional unit of our quantum-network simulations is the “service”, which is defined by an input, an output, and its intended function. An example of a service that can be defined on a node is the measurement service. It takes as input a request to measure a qubit, and the intended function is that the qubit is measured. As output, the service returns the measurement outcome.

A service is distinct from its implementation, which is a protocol. Protocols make sure the intended function is fulfilled and generate the appropriate output. Different protocols can fulfill the same function. For example, in the case of the measurement service, a protocol that simulates a direct measurement of the required qubit (e.g., a fluorescence measurement) could be activated. Another possible implementation would be a protocol that first swaps the quantum state of the required qubit to some different physical qubit (that perhaps allows for higher-fidelity measurements), and then simulates a measurement of that qubit. The distinction between service and its implementation is illustrated in Figure 3.16, which emphasizes that the same high-level functionality can be implemented using different physical systems.

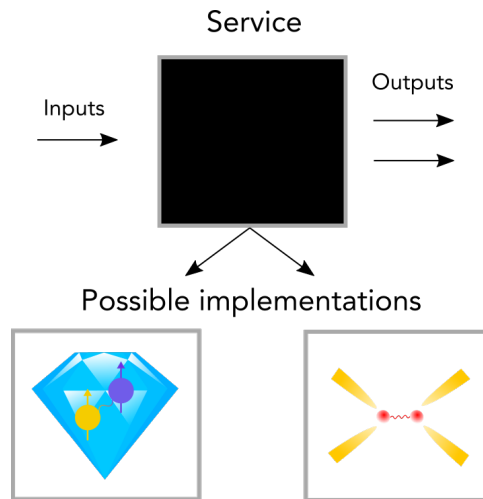


Figure 3.16: The black box represents a service, defined by a set of inputs, a set of outputs and some promised functionality. The protocols interacting with the service need not know how this functionality is implemented. Therefore, different implementations can be swapped in and out. In the figure, color centers and trapped ions are depicted to emphasize that the same high-level functionality can be executed by different physical systems.

Treating services and their implementation separately has two distinct advantages for our simulations. First, it allows us to easily run the same protocols on different types of simulated hardware. Take as example performing an entanglement swap in the broader context of a repeater chain. To do so, the repeater protocol will place a request with the local entanglement-swap service. The repeater protocol does not need to know how the swap is implemented. On an abstract quantum processor, it can be implemented using a CNOT gate, while on an ion trap, it can be implemented using a Mølmer–Sørensen gate. Second, it allows for a modular stack of protocols, where protocols implementing a specific service can easily be interchanged. In the example of the repeater protocol, requests are

made of an entanglement-generation service before the swap can be performed. If the protocol runs on an NV node, entanglement could either be generated using a single-click or double-click protocol. Switching between these two modes is easily realized by changing the protocol that implements the entanglement-generation service. Again, the repeater-node protocol does not need to be adapted.

The main interface of the repeater chain itself is also defined by a service. The service implemented by the repeater chain is a link-layer service [79, 117], which provides robust entanglement generation between the end nodes of the chain. These requests should be put on the end nodes of the chain, which activates a protocol that uses a messaging service to put requests on the SWAP-ASAP repeater services defined on the repeater nodes of the network. When the end-node protocols confirm they share entanglement (using a protocol that tracks entanglement in the network based on the classical communication shared by nodes), an appropriate output message is returned by the service. This is the cue that we use in our simulations to collect the density matrix of the created state and the time it took to create it.

3.13.2 SWAP-ASAP protocol

A SWAP-ASAP repeater chain is one in which repeater nodes perform an entanglement swap as soon as they hold two entangled qubits that were generated with different neighbors. This is in contrast to e.g. nested repeater schemes [118, 119]. We have implemented two different SWAP-ASAP repeater protocols. The first is suitable for repeater chains of any length and node spacing, and for repeater nodes that can generate entanglement with either one or both neighbors at the same time. The second, on the other hand, has been tailored more specifically to the one-repeater scenario studied in this chapter. It assumes that entanglement generation is limited to a single neighbor at a time. First a request is issued to generate entanglement over a single connection. Once that has finished, a request is issued for the second link, and a swap is executed as soon as entanglement is confirmed. In case the connections are not of equal length, entanglement generation takes place on the longer link first. The reason for this is that the longer connection is expected to be the connection on which entanglement generation takes longer. By finishing the longer link first, the total time that entanglement needs to be stored in quantum memory is minimized. The second protocol is the one used to generate the results reported in this chapter.

To generate entanglement over elementary links, the repeater protocols issue requests with the entanglement service. In the protocol that we use to implement this service, these requests are queued. The number of requests that are processed simultaneously is hardware-dependent, and is a free parameter in our simulations. When handling a request for entanglement the protocol will, before doing anything else, issue a request to an agreement service. This service is in charge of synchronizing neighboring nodes that want to generate entanglement together. This is needed as typically both nodes need to be actively involved in generating entanglement for a state to be created between the two. In our simulations, we use an implementation of the agreement service where even-numbered nodes in the chain always initiate entanglement generation. These nodes will send a classical message to their neighbors when a request for agreement is made, and then wait for those nodes to send a classical reply indicating readiness, after which entanglement generation can start. On the other hand, when a request is made on an odd node, it will check whether a classical message has been received by the neighboring even node

in the past. If so, it will reply indicating readiness. Otherwise, the request for agreement will be rejected. In that case, the entanglement service can try to process the next request in the queue, and see if agreement can be reached with this node again at some later time.

In case agreement is reached between two nodes, the entanglement protocols of the nodes will start entanglement generation. In our simulations, this is done using analytical models that decide after how much time an entangled state should be created between the nodes, and what this state should look like. This process is known as *magic* [96] and is further discussed in Section 3.6.8.

3

Finally, there is a cut-off protocol active on repeater nodes. It discards qubits that have been stored in quantum memories for too long. The exact amount of time after which states are discarded is called the cut-off time, and is a tunable parameter that allows for a trade-off between end-to-end entangling rate and fidelity. Every node runs an entanglement-tracking protocol that keeps track of both any local entangled qubits, and what entangled states currently exist in the network at large. Whenever the entanglement service registers a new qubit at the entanglement tracker, the cut-off protocol starts a timer. When the timer goes off, the cut-off protocol checks whether the entangled qubit still exists in local memory. If so, the entanglement tracker is told to discard the qubit. The entanglement tracker will also communicate classically with the entanglement trackers of other nodes in the network to inform them that the qubit has been discarded. If an entanglement tracker learns that a qubit has been discarded that was entangled with one of its local qubits, it responds by discarding that qubit as well. Links corresponding to discarded qubits must be regenerated. We note that the cut-off protocol does not run on the end nodes of the repeater chain. This is to prevent the possibility of one end node believing end-to-end entanglement has been achieved, while the other end node has in actuality discarded its qubit (but the classical message has not yet reached the first end node).

3.13.3 Configuring quantum networks

In our simulations, quantum networks are made up of nodes. Each node represents a single physical location, and contains an object that we refer to as “driver”. This object provides a mapping between services and protocols that implement those services. The driver allows access to services without knowledge of their implementations. Each node has its own driver. Apart from drivers, nodes hold components that represent quantum hardware, which allow for the storage and/or manipulation of quantum states. The protocols running on the node can use this quantum hardware to implement specific services. The nodes in our simulations are ready-made packages with both driver and hardware included. In order to use them in a quantum network, they just need to be initialized (thereby specifying their parameters) and connected to other nodes.

The simulations performed for this chapter contain three different types of nodes. The first is the NV node. It holds an NV quantum processor, which is imported from the Python package NetSquid-NV [113]. The second is the ion-trap node. This node holds an ion-trap quantum processor, imported from the Python package NetSquid-TrappedIons [115]. Finally, there is the abstract node, which contains an abstract quantum processor imported from the Python package NetSquid-AbstractModel [120]. On initialization, each of these takes hardware parameters specific to the type of hardware being simulated, and a number of parameters used to configure the protocols used at the node. For example,

the cut-off time needs to be specified, and in case of single-click heralded entanglement generation, the bright-state parameter as well.

Nodes are connected by two types of connections. These connections are themselves also ready-made packages, and can be found in the Python package NetSquid-PhysLayer [114]. The first type is the classical connection, which represents optical fiber that can be used to send classical messages. The second type is the heralded connection. It represents a midpoint station connected to two nodes by optical fiber, where optical Bell-state measurements can be performed on incoming photons. Such a connection can be used to perform heralded entanglement generation. As discussed above, we do not simulate the process of heralded entanglement generation itself, but instead use analytical models to magically create entangled states. However, the heralded connections still perform an important role as placeholders. Parameters passed to the heralded connection when configuring the network are later retrieved by the analytical models to decide how long it should take before a state is created, and what that state should be exactly. One key parameter specified in the heralded connection is whether single-click or double-click heralded entanglement distribution is used. In the simulations presented in this chapter neighboring nodes are always connected by both a classical connection and a heralded connection.

To put together nodes and connections for the creation of quantum networks, and to configure their parameters, we make use of the Python package NetSquid-NetConf [112]. The tools provided in this package allow for the writing of human-readable configuration files. These configuration files contain entries for all the different nodes and connections in the network. Their type is specified (such as “NV node” or “heralded connection”), as well as their parameters and how they are connected. These configuration files can also be used to vary some of the parameters, allowing to e.g. perform a parameter scan over one of them and observe its effect on the network performance.

3.14 Extra optimization results

In this section, we present results of optimizations we performed that were not presented in the main text, but might still be of interest.

3.14.1 To move or not to move

As mentioned in the main text, the communication qubit of color centers has typically shorter coherence times than the memory qubits. For the baseline hardware parameters we investigated, the communication qubit had $T_1 = 1$ hours [51] and $T_2 = 0.5$ s [50], whereas the memory qubits had $T_1 = 10$ hours and $T_2 = 1$ s [52]. It might then be worthwhile for the end node that generates entanglement with the repeater first, i.e., the Eindhoven node, to move its half of the entangled state to memory while waiting for end-to-end entanglement to be established, even though that comes at the cost of more noise being introduced in this operation. A diagram of the circuit used for this operation can be found in Supplementary Note 5 B of [61]. To investigate this, we applied our methodology to two single-repeater color-center setups performing double-click entanglement generation. In one of the setups, which we name “move scenario”, once the first elementary link is established, the end node performs the move operation while the waiting for the second link to be established. In the other setup, which we name “no-move scenario”, the state is kept in the electron spin until end-to-end entanglement is established. The hardware requirements for these two scenarios are shown in Figure 3.17. The move scenario requires

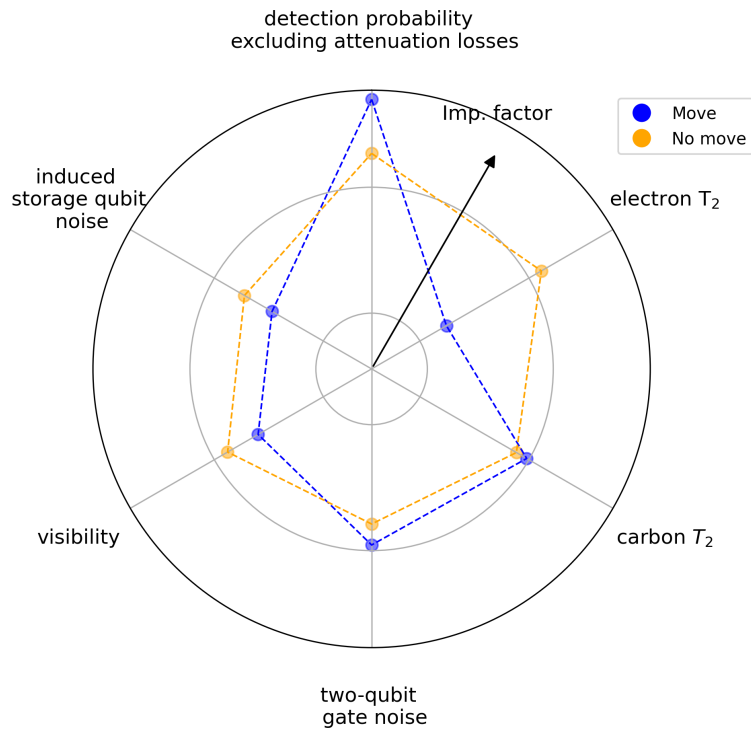


Figure 3.17: Directions along which color-center hardware must be improved to achieve entanglement generation rate $R = 0.1$ Hz and teleportation fidelity $F_T = 0.8717$, enabling VQC between Delft and Eindhoven, assuming that a double-click entanglement generation protocol is used. The blue (orange) line corresponds to the direction of hardware improvement in case the Eindhoven end node (does not) move their half of the entangled state to the memory qubit. Note the use of a logarithmic scale.

that the two-qubit gate be significantly improved, which is to be expected as the move operation requires the application of two of these gates [61]. On the other hand, the move scenario does not require an improvement on the electron spin's coherence time, in contrast with the no-move scenario. This is also not surprising, as in the move scenario entanglement is not stored in the electron spin for a significant amount of time.

The overall cost associated to the no-move scenario is slightly lower than the cost of the move scenario, so all the NV center results presented in the main text were obtained in the no-move scenario. We stress that this finding, although relevant for our particular case study, is not general. It might be that different baselines, different goals or different setups would lead to laxer hardware requirements for the move scenario.

3.14.2 Architecture comparison

As discussed in detail in Section 3.6, the fiber network we study contains four nodes in the shortest path connecting the Dutch cities of Delft and Eindhoven. This means that there is some freedom in how to place the two heralding stations and repeater node required for a single-repeater setup, as shown in Figure 3.7. In order to decide how to make this placement, we determined the minimal hardware requirements for achieving an entanglement generation rate $R = 0.1$ Hz and a teleportation fidelity $F_T = 0.8717$, enabling VBQC between Delft and Eindhoven, for both possibilities. These requirements are shown in Figure 3.18. The requirements are qualitatively similar for both architectures, with the photon detection probability excluding attenuation losses and induced noise on memory qubits (see Section 3.6 for details on our modeling of color-center based repeaters) being the parameters requiring the most improvement. The architecture on the left in Figure 3.7 required more modest improvements overall, so this was the architecture considered in our work.

3.14.3 Connecting Delft and Eindhoven without a repeater

The main contribution of this work was the investigation of the hardware requirements for enabling 2-qubit VBQC between two cities separated by 226.5 km of optical fiber using a single repeater node. We investigated two sets of performance targets compatible with this goal, namely (i) $R = 0.1$ Hz, $F_T = 0.8717$ and (ii) $R = 0.5$ Hz, $F_T = 0.8571$. While (ii) is impossible to achieve via direct transmission, i.e., without a repeater, due to fiber loss, this is not the case for (i) if a single-click entanglement generation protocol is employed. In Figure 3.19 we show directions along which color-center hardware would have to be improved to meet (i) without using a repeater. For comparison, we also reproduce the improvement directions for color-center hardware to meet the same targets with a repeater employing double-click entanglement generation, because this was the repeater setup requiring smallest improvements as measured by our cost function.

The direct transmission setup requires less improvement in all parameters. In fact, the only parameter that requires significant improvement is photon detection probability excluding attenuation losses, although still less than what is required for the repeater setup. The reason for this is that the elementary link state generated with the single-click protocol and state-of-the-art parameters already has high enough fidelity, so the only constraint is that these states are generated fast enough. The required value for the photon detection probability excluding attenuation losses is 0.39, less than the 0.73 required for the repeater with double-click entanglement generation case, but still above the limit imposed by the

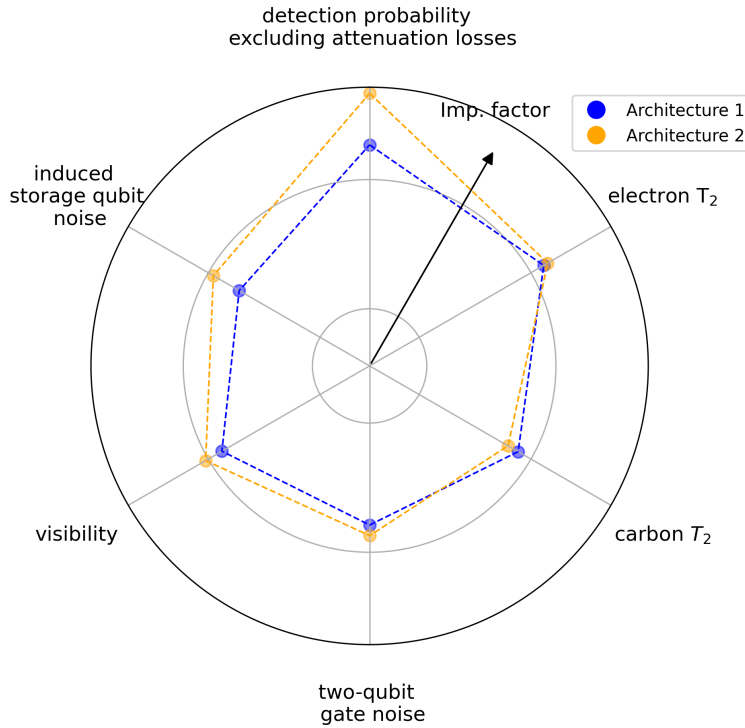


Figure 3.18: Directions along which color-center hardware must be improved to achieve entanglement generation rate $R = 0.1$ Hz and teleportation fidelity $F_T = 0.8717$, enabling VBQC between Delft and Eindhoven, assuming that a double-click entanglement generation protocol is used. The blue (orange) line corresponds to the direction of hardware improvement for the architecture shown on the left (right) in Figure 3.7. Note the use of a logarithmic scale.

zero-phonon line.

These results indicate that performing VBQC over this particular setup might best be done without a repeater, but nevertheless do not detract from the main goal of the chapter, which was to investigate hardware requirements if a repeater were to be used.

3.14.4 Hardware requirements for repeaters with single and double-click entanglement generation

We investigated also how the hardware requirements for color centers running single and double-click entanglement generation protocols differ. We considered a rate target of $R = 0.1$ Hz and an average teleportation fidelity target of $F_T = 0.8717$. These two sets of hardware requirements are presented in Figure 3.20.

The hardware requirements are more stringent for a color-center repeater performing single-click entanglement generation. This is due to the fairly demanding fidelity target, which does not leave much room for noise in a protocol that inherently generates imperfect entangled states. We must however stress that this conclusion is specific to this particular setup and these performance targets, and does not imply that double-click should in

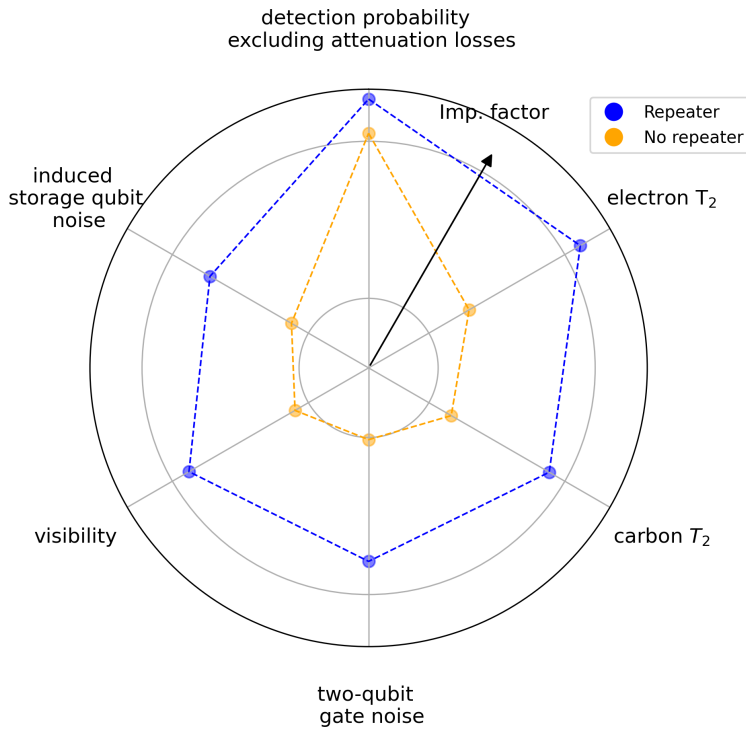


Figure 3.19: Directions along which hardware must be improved to achieve entanglement generation rate $R = 0.1$ Hz and teleportation fidelity $F_T = 0.8717$, enabling VBQC between Delft and Eindhoven. The blue (orange) line corresponds to the direction of hardware improvement for the case in which a repeater is (is not) used. The repeater scenario employs a double-click entanglement generation protocol, whereas in the direct transmission case single-click entanglement generation is employed. Note the use of a logarithmic scale.

general be chosen over single-click. In fact, one need only look at the second set of performance targets we considered in the main text to understand this point. These targets are impossible to achieve using a color-center repeater performing double-click entanglement generation, but are feasible if single-click is employed.

3.14.5 Hardware improvement costs

In Table 3.7 we present the cost of hardware improvement associated with the minimal hardware requirements found for every setup we investigated.

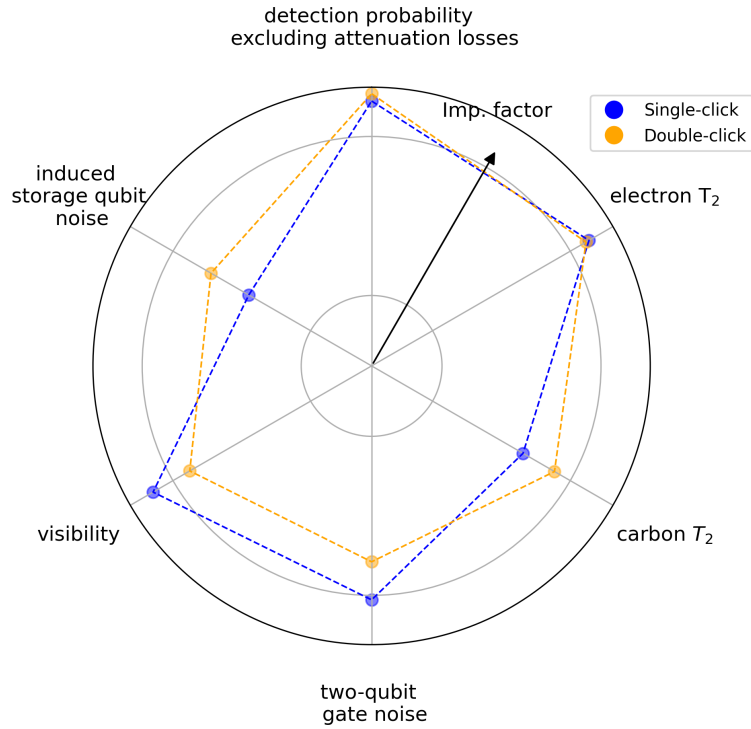


Figure 3.20: Hardware requirements for executing 2-qubit VBQC using a color-center repeater performing double-click (orange) and single-click entanglement generation (blue). These are the requirements for achieving an entanglement generation rate of $R = 0.1$ Hz and an average teleportation fidelity of $F_T = 0.8717$.

Platform	Target	Setup	Protocol	Cost
Color center	R = 0.1 Hz	Standard	Double-click, no-move	26.2
		Fiber network	Single-click, no-move	82.6
			Single-click, move	165.5
			Double-click, no-move	59.8
			Double-click, move	100.1
		Fiber network (repeaterless)	Single-click	20.5
		Alternative fiber network	Double-click, no-move	116.1
	R = 0.5 Hz	Fiber network	Single-click, no-move	153.3
			Single-click, move	227.3
Trapped ions	R = 0.1 Hz	Fiber network	Double-click	171.1
Abstract	R = 0.1 Hz	Fiber network, color center baseline	Double-click	40.7
		Fiber network, trapped ion baseline		50.1
		Fiber network, converted from color center		37.2
		Fiber network, converted from trapped ion		121.0

Table 3.7: Improvement cost, as defined in Section 3.11, of minimal hardware requirements for all setups we investigated.

References

- [1] J. Amirloo, M. Razavi, and A. H. Majedi, *Quantum key distribution over probabilistic quantum repeaters*, Physical Review A **82**, 032304 (2010).
- [2] F. K. Asadi, N. Lauk, S. Wein, N. Sinclair, C. O'Brien, and C. Simon, *Quantum repeaters with individual rare-earth ions at telecommunication wavelengths*, Quantum **2**, 93 (2018).
- [3] N. K. Bernardes, L. Praxmeyer, and P. van Loock, *Rate analysis for a hybrid quantum repeater*, Physical Review A **83**, 012323 (2011).
- [4] J. Borregaard, P. Komar, E. Kessler, A. S. Sørensen, and M. D. Lukin, *Heralded quantum gates with integrated error detection in optical cavities*, Physical Review Letters **114**, 110502 (2015).
- [5] D. E. Bruschi, T. M. Barlow, M. Razavi, and A. Beige, *Repeat-until-success quantum repeaters*, Physical Review A **90**, 032306 (2014).
- [6] Z.-B. Chen, B. Zhao, Y.-A. Chen, J. Schmiedmayer, and J.-W. Pan, *Fault-tolerant quantum repeater with atomic ensembles and linear optics*, Physical Review A **76**, 022329 (2007).

- [7] O. Collins, S. Jenkins, A. Kuzmich, and T. Kennedy, *Multiplexed memory-insensitive quantum repeaters*, Physical review letters **98**, 060502 (2007).
- [8] S. Guha, H. Krovi, C. A. Fuchs, Z. Dutton, J. A. Slater, C. Simon, and W. Tittel, *Rate-loss analysis of an efficient quantum repeater architecture*, Physical Review A **92**, 022357 (2015).
- [9] L. Hartmann, B. Kraus, H.-J. Briegel, and W. Dür, *Role of memory errors in quantum repeaters*, Physical Review A **75**, 032310 (2007).
- [10] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, *Quantum repeater with encoding*, Physical Review A **79**, 032325 (2009).
- [11] K. Nemoto, M. Trupke, S. J. Devitt, B. Scharfenberger, K. Buczak, J. Schmiedmayer, and W. J. Munro, *Photonic quantum networks formed from nv- centers*, Scientific reports **6**, 1 (2016).
- [12] M. Razavi, M. Piani, and N. Lütkenhaus, *Quantum repeaters with imperfect memories: Cost and scalability*, Physical Review A **80**, 032301 (2009).
- [13] M. Razavi and J. H. Shapiro, *Long-distance quantum communication with neutral atoms*, Physical Review A **73**, 042303 (2006).
- [14] C. Simon, H. De Riedmatten, M. Afzelius, N. Sangouard, H. Zbinden, and N. Gisin, *Quantum repeaters with photon pair sources and multimode memories*, Physical review letters **98**, 190503 (2007).
- [15] S. E. Vinay and P. Kok, *Practical repeaters for ultralong-distance quantum communication*, Physical Review A **95**, 052336 (2017).
- [16] Y. Wu, J. Liu, and C. Simon, *Near-term performance of quantum repeaters with imperfect ensemble-based quantum memories*, Physical Review A **101**, 042301 (2020).
- [17] N. Sangouard, C. Simon, J. Minář, H. Zbinden, H. De Riedmatten, and N. Gisin, *Long-distance entanglement distribution with single-photon sources*, Physical Review A **76**, 050301 (2007).
- [18] N. Sangouard, C. Simon, B. Zhao, Y.-A. Chen, H. De Riedmatten, J.-W. Pan, and N. Gisin, *Robust and efficient quantum repeaters with atomic ensembles and linear optics*, Physical Review A **77**, 062301 (2008).
- [19] J. Borregaard, H. Pichler, T. Schröder, M. D. Lukin, P. Lodahl, and A. S. Sørensen, *One-way quantum repeater based on near-deterministic photon-emitter interfaces*, Physical Review X **10**, 021071 (2020).
- [20] D. Luong, L. Jiang, J. Kim, and N. Lütkenhaus, *Overcoming lossy channel bounds using a single quantum repeater node*, Applied Physics B **122**, 1 (2016).
- [21] F. Rozpędek, K. Goodenough, J. Ribeiro, N. Kalb, V. C. Vivoli, A. Reiserer, R. Hanson, S. Wehner, and D. Elkouss, *Parameter regimes for a single sequential quantum repeater*, Quantum Science and Technology **3**, 034002 (2018).

- [22] F. Rozpędek, R. Yehia, K. Goodenough, M. Ruf, P. C. Humphreys, R. Hanson, S. Wehner, and D. Elkouss, *Near-term quantum-repeater experiments with nitrogen-vacancy centers: Overcoming the limitations of direct transmission*, Physical Review A **99**, 052330 (2019).
- [23] P. van Loock, W. Alt, C. Becher, O. Benson, H. Boche, C. Deppe, J. Eschner, S. Höfling, D. Meschede, P. Michler, F. Schmidt, and H. Weinfurter, *Extending Quantum Links: Modules for Fiber- and Memory-Based Quantum Repeaters*, Advanced Quantum Technologies **3**, 1900141 (2020).
- [24] L. Kamin, E. Shchukin, F. Schmidt, and P. van Loock, *Exact rate analysis for quantum repeaters with imperfect memories and entanglement swapping as soon as possible*, (2022), arXiv:2203.10318 .
- [25] S. Abruzzo, S. Bratzik, N. K. Bernardes, H. Kampermann, P. Van Loock, and D. Bruß, *Quantum repeaters and quantum key distribution: Analysis of secret-key rates*, Physical Review A **87**, 052315 (2013).
- [26] J. B. Brask and A. S. Sørensen, *Memory imperfections in atomic-ensemble-based quantum repeaters*, Physical Review A **78**, 012350 (2008).
- [27] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, *Ultrafast and fault-tolerant quantum communication across long distances*, Physical review letters **112**, 250501 (2014).
- [28] M. Pant, H. Krovi, D. Englund, and S. Guha, *Rate-distance tradeoff and resource costs for all-optical quantum repeaters*, Physical Review A **95**, 012304 (2017).
- [29] T. D. Ladd, P. van Loock, K. Nemoto, W. J. Munro, and Y. Yamamoto, *Hybrid quantum repeater based on dispersive cqed interactions between matter qubits and bright coherent light*, New Journal of Physics **8**, 184 (2006).
- [30] P. Van Loock, T. Ladd, K. Sanaka, F. Yamaguchi, K. Nemoto, W. Munro, and Y. Yamamoto, *Hybrid quantum repeater using bright coherent light*, Physical review letters **96**, 240501 (2006).
- [31] M. Zwerger, B. Lanyon, T. Northup, C. Muschik, W. Dür, and N. Sangouard, *Quantum repeaters based on trapped ions with decoherence-free subspace encoding*, Quantum Science and Technology **2**, 044001 (2017).
- [32] L. Jiang, J. Taylor, and M. Lukin, *Fast and robust approach to long-distance quantum communication with atomic ensembles*, Physical Review A **76**, 012301 (2007).
- [33] X. Wu, A. Kolar, J. Chung, D. Jin, T. Zhong, R. Kettimuthu, and M. Suchara, *SeQUeNCe: A customizable discrete-event simulator of quantum networks*, Quantum Science and Technology **6**, 045027 (2021).
- [34] N. Kalb, P. C. Humphreys, J. Slim, and R. Hanson, *Dephasing mechanisms of diamond-based nuclear-spin memories for quantum networks*, Physical Review A **97**, 062330 (2018).

- [35] F. F. da Silva, G. Avis, J. A. Slater, and S. Wehner, *Requirements for upgrading trusted nodes to a repeater chain over 900 km of optical fiber*, (2023), arXiv:2303.03234 .
- [36] D. Leichtle, L. Music, E. Kashefi, and H. Ollivier, *Verifying bqp computations on noisy devices with minimal overhead*, PRX Quantum **2**, 040302 (2021).
- [37] J. F. Fitzsimons and E. Kashefi, *Unconditionally verifiable blind quantum computation*, Physical Review A **96**, 012303 (2017).
- [38] T. Morimae and K. Fujii, *Blind topological measurement-based quantum computation*, Nature communications **3**, 1036 (2012).
- [39] H.-L. Huang, Q. Zhao, X. Ma, C. Liu, Z.-E. Su, X.-L. Wang, L. Li, N.-L. Liu, B. C. Sanders, C.-Y. Lu, *et al.*, *Experimental blind quantum computing for a classical client*, Physical review letters **119**, 050503 (2017).
- [40] A. Gheorghiu, E. Kashefi, and P. Wallden, *Robustness and device independence of verifiable blind quantum computing*, New Journal of Physics **17**, 083040 (2015).
- [41] V. Dunjko, E. Kashefi, and A. Leverrier, *Blind quantum computing with weak coherent pulses*, Physical review letters **108**, 200502 (2012).
- [42] A. Broadbent, J. Fitzsimons, and E. Kashefi, *Universal blind quantum computation*, in *2009 50th Annual IEEE Symposium on Foundations of Computer Science (IEEE, 2009)* pp. 517–526.
- [43] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, *Demonstration of blind quantum computing*, science **335**, 303 (2012).
- [44] C. H. Bennett, D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, and W. K. Wootters, *Remote state preparation*, Physical Review Letters **87**, 077902 (2001).
- [45] H. Bernien, B. Hensen, W. Pfaff, G. Koolstra, M. S. Blok, L. Robledo, T. H. Taminiau, M. Markham, D. J. Twitchen, L. Childress, *et al.*, *Heralded entanglement between solid-state qubits separated by three metres*, Nature **497**, 86 (2013).
- [46] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenbergh, R. F. Vermeulen, R. N. Schouten, C. Abellán, *et al.*, *Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres*, Nature **526**, 682 (2015).
- [47] N. Kalb, A. A. Reiserer, P. C. Humphreys, J. J. Bakermans, S. J. Kamerling, N. H. Nickerson, S. C. Benjamin, D. J. Twitchen, M. Markham, and R. Hanson, *Entanglement distillation between solid-state quantum network nodes*, Science **356**, 928 (2017).
- [48] P. C. Humphreys, N. Kalb, J. P. Morits, R. N. Schouten, R. F. Vermeulen, D. J. Twitchen, M. Markham, and R. Hanson, *Deterministic delivery of remote entanglement on a quantum network*, Nature **558**, 268 (2018).
- [49] M. Pompili, S. L. Hermans, S. Baier, H. K. Beukers, P. C. Humphreys, R. N. Schouten, R. F. Vermeulen, M. J. Tiggeleman, L. dos Santos Martins, B. Dirkse, *et al.*, *Realization of a multinode quantum network of remote solid-state qubits*, Science **372**, 259 (2021).

- [50] S. Hermans, M. Pompili, H. Beukers, S. Baier, J. Borregaard, and R. Hanson, *Qubit teleportation between non-neighbouring nodes in a quantum network*, *Nature* **605**, 663 (2022).
- [51] M. H. Abobeih, J. Cramer, M. A. Bakker, N. Kalb, M. Markham, D. J. Twitchen, and T. H. Taminiau, *One-second coherence for a single electron spin coupled to a multi-qubit nuclear-spin environment*, *Nature communications* **9**, 1 (2018).
- [52] C. Bradley, J. Randall, M. Abobeih, R. Berrevoets, M. Degen, M. Bakker, M. Markham, D. Twitchen, and T. Taminiau, *A ten-qubit solid-state spin register with quantum memory up to one minute*, *Physical Review X* **9**, 031045 (2019).
- [53] V. Krutyanskiy, M. Canteri, M. Meraner, J. Bate, V. Krcmarsky, J. Schupp, N. Sangouard, and B. P. Lanyon, *A telecom-wavelength quantum repeater node based on a trapped-ion processor*, (2022), arXiv:2210.05418 .
- [54] V. Krutyanskiy, M. Galli, V. Krcmarsky, S. Baier, D. A. Fioretto, Y. Pu, A. Mazloom, P. Sekatski, M. Canteri, M. Teller, J. Schupp, J. Bate, M. Meraner, N. Sangouard, B. P. Lanyon, and T. E. Northup, *Entanglement of trapped-ion qubits separated by 230 meters*, *Physical Review Letters* **130**, 050803 (2023).
- [55] V. Krutyanskiy, M. Meraner, J. Schupp, V. Krcmarsky, H. Hainzer, and B. Lanyon, *Light-matter entanglement over 50 km of optical fibre*, *npj Quantum Information* **5**, 1 (2019).
- [56] J. Schupp, V. Krcmarsky, V. Krutyanskiy, M. Meraner, T. Northup, and B. Lanyon, *Interface between Trapped-Ion Qubits and Traveling Photons with Close-to-Optimal Efficiency*, *PRX Quantum* **2**, 020331 (2021), publisher: American Physical Society.
- [57] V. Krutyanskiy, M. Meraner, J. Schupp, and B. P. Lanyon, *Polarisation-preserving photon frequency conversion from a trapped-ion-compatible wavelength to the telecom C-band*, *Applied Physics B* **123**, 228 (2017).
- [58] A. H. Myerson, D. J. Szwer, S. C. Webster, D. T. C. Allcock, M. J. Curtis, G. Imreh, J. A. Sherman, D. N. Stacey, A. M. Steane, and D. M. Lucas, *High-Fidelity Readout of Trapped-Ion Qubits*, *Physical Review Letters* **100**, 200502 (2008).
- [59] C. F. Roos, M. Chwalla, K. Kim, M. Riebe, and R. Blatt, *‘Designer atoms’ for quantum metrology*, *Nature* **443**, 316 (2006).
- [60] S. Baier, M. Galli, V. Krutyanskii, B. Lanyon, and T. Northup, private communications (2022).
- [61] T. Coopmans, R. Knegjens, A. Dahlberg, D. Maier, L. Nijsten, J. de Oliveira Filho, M. Papendrecht, J. Rabbie, F. Rozpędek, M. Skrzypczyk, *et al.*, *Netsquid, a network simulator for quantum information using discrete events*, *Communications Physics* **4**, 1 (2021).
- [62] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Quantum repeaters: the role of imperfect local operations in quantum communication*, *Physical Review Letters* **81**, 5932 (1998).

- [63] M. Ruf, N. H. Wan, H. Choi, D. Englund, and R. Hanson, *Quantum networks based on color centers in diamond*, Journal of Applied Physics **130**, 070901 (2021).
- [64] M. Ruf, M. J. Weaver, S. B. van Dam, and R. Hanson, *Resonant excitation and purcell enhancement of coherent nitrogen-vacancy centers coupled to a fabry-perot microcavity*, Physical Review Applied **15**, 024049 (2021).
- [65] P. Schindler, D. Nigg, T. Monz, J. T. Barreiro, E. Martinez, S. X. Wang, S. Quint, M. F. Brandl, V. Nebendahl, C. F. Roos, M. Chwalla, M. Hennrich, and R. Blatt, *A quantum information processor with trapped ions*, New Journal of Physics **15**, 123012 (2013).
- [66] K. Mølmer and A. Sørensen, *Multiparticle entanglement of hot trapped ions*, Physical Review Letters **82**, 1835 (1999).
- [67] C. Cabillo, J. I. Cirac, P. Garcia-Fernandez, and P. Zoller, *Creation of entangled states of distant atoms by interference*, Physical Review A **59**, 1025 (1999).
- [68] S. D. Barrett and P. Kok, *Efficient high-fidelity quantum computation using matter qubits and linear optics*, Physical Review A **71**, 060310 (2005).
- [69] G. Vardoyan, M. Skrzypczyk, and S. Wehner, *On the quantum performance evaluation of two distributed quantum architectures*, Performance Evaluation **153**, 102242 (2022).
- [70] M. Horodecki, P. Horodecki, and R. Horodecki, *General teleportation channel, singlet fraction, and quasidistillation*, Physical Review A **60**, 1888 (1999), publisher: American Physical Society.
- [71] L. Jiang, J. M. Taylor, N. Khaneja, and M. D. Lukin, *Optimal approach to quantum communication using dynamic programming*, Proceedings of the National Academy of Sciences **104**, 17291 (2007).
- [72] T. Coopmans, S. Brand, and D. Elkouss, *Improved analytical bounds on delivery times of long-distance entanglement*, Physical Review A **105**, 012608 (2022).
- [73] N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin, *Quantum repeaters based on atomic ensembles and linear optics*, Reviews of Modern Physics **83**, 33 (2011).
- [74] W. Dür and H. J. Briegel, *Entanglement purification and quantum error correction*, Reports on Progress in Physics **70**, 1381 (2007).
- [75] C. K. Hong, Z. Y. Ou, and L. Mandel, *Measurement of subpicosecond time intervals between two photons by interference*, Physical Review Letters **59**, 2044 (1987), publisher: American Physical Society.
- [76] F. Bouchard, A. Sit, Y. Zhang, R. Fickler, F. M. Miatto, Y. Yao, F. Sciarrino, and E. Karimi, *Two-photon interference: The Hong–Ou–Mandel effect*, Reports on Progress in Physics **84**, 012402 (2020).
- [77] W. Pfaff, B. J. Hensen, H. Bernien, S. B. van Dam, M. S. Blok, T. H. Taminiau, M. J. Tiggelman, R. N. Schouten, M. Markham, D. J. Twitchen, et al., *Unconditional quantum teleportation between distant solid-state quantum bits*, Science **345**, 532 (2014).

- [78] A. Stute, B. Casabone, P. Schindler, T. Monz, P. O. Schmidt, B. Brandstätter, T. E. Northup, and R. Blatt, *Tunable ion–photon entanglement in an optical cavity*, *Nature* **485**, 482 (2012).
- [79] A. Dahlberg, M. Skrzypczyk, T. Coopmans, L. Wubben, F. Rozpędek, M. Pompili, A. Stolk, P. Pawełczak, R. Knegjens, J. de Oliveira Filho, R. Hanson, and S. Wehner, *A link layer protocol for quantum networks*, in *Proceedings of the ACM Special Interest Group on Data Communication, SIGCOMM '19* (Association for Computing Machinery, New York, NY, USA, 2019) pp. 159–173.
- [80] F. F. da Silva, A. Torres-Knoop, T. Coopmans, D. Maier, and S. Wehner, *Optimizing entanglement generation and distribution using genetic algorithms*, *Quantum Science and Technology* (2021).
- [81] J. Cramer, N. Kalb, M. A. Rol, B. Hensen, M. S. Blok, M. Markham, D. J. Twitchen, R. Hanson, and T. H. Taminiau, *Repeated quantum error correction on a continuously encoded qubit by real-time feedback*, *Nature communications* **7**, 1 (2016).
- [82] T. H. Taminiau, J. Cramer, T. van der Sar, V. V. Dobrovitski, and R. Hanson, *Universal control and error correction in multi-qubit spin registers in diamond*, *Nature nanotechnology* **9**, 171 (2014).
- [83] A. Reiserer, N. Kalb, M. S. Blok, K. J. van Bemmelen, T. H. Taminiau, R. Hanson, D. J. Twitchen, and M. Markham, *Robust quantum-network memory using decoherence-protected subspaces of nuclear spins*, *Physical Review X* **6**, 021040 (2016).
- [84] H. G. Barros, A. Stute, T. E. Northup, C. Russo, P. O. Schmidt, and R. Blatt, *Deterministic single-photon source from a single ion*, *New Journal of Physics* **11**, 103004 (2009).
- [85] B. Casabone, A. Stute, K. Friebe, B. Brandstätter, K. Schüppert, R. Blatt, and T. E. Northup, *Heralded Entanglement of Two Ions in an Optical Cavity*, *Physical Review Letters* **111**, 100505 (2013).
- [86] M. Keller, B. Lange, K. Hayasaka, W. Lange, and H. Walther, *Continuous generation of single photons with controlled waveform in an ion-trap cavity system*, *Nature* **431**, 1075 (2004).
- [87] M. Meraner, A. Mazloom, V. Krutyanskiy, V. Krcmarsky, J. Schupp, D. Fioretto, P. Sekatski, T. E. Northup, N. Sangouard, and B. P. Lanyon, *Indistinguishable photons from a trapped-ion quantum network node*, *Physical Review A* **102**, 052614 (2020).
- [88] A. Stute, B. Casabone, B. Brandstätter, D. Habicher, H. G. Barros, P. O. Schmidt, T. E. Northup, and R. Blatt, *Toward an ion–photon quantum interface in an optical cavity*, *Applied Physics B* **107**, 1145 (2012).
- [89] T. Walker, S. V. Kashanian, T. Ward, and M. Keller, *Improving the indistinguishability of single photons from an ion-cavity system*, *Physical Review A* **102**, 032616 (2020).

- [90] T. Walker, K. Miyanishi, R. Ikuta, H. Takahashi, S. Vartabi Kashanian, Y. Tsujimoto, K. Hayasaka, T. Yamamoto, N. Imoto, and M. Keller, *Long-Distance Single Photon Transmission from a Trapped Ion via Quantum Frequency Conversion*, Physical Review Letters **120**, 203601 (2018).
- [91] L. J. Stephenson, D. P. Nadlinger, B. C. Nichol, S. An, P. Drmota, T. G. Ballance, K. Thirumalai, J. F. Goodwin, D. M. Lucas, and C. J. Ballance, *High-Rate, High-Fidelity Entanglement of Qubits Across an Elementary Quantum Network*, Physical Review Letters **124**, 110501 (2020).
- [92] T. van Leent, M. Bock, F. Fertig, R. Garthoff, S. Eppelt, Y. Zhou, P. Malik, M. Seubert, T. Bauer, W. Rosenfeld, W. Zhang, C. Becher, and H. Weinfurter, *Entangling single atoms over 33 km telecom fibre*, Nature **607**, 69 (2022).
- [93] C. Crocker, M. Lichtman, K. Sosnova, A. Carter, S. Scarano, and C. Monroe, *High purity single photons entangled with an atomic qubit*, Optics Express **27**, 28143 (2019).
- [94] I. V. Inlek, C. Crocker, M. Lichtman, K. Sosnova, and C. Monroe, *Multispecies Trapped-Ion Node for Quantum Networking*, Physical Review Letters **118**, 250502 (2017).
- [95] D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, E. Y.-Z. Tan, P. Sekatski, R. L. Urbanke, R. Renner, N. Sangouard, and J.-D. Bancal, *Device-Independent Quantum Key Distribution*, Nature **607**, 682 (2022).
- [96] NetSquid-Magic, <https://gitlab.com/softwarequtech/netsquid-snippets/netsquid-magic> (2022).
- [97] J. Watrous, *The Theory of Quantum Information*, 1st ed. (Cambridge University Press).
- [98] C. H. Bennett, D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, and W. K. Wootters, *Remote state preparation*, Phys. Rev. Lett. **87**, 077902 (2001).
- [99] J. L. W. V. Jensen, *Sur les fonctions convexes et les inégalités entre les valeurs Moyennes*, (1906).
- [100] M. D. Bowdrey, D. K. L. Oi, A. Short, K. Banaszek, and J. Jones, *Fidelity of single qubit maps*, Physics Letters A **294**, 258 (2002).
- [101] S. O. Hansson, *Do we need second-order probabilities?* Dialectica **62**, 525 (2008).
- [102] V. Bužek, M. Hillery, and R. F. Werner, *Optimal manipulations with qubits: Universal-NOT gate*, Physical Review A **60**, R2626 (1999).
- [103] A. Klappenecker and M. Rotteler, *Mutually unbiased bases are complex projective 2-designs*, in *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005.* (2005) pp. 1740–1744.
- [104] S. D. Barrett and P. Kok, *Efficient high-fidelity quantum computation using matter qubits and linear optics*, **71**, 060310, publisher: American Physical Society.

- [105] A. Meurer, C. P. Smith, M. Paprocki, O. Čertík, S. B. Kirpichev, M. Rocklin, A. Kumar, S. Ivanov, J. K. Moore, S. Singh, T. Rathnayake, S. Vig, B. E. Granger, R. P. Muller, F. Bonazzi, H. Gupta, S. Vats, F. Johansson, F. Pedregosa, M. J. Curry, A. R. Terrel, v. Roučka, A. Saboo, I. Fernando, S. Kulal, R. Cimrman, and A. Scopatz, *Sympy: symbolic computing in python*, *PeerJ Computer Science* **3**, e103 (2017).
- [106] G. Avis, F. Ferreira da Silva, T. Coopmans, A. Dahlberg, H. Jirovská, D. Maier, and J. Rabbie, *Simulation code for Requirements for a processing-node quantum repeater on a real-world fiber grid* · *GitLab*, <https://gitlab.com/softwarequtech/simulation-code-for-requirements-for-a-processing-node-quantum-repeater-on-a-real-world-fiber-grid>.
- [107] B. Kambs and C. Becher, *Limitations on the indistinguishability of photons from remote solid state sources*, **20**, 115003.
- [108] D. A. Fioretto, *Towards a flexible source for indistinguishable photons based on trapped ions and cavities*, .
- [109] *Smart-Stopos*, <https://gitlab.com/aritoka/smart-stopos>.
- [110] B. J. Jain, H. Pohlheim, and J. Wegener, *On termination criteria of evolutionary algorithms*, in *Proceedings of the 3rd Annual Conference on Genetic and Evolutionary Computation* (2001) pp. 768–768.
- [111] A. Labay Mora, *Genetic algorithm-based optimisation of entanglement distribution to minimise hardware cost*, (2021).
- [112] *NetSquid-NetConf*, <https://gitlab.com/softwarequtech/netsquid-snippets/netsquid-netconf> (2022).
- [113] *NetSquid-NV*, <https://gitlab.com/softwarequtech/netsquid-snippets/netsquid-nv> (2022).
- [114] *NetSquid-PhysLayer*, <https://gitlab.com/softwarequtech/netsquid-snippets/netsquid-physlayer> (2022).
- [115] *NetSquid-TrappedIons*, <https://gitlab.com/softwarequtech/netsquid-snippets/netsquid-trappedions> (2022).
- [116] *NetSquid-SimulationTools*, <https://gitlab.com/softwarequtech/netsquid-snippets/netsquid-simulationtools> (2022).
- [117] M. Pompili, C. Delle Donne, I. te Raa, B. van der Vecht, M. Skrzypczyk, G. Ferreira, L. de Kluijver, A. J. Stolk, S. L. N. Hermans, P. Pawełczak, W. Kozłowski, R. Hanson, and S. Wehner, *Experimental demonstration of entanglement delivery using a quantum network stack*, *npj Quantum Information* **8**, 1 (2022).
- [118] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication*, *Physical Review Letters* **81**, 5932 (1998).

- [119] L.-M. Duan, M. Lukin, I. Cirac, and P. Zoller, *Long-distance quantum communication with atomic ensembles and linear optics*, *Nature* **414**, 413 (2001).
- [120] *NetSquid-AbstractModel*, <https://gitlab.com/softwarequtech/netsquid-snippets/netsquid-abstractmodel> (2022).

4

Asymmetric node placement in fiber-based quantum networks

4

Guus Avis, Robert Knegjens, Anders S. Sørensen and Stephanie Wehner.

Restrictions imposed by existing infrastructure can make it hard to ensure an even spacing between the nodes of future fiber-based quantum networks. We here investigate the negative effects of asymmetric node placement by considering separately the placement of midpoint stations required for heralded entanglement generation, as well as of processing-node quantum repeaters in a chain. For midpoint stations, we describe the effect asymmetry has on the time required to perform one entangling attempt, the success probability of such attempts, and the fidelity of the entangled states created. This includes accounting for the effects of chromatic dispersion on photon indistinguishability. For quantum-repeater chains we numerically investigate how uneven spacing between repeater nodes leads to bottlenecks, thereby increasing both the waiting time and the time states are stored in noisy quantum memory. We find that while the time required to perform one entangling attempt may increase linearly with the midpoint's asymmetry, the success probability and fidelity of heralded entanglement generation and the distribution time and error rate for repeater chains all have vanishing first derivatives with respect to the amount of asymmetry. This suggests resilience of quantum-network performance against small amounts of asymmetry.

In order to build a quantum network, decisions need to be made on where its nodes are positioned and how they are connected. These nodes include the end nodes of the network, quantum repeaters and potentially midpoint stations as required by heralded entanglement generation (as depicted in Figure 4.1) [1, 2]. For the midpoint stations, and for quantum repeaters running at least some specific types of protocols (such as the one investigated in this chapter), optimal network performance requires the nodes to be positioned *symmetrically*. That is, with an internode spacing that is the same between all neighboring nodes. To understand why symmetric placement of repeater nodes can be favourable to

This chapter is based on the preprint arXiv:2305.09635.

the performance, consider the following. For quantum repeaters in a chain, the end-to-end capacity for generating entanglement is equal to the minimal capacity over all pairs of neighboring nodes in the chain [3]. This minimal capacity is maximized by a symmetric placement of repeater nodes, and hence a symmetric placement optimizes the end-to-end capacity. We note however that there exist specific repeater protocols that do perform best, according to specific performance metrics, under asymmetric node placement [4, 5]. The suboptimal capacity of such a node placement suggests that improvements on the protocols could perhaps result in a symmetric placement being optimal again. This is demonstrated by Ref. [6], where it is shown that the advantage found in Ref. [5] vanishes when one further optimizes the protocol.

However, symmetric placement of nodes in a quantum network may not always be possible. For instance, if a quantum network is built using existing infrastructure this restricts the freedom in choosing the locations of the nodes, an example of which we have seen in Chapter 3. Therefore, in this chapter, we address the question how severely one can expect asymmetric node placement to affect the performance of a quantum network. We do so by investigating two separate aspects of asymmetric quantum networks: first, we consider asymmetric placement of midpoint stations and examine how entanglement generation between two neighboring nodes is affected (Section 4.1). We identify three independent effects, namely on the cycle time of entanglement generation (Section 4.1.1, see the beginning of Section 4.1 for a definition), on the success probability of entanglement generation and the fidelity of generated entanglement through the introduction of imbalanced losses (Section 4.1.2), and on the photon indistinguishability through chromatic dispersion (Section 4.1.3). Second, we consider asymmetric placement of quantum repeaters in a chain (Section 4.2). Here, we focus specifically on processing-node repeaters executing a SWAP-ASAP protocol (as explained in Section 4.2 and studied in, e.g., Refs. [7, 8]). Notably, the results presented in this chapter indicate robustness against small amounts of asymmetry. For asymmetry in the placement of the midpoint station, we find that both the success probability and fidelity have a vanishing first derivative with respect to how asymmetrically the midpoint is positioned (granted that the photons are shaped such that the effects of chromatic dispersion are negligible). However, the cycle time increases linearly with the asymmetry in case the time required to exchange signals between neighboring nodes is the limiting factor (it may be independent of asymmetry if this is not the case). Similarly, we find that both the entangling rate and error rate in a SWAP-ASAP repeater chain have vanishing first derivatives with respect to how asymmetrically the repeater nodes are positioned. This robustness suggests that, when designing a quantum network, nodes do not need to be placed exactly symmetrically. It furthermore suggests that the effects of constraints on node locations imposed by existing infrastructure on network performance may not be too severe.

4.1 Asymmetry in midpoint placement

Two popular methods for the creation of entanglement between neighboring nodes in a quantum network are single-click heralded entanglement generation [1, 9, 10] and double-click heralded entanglement generation (also known as the Barrett-Kok protocol) [2, 11–14]. In both of these protocols, time is slotted. In each time slot, the nodes perform a single attempt at entanglement generation. Such an attempt consists of both nodes sending a photon entangled with a local qubit to a midpoint station, where the photons are

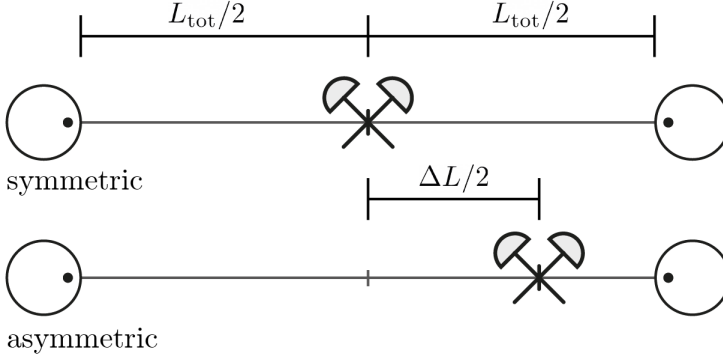


Figure 4.1: Symmetric and asymmetric positioning of a midpoint station for heralded entanglement generation. The magnitude of the parameter ΔL is a measure for how large the asymmetry is. ΔL and L_{tot} are defined in Equation (4.3).

interfered and measured. The midpoint then sends a message to the end nodes containing the measurement outcome. Depending on the measurement outcome, the attempt is declared either a success or a failure. The probability that it is declared a success is called the success probability and denoted by P_{succ} . The duration of each time slot (i.e., the time required to perform one attempt) is called the cycle time and denoted by T_{cycle} . The (average) rate at which successes occur is then given by

$$R = \frac{P_{\text{succ}}}{T_{\text{cycle}}}. \quad (4.1)$$

After a successful attempt a state ρ is shared by the two neighboring nodes. Ideally, the state ρ is some pure maximally-entangled target state $|\phi\rangle\langle\phi|$. However, due to noise, ρ will instead be a mixed state with fidelity

$$F = \langle\phi|\rho|\phi\rangle. \quad (4.2)$$

We will use the success probability P_{succ} , the cycle time T_{cycle} and the fidelity F as performance metrics for heralded entanglement generation.

In this section we study the effect of displacing the midpoint station from the exact center between the nodes (as illustrated in Figure 4.1) on our performance metrics. We do so by separately examining the effect on the cycle time, the effect that the resulting imbalanced losses have on the success probability and the fidelity, and the effect on the photon indistinguishability (which in turn affects primarily the fidelity but also the success probability). In order to do so we first need a method for quantifying how far the midpoint has been displaced. To that end, let the fiber distance between the midpoint station and the left-hand (right-hand) node be denoted L_{left} (L_{right}). Then we define

$$\begin{aligned} \Delta L &= L_{\text{left}} - L_{\text{right}}, \\ L_{\text{tot}} &= L_{\text{left}} + L_{\text{right}}. \end{aligned} \quad (4.3)$$

The parameter ΔL is then a measure of the amount of asymmetry, as shown in Figure 4.1. As we will show below, the effects of asymmetric midpoint placement on the cycle time, success probability and fidelity are all quantified by $|\Delta L|$.

4.1.1 Cycle time

First we consider the effect of asymmetric midpoint placement on the cycle time of the entanglement-generation protocol between neighboring nodes. During each cycle both nodes need to emit entangled photons that reach the midpoint station simultaneously. Then the midpoint station sends a message with the measurement result back to each of the nodes. Assuming both the entangled photons and the messages travel with the same velocity c , the cycle time at least includes the communication time between the midpoint station and the node that is furthest away. That is, $T_{\text{cycle}} \geq \frac{2}{c} \max(L_{\text{left}}, L_{\text{right}})$. This can be rewritten as

$$T_{\text{cycle}} \geq \frac{1}{c}(L_{\text{tot}} + |\Delta L|). \quad (4.4)$$

When the cycle time is limited only by the speed-of-light communication delay the cycle time will be exactly equal to the right-hand side of the equation. However, we note that in practice the cycle time is often much longer (see, e.g., Refs [10, 14]), for example due to local operations or the limited rate at which entangled photons can be emitted. In that regime, the cycle time may be independent of ΔL until the asymmetry becomes so large that the communication delays are again the limiting factor.

4.1.2 Imbalanced losses

As attenuation loss in fiber scales exponentially with the length of the fiber, having a midpoint station that is off center will result in an imbalance between the losses encountered by the photons. To be more precise, let P_0 be the probability that when a node attempts photon emission, this photon is emitted successfully, couples successfully to fiber, and is then successfully detected at a detector at the end of the fiber, given that the fiber has length zero. Then, the probability that photon emission at the left node leads to photon detection at the midpoint station is given by

$$P_{\text{left}} = P_0 e^{-\frac{L_{\text{left}}}{L_{\text{att}}}}, \quad (4.5)$$

where L_{att} is the attenuation coefficient of the fiber. The same equation holds for P_{right} , but with L_{left} replaced by L_{right} . In an asymmetric setup we will have $P_{\text{left}} \neq P_{\text{right}}$, which is what we mean by imbalanced losses. This can affect both the success probability P_{succ} and the fidelity F of heralded entanglement generation.

For both the single- and double-click protocol, expressions for P_{succ} and F in terms of, among other parameters, P_{left} and P_{right} can be found in Chapter 3. In order to make the effect of imbalanced losses explicit in these expressions we here introduce the parameters

$$\begin{aligned} P_{\text{tot}} &\equiv P_{\text{left}} P_{\text{right}} = P_0^2 e^{-\frac{L_{\text{tot}}}{L_{\text{att}}}}, \\ P_{\text{sum}} &\equiv P_{\text{left}} + P_{\text{right}} = 2 \sqrt{P_{\text{tot}}} \cosh\left(\frac{|\Delta L|}{2L_{\text{att}}}\right). \end{aligned} \quad (4.6)$$

Nontrivially, we find that for both protocols (to leading order, as discussed below) we can eliminate P_{left} and P_{right} completely from the expressions for P_{succ} and F in favour of P_{tot}

and P_{sum} . The effect of imbalanced losses is then captured entirely by the dependence of P_{sum} on ΔL . We discuss the resulting expressions and their implications for the single- and double-click protocol separately below.

In the double-click protocol, both nodes emit a photon. The mode that the photon is emitted in (e.g., its polarization) is entangled with the state of the emitter, and entanglement between the emitters is heralded when both photons are detected in different modes at the midpoint station after interfering on a beam splitter. By eliminating P_{left} and P_{right} as described above we find (see Section 4.5)

$$\begin{aligned} P_{\text{succ, 2click}} &= d_1 + 2p_{\text{dc}}P_{\text{sum}} + \mathcal{O}(p_{\text{dc}}^2), \\ F_{\text{2click}} &= d_2 - d_3p_{\text{dc}}P_{\text{sum}} + \mathcal{O}(p_{\text{dc}}^2). \end{aligned} \quad (4.7)$$

The parameters d_1 , d_2 , and d_3 have no direct dependence on ΔL and are given by

$$\begin{aligned} d_1 &= \frac{1}{2}P_{\text{tot}} - p_{\text{dc}} \left(4 + r - \frac{1}{2}(2-r)(1+V) \right) P_{\text{tot}}, \\ d_2 &= \left(\frac{1}{2}q_{\text{em}}(1+V) + \frac{1}{4}(1-q_{\text{em}}) \right) (1 + 8p_{\text{dc}}) \\ &\quad - \frac{1}{2}(2-r)q_{\text{em}}p_{\text{dc}}(1+V)^2, \\ d_3 &= \frac{q_{\text{em}}}{P_{\text{tot}}}(2V+1). \end{aligned} \quad (4.8)$$

Here, p_{dc} denotes the detector dark-count probability. The notation $\mathcal{O}(x^n)$ represents any terms that are of order n in the parameter x . As p_{dc} is typically small, we have only included leading-order terms in Equations (4.7) (the full expressions can be found in Section 4.5). V denotes the indistinguishability of the photons, which can itself depend on the asymmetry through the effect of chromatic dispersion as discussed in Section 4.1.3. It is assumed that the state shared between a node's emitter and the photon it emits is given by $\frac{1}{3}(4F-1)|\psi\rangle\langle\psi| + \frac{1}{3}(1-F)\mathbb{1}$, which has fidelity F to the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and where $F = F_{\text{em, left}}$ ($F = F_{\text{em, right}}$) for the left (right) node. We then have

$$q_{\text{em}} = \frac{1}{9}(4F_{\text{em, left}} - 1)(4F_{\text{em, right}} - 1). \quad (4.9)$$

Finally,

$$r = \begin{cases} 1 & \text{for non-photon-number-resolving detectors,} \\ 2 & \text{for photon-number-resolving detectors.} \end{cases} \quad (4.10)$$

We see that when the dark-count probability is zero, the double-click protocol is not affected by imbalanced losses at all. This is explained by the fact that the probability of both photons surviving their respective fiber segments is equal to the probability of a single photon surviving the full fiber length L_{tot} , which is not affected by asymmetry. The reason why the protocol is affected in the presence of dark counts is that as the photon arrival probability on the longer leg becomes of the same order as the dark-count probability, the probability of falsely heralding successful entanglement becomes large. This results both in an increased rate and a reduced fidelity.

In the single-click protocol, both nodes also perform photon emission and send those photons to the midpoint station. However, before emission starts, the emitter is prepared in an unbalanced superposition of a bright state from which photons can be emitted and a dark state from which emission is impossible. How large the amplitude of the bright state is, is parameterized by the bright-state parameter α . As a result, after emission, the state shared by the emitter and the photon takes the form

$$\sqrt{1-\alpha}|\text{dark}\rangle|0\rangle + \sqrt{\alpha}|\text{bright}\rangle|1\rangle, \quad (4.11)$$

where $|0\rangle$ ($|1\rangle$) indicates the absence (presence) of the photon. An attempt is then considered a success in case only one photon is detected at the midpoint station (as opposed to two for the double-click protocol), creating an entangled state that is a superposition of the left-node emitter being in the bright state but the right-node emitter in the dark state and vice versa. However, in case both emitters are in the bright state but one of the emitted photons is lost, a success is heralded without the creation of an entangled state. Therefore, even when the only imperfection in the system is fiber attenuation, the created entangled state is never pure. The fidelity of the created entangled state will depend on the choice of α ; when α is small, the relative probability that both nodes are found in the bright state is suppressed resulting in a good fidelity. However, using a small α also results in a small success probability. In case the midpoint is placed symmetrically and there are no imperfections but losses, for $\alpha \ll 1$, the success probability and fidelity can be approximated as $P_{\text{succ}} \approx 2\alpha\sqrt{P_{\text{tot}}}$ and $F \approx 1 - \alpha$. See, e.g., Ref. [15] for a further discussion of this effect. Thus, choosing the value of α is a matter of trading off success probability and fidelity. In an asymmetric setup it has been found that in case one wants to optimize the fidelity, the equation $\alpha_{\text{left}}P_{\text{left}} \approx \alpha_{\text{right}}P_{\text{right}}$ should be satisfied [10]. Therefore, we here assume the bright-state parameters are always chosen such that

$$\alpha_{\text{left}}P_{\text{left}} = \alpha_{\text{right}}P_{\text{right}} \equiv q, \quad (4.12)$$

where q parameterizes the remaining degree of freedom. As the bright-state parameter needs to be small in order to get a good fidelity, we will here present a result that is not only leading order in the dark-count probability but also in the parameter q . Eliminating α_{left} and α_{right} in favour of q and P_{left} and P_{right} in favour of P_{tot} and P_{sum} we find (see Section 4.5)

$$\begin{aligned} P_{\text{succ, 1click}} &= 2q + 2p_{\text{dc}} + \mathcal{O}(q^2, p_{\text{dc}}^2, qp_{\text{dc}}), \\ F_{\text{1click}} &= s_1 - s_2P_{\text{sum}} + \mathcal{O}(q^2, p_{\text{dc}}^2, qp_{\text{dc}}). \end{aligned} \quad (4.13)$$

Here, the parameters s_1 and s_2 are defined by

$$\begin{aligned} s_1 &= \frac{1}{2}(1 + \sqrt{V}) \frac{q}{q + p_{\text{dc}}} \left(1 + q - (1+r)p_{\text{dc}} \right. \\ &\quad \left. + \frac{q}{q + p_{\text{dc}}} \left[rp_{\text{dc}} - \frac{1}{4}(2-r)(1+V)q \right] \right), \\ s_2 &= \frac{1}{2}(1 + \sqrt{V}) \frac{q}{q + p_{\text{dc}}} \frac{1}{P_{\text{tot}}} \left(\frac{1}{2}q - p_{\text{dc}} \right). \end{aligned} \quad (4.14)$$

Note that the success probability of the single-click scheme is not affected when ΔL is increased, as long as the bright-state parameters are chosen to keep q constant. This behaviour is not a consequence of the leading-order expansion. It is shown in Section 4.5

that the exact expression for the success probability has no direct dependence on the asymmetry either.

The success probability and fidelity as a function of the asymmetry are shown in Figure 4.2 for both protocols. We see that in both cases imbalanced losses do not reduce the success probability. Additionally the fidelity falls in a similar way for both cases, with a vanishing first derivative at $\Delta L = 0$. The reason for this is that the hyperbolic cosine to which P_{sum} is proportional (see Equations (4.6)) has a vanishing first derivative at zero. As a result, the success probability and fidelity are resilient against small amounts of asymmetry. For instance, for the parameters considered in Figure 4.2, we see that the fidelity is still above 99% of the value it attains for symmetric midpoint placement at $\Delta L = 30$ km.

4.1.3 Photon indistinguishability

Light waves traveling through optical fiber are subject to chromatic dispersion, meaning that different frequency components travel at different velocities. As a result, when performing heralded entanglement generation, the photons that arrive at the midpoint station are shaped differently than the photons that are emitted by the nodes. A key requirement for the creation of an entangled state through the interference and measurement of the photons is that the photons are indistinguishable, i.e., their wave packets need to be identical and arrive at the midpoint simultaneously. Although chromatic dispersion always results in photon deformation, the indistinguishability will not be affected if both photons are subjected to the same amount of dispersion. This is the consequence of a phenomenon known as dispersion cancellation [16, 17]. The situation is different in case the midpoint station is placed asymmetrically. If the photons travel through fibers of different lengths they will undergo different amounts of dispersion and hence be deformed differently.

A wave packet ϕ in a one-dimensional medium emitted at time $t = t_0$ and location $x = 0$ takes the form

$$\phi(x, t) = \int d\omega \phi(\omega) e^{i\omega(t-t_0) - i\beta(\omega)x}. \quad (4.15)$$

Here, $\beta(\omega)$ is the wave number corresponding to a monochromatic wave with angular frequency ω , which is determined by the medium the wave travels in. Now, let ϕ_l (ϕ_r) be the wave packet of the photon emitted by the left (right) node. The indistinguishability V between these photons at the midpoint station (i.e., at $x = L_{\text{left}}$ for ϕ_l and at $x = L_{\text{right}}$ for ϕ_r) is then defined by

$$V = |\mu|^2, \quad (4.16)$$

where μ is given by

$$\begin{aligned} \mu &= \int dt \phi_l(L_{\text{left}}, t) \phi_r^*(L_{\text{right}}, t) \\ &= \int d\omega \phi_l(\omega) \phi_r^*(\omega) e^{i\beta(\omega)\Delta L + i\omega\Delta t}. \end{aligned} \quad (4.17)$$

Here, we have $\Delta t = t_l - t_r$, where t_l (t_r) is the time of emission of the photon at the left (right) node. As discussed in Section 4.1.2, the indistinguishability V affects both the success probability and the fidelity of the single- and double-click protocols.

We assume that the wave packets have a central frequency that is close to some frequency ω_0 . It is then useful to Taylor expand the wave number of the fiber as [18]

$$\beta(\omega) \approx \beta_0 + \beta_1(\omega - \omega_0) + \frac{1}{2}\beta_2(\omega - \omega_0)^2 + \frac{1}{6}\beta_3(\omega - \omega_0)^3. \quad (4.18)$$

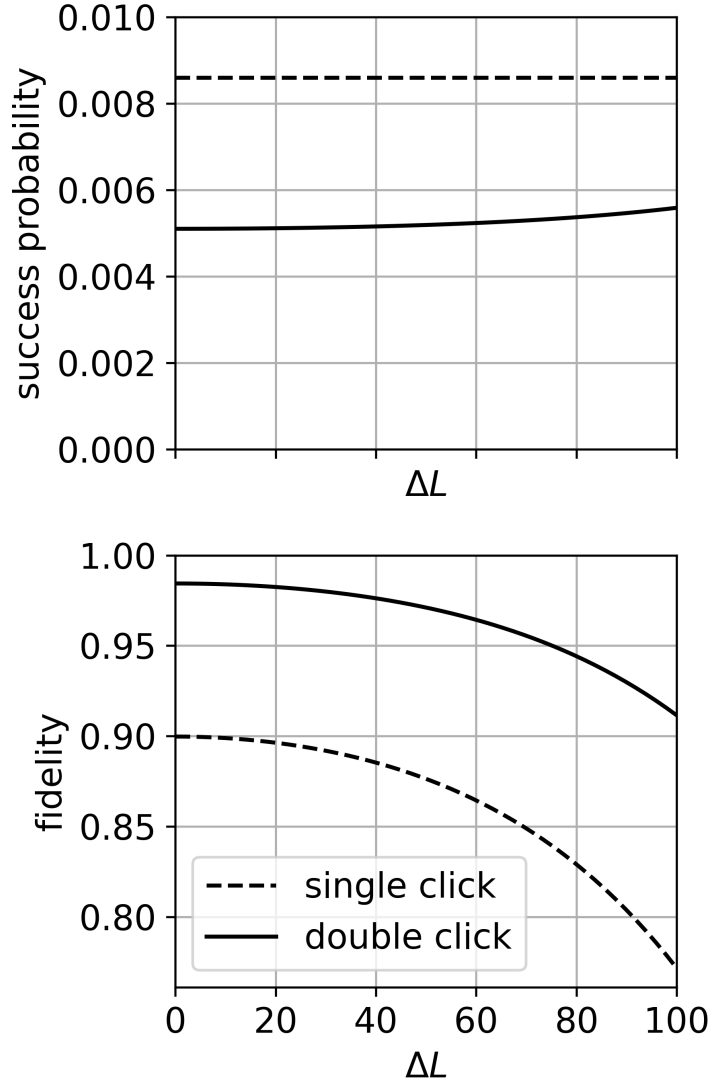


Figure 4.2: Leading-order results (presented in Equations (4.7) and (4.13)) for the probability that an entanglement-generation attempt is heralded as a success and the fidelity of entangled states created upon a heralded success of both the single-click and double-click protocol as a function of the difference in length between the two fibers connecting the midpoint station (ΔL , defined in Equation (4.3)). This figure has been created using the parameters $L_{\text{tot}} = 100$ km, $p_{\text{dc}} = 3 \cdot 10^{-4}$, $q = 4 \cdot 10^{-3}$ and $L_{\text{att}} \approx 22$ km. Apart from attenuation losses and dark counts no imperfections have been included.

Here, $\beta_0 = 1/v_p$ and $\beta_1 = 1/v_g$, where v_p and v_g are the phase and group velocity in the fiber respectively. β_2 is the Group-Velocity Dispersion (GVD) parameter and β_3 the Third-Order Dispersion (TOD) parameter. As the β_0 contribution will only alter the global phase of μ , it does not affect the indistinguishability and can effectively be dropped from the expression. Furthermore, we assume $\Delta t = -\beta_1 \Delta L + \delta t$, where δt is the alignment mismatch (for $\delta t = 0$, both emissions are timed such that the photons arrive at the midpoint station exactly at the same time). Then, using $\Delta\omega \equiv \omega - \omega_0$, we can effectively write

$$\mu = \int \phi_l(\omega_0 + \Delta\omega) \phi_r^*(\omega_0 + \Delta\omega) \times e^{i\Delta L(\frac{1}{2}\beta_2\Delta\omega^2 + \frac{1}{6}\beta_3\Delta\omega^3) + i\delta t\Delta\omega} d\Delta\omega. \quad (4.19)$$

The value of V and how much it is degraded by chromatic dispersion depends on the exact shapes of the photons, i.e., on ϕ_l and ϕ_r . In general, we expect the photons to be affected by chromatic dispersion less if their spread in frequency is small, as frequency components that are far apart also travel at velocities that are far apart. Below, we derive expressions for V in case of two specific wave-packet shapes, namely Gaussian and Lorentzian. (Attenuated) laser pulses are often approximated as Gaussian, and approximate Gaussian photons can, e.g., be produced using cavity quantum electrodynamics [19] or spontaneous four-wave mixing [20]. We here take Gaussian wave packets as a generic example of a pulse which is well localised in time and frequency, allowing us to obtain analytical results. On the other hand, Lorentzian photons are created through the radiative decay of a two-level system. In practice, photons will rarely be exactly Gaussian or Lorentzian as they interact with other components in the system such as filters and cavities. Yet, we can think of the two types of photons as two extremes in how spread out their frequency distributions are, and therefore how sensitive they are to chromatic dispersion. It was noted in Ref. [21] that a Gaussian wave packet, for a fixed value of the time-distribution standard deviation, has a frequency-distribution standard deviation that is as small as possibly allowed by the Heisenberg uncertainty principle. From this the authors concluded that Gaussian photons offer the best protection against alignment mismatch δt . Here, it leads us to expect Gaussian photons are well protected against chromatic dispersion. Lorentzian photons on the other hand have frequency distributions with very long tails, with $|\phi_{l/r}(\omega)|^2$ only going to zero as $\frac{1}{\omega^2}$. It is expected that they are therefore much more susceptible to the effects of chromatic dispersion.

Gaussian photons

The wave packets of two Gaussian photons with frequency mismatch $\delta\omega$ can be written as

$$\phi_{l/r}(\omega) = \frac{1}{\sqrt[4]{2\pi\sigma^2}} e^{-\frac{1}{4\sigma^2}(\omega - \omega_0 \pm \frac{1}{2}\delta\omega)^2}. \quad (4.20)$$

The probability distributions $|\phi_{l/r}(\omega)|^2$ are Gaussian with standard deviation σ . When there is no TOD, the indistinguishability can be calculated exactly, giving

$$V|_{\beta_3=0} = \frac{\exp\left(-2\left(\frac{\delta\omega}{\sigma}\right)^2 - \frac{(\delta t\sigma)^2}{1 + \Delta L^2 \beta_2^2 \sigma^4}\right)}{\sqrt{1 + \Delta L^2 \beta_2^2 \sigma^4}}. \quad (4.21)$$

We derive this result in Section 4.6. A similar expression has been derived under the more restrictive assumption $\delta t = \delta\omega = \beta_3 = 0$ in Ref. [22], with which ours is consistent. In case the photon indistinguishability is close to one, $1 - V|_{\beta_3=0} \ll 1$, it is well-approximated by the leading-order expansion

$$V|_{\beta_3=0} \approx 1 - 2 \left(\frac{\delta\omega}{\sigma} \right)^2 - (\delta t \sigma)^2 - \frac{1}{2} \Delta L^2 \beta_2^2 \sigma^4 \quad (4.22)$$

Finding an exact solution to Equation (4.19) when the TOD is nonzero is difficult, but a leading-order result can be readily found to yield

$$V = V|_{\beta_3=0} \left(1 - \Delta L \beta_3 \delta t \sigma^4 \right) + \mathcal{O} \left(\Delta L^2 \beta_3^2 \sigma^6, \Delta L^3 \beta_2^2 \beta_3 \delta t \sigma^8, \Delta L \beta_3 \delta t^3 \sigma^6 \right). \quad (4.23)$$

This result as well is derived in Section 4.6. Note that, to first order, the TOD does not affect the indistinguishability in case $\delta t = 0$. If the alignment mismatch is itself small, $|\delta t \sigma| \ll 1$, we can expect the TOD to have only a very small effect on the indistinguishability.

Lorentzian photons

For two Lorentzian wave packets with frequency mismatch $\delta\omega$ we can write

$$\phi_{l/r}(\omega) = \sqrt{\frac{2\tau}{\pi}} \frac{1}{1 - 2i\tau(\omega - \omega_0 \pm \frac{1}{2}\delta\omega)}. \quad (4.24)$$

While the corresponding frequency distributions are Lorentzian functions with $\frac{1}{\tau}$ as full width at half maximum, the time distributions of these photons are one-sided exponentials with standard deviation τ . We are not aware of an analytical method for determining the indistinguishability for Lorentzian photons in full generality. One method to evaluate the indistinguishability is numerical integration as done in Refs. [23, 24]. Instead we make the simplifying assumptions that the photons arrive at the same time ($\delta t = 0$), they have the same central frequency ($\delta\omega = 0$), and there is no TOD ($\beta_3 = 0$). The indistinguishability then becomes exactly solvable, giving (see Section 4.6 for a derivation)

$$V|_{\delta t=\delta\omega=\beta_3=0} = 1 - \frac{2\sqrt{2}}{\sqrt{\pi}} (C + S) + \frac{4}{\pi} (C^2 + S^2). \quad (4.25)$$

Here, C and S are Fresnel integrals defined by $S = \int_0^x \sin(t^2) dt$ and $C = \int_0^x \cos(t^2) dt$ with $x = \sqrt{\frac{1}{2}|\Delta L \beta_2|} \tau^{-2}$. To linear order, $C = x$ and $S = 0$, and therefore when the effect of dispersion is small we can use the approximation

$$V|_{\delta t=\delta\omega=\beta_3=0} = 1 - \frac{2}{\sqrt{\pi}} \frac{\sqrt{|\Delta L \beta_2|}}{\tau} + \mathcal{O}(|\Delta L \beta_2| \tau^{-2}). \quad (4.26)$$

We stress that the assumption $\delta t = \delta\omega = \beta_3 = 0$ is not generally expected to hold in a real experiment; it is introduced solely to make the problem analytically more tractable. However, by comparing to results obtained through numerical integration we find that the

assumption $\beta_3 = 0$ does not greatly affect the result in conditions typical to single-mode fiber (see the discussion below and Figure 4.4). Therefore, while the above equations may not be able to capture the effects of δt and $\delta\omega$, they do accurately capture the effects of asymmetry in the placement of the midpoint station, as is the focus of this section. Furthermore, we note that it may sometimes already be desirable to use frequency conversion to convert photons to frequencies that incur relatively less attenuation losses in fiber. This opens up the possibility for correcting any frequency mismatch and bringing $\delta\omega$ close to zero [25].

Requirements for indistinguishable photons

The results above describe how the indistinguishability V is diminished through the effect of chromatic dispersion in the case of asymmetric midpoint placement. From these results, it becomes clear that how badly V is reduced depends on the characteristics of the photon. In particular, for Gaussian photons it depends on the parameter σ , while for Lorentzian photons it depends on the parameter τ . As expected, for both photons the effect of dispersion is increased as the width of the frequency distribution is increased, or equivalently, as the length of the time distribution is decreased. In Figure 4.3 we investigate how much indistinguishability is lost as a function of the length of the photon wave packet, assuming the photons are otherwise perfectly indistinguishable. We here make the simplifying assumption that there is no TOD, thereby enabling the use of the exact analytical results obtained above. This simplification is motivated by the fact that comparing our analytical results in case the TOD is zero with results obtained through numerical integration for a typical value of the TOD in single-mode optical fiber suggests that the TOD has only a negligible effect in this case, as shown in Figure 4.4. Unsurprisingly we see in Figure 4.3 that Lorentzian photons with their long tails in frequency are affected (much) worse by chromatic dispersion than Gaussian photons with the same length. However, even for Lorentzian photons we see that (for standard single-mode fiber and $\Delta L = 40$ km) the decrease in V is only of the order 10^{-2} when the length of the wave packet is of the order of nanoseconds.

In case the photon length and ΔL are such that the decrease in photon indistinguishability can be significant, it is clear that it is better if the photons are closer in shape to a Gaussian than a Lorentzian. This strengthens the case for Gaussian photons made in Ref. [21], where it was found that Gaussian photons protect favourably against alignment mismatch. However, some sources naturally emit photons that are more Lorentzian than Gaussian. Potentially, photon-shaping techniques could be used to convert such photons to a more Gaussian waveform [35–39]. A simpler solution could be to send Lorentzian photons through a filter to remove the long tails of their frequency distribution. While this would introduce extra losses, the spread in frequency could be greatly reduced, resulting in a much more Gaussian photon.

Lastly we point out that there are various methods for reducing the drop in indistinguishability in case of asymmetric midpoint placement irrespective of photon shape. The telecom C-band (1530 nm - 1565 nm) is the band conventionally used to transmit signals as it minimizes attenuation losses (a typical value of 0.275 dB/km in standard single-mode fiber [26]). In contrast the telecom O-band (1260 nm - 1360 nm) incurs much heavier attenuation losses (typically 0.5 dB/km [26]), but as it is centered around the zero-dispersion wavelength (1310 nm) of standard single-mode optical fiber it minimizes dispersive effects. By using the O-band instead of the C-band one can lessen the effects of chromatic

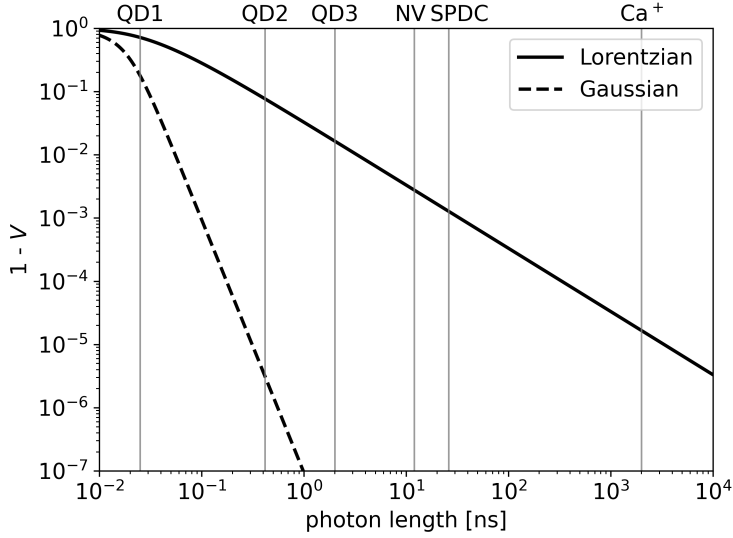


Figure 4.3: Loss in the indistinguishability V as a function of the temporal photon length, as measured by the standard deviation of the time distribution $|\phi(x=0, t)|^2$. We include results for both Gaussian and Lorentzian photons (Equations (4.23) and (4.26)), for which the standard deviations are given by $\frac{1}{\sqrt{2}\sigma}$ and τ respectively. The results assume $\Delta L = 40$ km and a GVD of $\beta_2 \approx -21.7 \text{ ps}^2/\text{km}$ (corresponding to a dispersion coefficient of $17 \text{ ps}/(\text{nm km})$, which is a typical value for single-mode optical fiber at 1550 nm [26]). The TOD parameter has been set to $\beta_3 = 0$. Other sources of noise are not included. That is, $\delta t = \delta \omega = 0$. The lengths of photons emitted by some specific sources have been indicated in the figure. QD1, QD2, QD3: quantum-dot sources from Refs. [27], [28] and [29] respectively. NV: nitrogen-vacancy centers in diamond [25, 30, 31]. (Some types of trapped ions, such as Ba^+ [32] and Sr^+ [13] emit photons at a length close to the NV one.) SPDC: frequency-multiplexed spontaneous parametric down-conversion sources that interface with atomic quantum memories [33, 34]. Ca^+ : trapped calcium ions [14] (lifetime estimated in Section 3.6.6).

dispersion at the cost of incurring extra losses. This strategy is utilized in e.g., Ref. [40]. An investigation in Ref. [22] based on Gaussian photons suggests that using the O-band may only be worth it for photons shorter than approximately 100 picoseconds. A second potential solution is the use of dispersion-shifted fiber. Such fiber has its zero-dispersion wavelength in the telecom C-band and provides simultaneously small dispersion and small attenuation loss [41]. However, such fiber is not widely deployed [22, 42] and hence not suitable when using existing fiber infrastructure to build a quantum network. Finally, one can use dispersion-compensating modules to reduce the effects of chromatic dispersion at the cost of incurring extra losses [42].

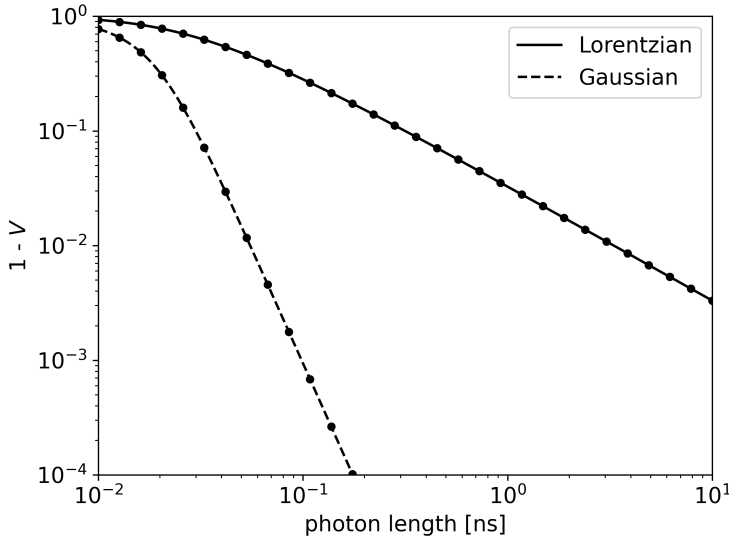


Figure 4.4: A comparison between our analytical results (the lines) for the photon indistinguishability V assuming the TOD is zero (Equations (4.21) and (4.26)) and results obtained through numerical integration assuming a nonzero TOD (the markers). The temporal photon length is used as x axis, as measured by the standard deviation of $|\phi(x=0, t)|^2$. The results assume $\Delta L = 40$ km, a GVD of $\beta_2 \approx -21.7 \text{ ps}^2/\text{km}$ and a TOD parameter of $\beta_3 \approx 0.127 \text{ ps}^3/\text{km}$ (corresponding to a dispersion coefficient of $17 \text{ ps}/(\text{nm km})$ and a dispersion slope of $0.056 \text{ ps}/(\text{nm}^2 \text{ km})$, which are typical values for single-mode optical fiber at 1550 nm [26]). Other sources of noise are not included. That is, $\delta t = \delta \omega = 0$). Error bars for the numerical results are smaller than the marker size.

4.2 Asymmetry in repeater chains

Now we turn our attention away from the placement of midpoint stations and instead consider the placement of repeater nodes in a quantum-repeater chain. First, in Section 4.2.1, we discuss the specific type of quantum-repeater chains we consider here. Then, we pose two research questions about asymmetry in such repeater chains in Section 4.2.2. These questions are made more precise in Sections 4.2.3, 4.2.4, and 4.2.5. This allows us to address the research questions using numerical simulations in Section 4.2.6. Finally, we reflect on the numerical results in Section 4.2.7.

4.2.1 SWAP-ASAP repeaters with parallel entanglement generation

While there exist many types of quantum repeaters [43, 44], we here focus on one specific type, namely the processing-node quantum repeater. Such quantum repeaters are capable of generating and storing entanglement with neighboring nodes and of executing quantum gates. These gates allow processing nodes to perform deterministic entanglement swapping, which is an operation such that if one qubit is entangled with some qubit A and the other qubit is entangled with some qubit B, performing entanglement swapping on those two qubits will result in qubits A and B being entangled [45]. Various proposed repeater platforms are processing nodes, such as trapped ions [46–49], color centers in diamond [10, 50, 51] and neutral atoms [52, 53].

We here assume that each repeater has exactly two qubits, each of which can be used

in parallel to perform heralded entanglement generation (as discussed in Section 4.1) with a different neighboring node. (Note that there exist also proposed repeater systems that can only generate entanglement with one neighbouring node at a time [6, 10, 54].) A chain of such repeaters can then create end-to-end entanglement by combining heralded entanglement generation and entanglement swapping. How these are combined exactly, and what additional operations are performed, is dictated by the protocol that the repeaters execute. Examples of additional operations that could be included are discarding entangled states when they have been stored in memory for too long [6, 8, 55, 56] and entanglement distillation [57–59], both of which can help mitigate the effects of noise. Optimizing repeater protocols is by no means an easy matter, and what protocols perform well depends both on the specific hardware used and the performance metric employed [4, 8, 55, 60–63]. Here, we consider the SWAP-ASAP protocol, in which no additional operations are included. In the SWAP-ASAP protocol, each pair of neighboring nodes performs entanglement generation whenever this is possible. That is, whenever at each node the qubit that is reserved for entanglement generation along that specific link is free. As soon as both qubits at a repeater node are entangled it performs entanglement swapping (thereby freeing both qubits up again). We have chosen to study this protocol as it is relatively simple both to understand and to study numerically. Moreover, it has been found that the SWAP-ASAP protocol outperforms schemes that include entanglement distillation for near-term hardware quality, as measured both by the fidelity of end-to-end entangled states and the generation duration [7]. Additionally, for the case when entanglement swapping is deterministic and entanglement is never discarded, it was found that the SWAP-ASAP protocol results in an optimal generation duration [8, 63]. Throughout the rest of this chapter, it will be assumed that quantum repeaters can generate entanglement with two neighbours in parallel and that they execute the SWAP-ASAP protocol.

4.2.2 Research questions

Asymmetric node placement will result in some fiber links between repeaters being shorter while others are longer. As attenuation losses grow exponentially with the fiber length, the longer links generate entanglement at a slower rate, and the shorter links at a faster rate. In other words, the entangling rates along the chain become uneven due to asymmetric repeater placement. The slower links could then potentially become bottlenecks. This is expected to increase not only the amount of time required to distribute end-to-end entanglement, but also the amount of time entangled states need to be stored in the SWAP-ASAP quantum repeaters until entanglement swapping takes place. The result of this would be an increased amount of noise due to memory decoherence.

The above observation motivates posing the following research question: what is the effect of uneven entangling rates in a SWAP-ASAP repeater chain in which repeaters can generate entanglement with both neighboring nodes simultaneously, as caused by the asymmetric distribution of the repeater nodes, on the performance of that chain? A particularly simple method that could perhaps be used to mitigate any negative effects of asymmetric node placement is what we here refer to as the “extended-fiber method”. In this method, spooled fiber is used at the repeater nodes to make the shorter links as long as the longer ones, thereby effectively making the repeater chain symmetric again. However, rather than making the bottlenecks faster, this method just makes the faster links slower. It seems perhaps unlikely that such a strategy can lead to any improvement. Therefore, we

pose a second research question: is the extended-fiber method effective at improving the performance of asymmetric SWAP-ASAP repeater chains in which repeaters can generate entanglement with both neighboring nodes simultaneously? In order to address these questions, they need to be made more precise. To that end, we first quantify how well a repeater chain performs in Section 4.2.3. Then, we quantify how asymmetrical a repeater chain is and how we can systematically vary the amount of asymmetry in Section 4.2.4. Finally, we introduce a simplified model for repeater chains in Section 4.2.5.

4.2.3 Quantifying repeater performance

We quantify the performance of a repeater chain in terms of how capable it is at supporting Quantum Key Distribution (QKD). Specifically, we consider the rate at which a secret key can be obtained when executing an entanglement-based implementation of the BB84 protocol [64, 65] in the asymptotic limit. The end nodes realize this protocol by keeping entangled quantum states stored in memory until they learn that all required entanglement swaps have been performed and hence end-to-end entanglement has been created. At that time, they each measure their qubit in either the Pauli X or Z basis. The corresponding asymptotic secret-key rate is given by [66]

$$\text{SKR} = \frac{1}{T} \max(1 - 2h(Q), 0). \quad (4.27)$$

Here, T is the generation duration, i.e., the average time required to distribute an end-to-end entangled state, Q is the Quantum-Bit Error Rate (QBER), and $h(x) = -x \log_2(x) - (1-x) \log_2(1-x)$ is the binary entropy function. The QBER is defined as the probability that, if both end nodes measure their qubits in the same basis, the parity between the outcomes is different than would be expected for the maximally-entangled target state. Therefore, the QBER can be considered a measure for the amount of noise. Note that, in general, the QBER can take a different value for measurements in the X basis than in the Z basis. However, as we will be using a depolarizing noise model (see Section 4.2.5 below), the two values will coincide. Our choice for the secret-key rate as performance metric is motivated not only by the fact that it has a clear operational interpretation, but also because it combines information about how quickly and how noisily entanglement is distributed into a single convenient number. While the secret-key rate is the primary performance metric considered here, the generation duration and QBER from which the secret-key rate is calculated can help provide a more detailed understanding of a repeater chain's performance.

4.2.4 Quantifying chain asymmetry

Now, we first discuss how asymmetry in a repeater chain can be quantified. We then use that to introduce a specific method for placing repeaters in a chain in such a way that the amount of asymmetry can be varied. Let \mathcal{R} be the set of all repeater nodes in the chain of interest. Then, for every $n \in \mathcal{R}$, the *node asymmetry parameter* is defined by

$$\mathcal{A}_n = \frac{|L_{\text{left of } n} - L_{\text{right of } n}|}{L_{\text{left of } n} + L_{\text{right of } n}} \quad (4.28)$$

and the *node asymmetry sign* is defined by

$$S_n = \text{Sgn}(L_{\text{left of } n} - L_{\text{right of } n}). \quad (4.29)$$

Here, $L_{\text{left of } n}$ ($L_{\text{right of } n}$) is the fiber distance between node n and its neighboring node to the left (right) and Sgn is the sign function. We note that \mathcal{A}_n is equivalent to $\Delta L/L_{\text{tot}}$ and S_n to $\text{Sgn}(\Delta L)$, where ΔL and L_{tot} are defined for that specific node as in Equation (4.3). While ΔL proved convenient to describe the effects of asymmetry in the placement of midpoint stations, we find the node asymmetry parameter more convenient in the context of repeater chains. This is because the value of L_{tot} can vary between different nodes in the chain, making it hard to understand just how asymmetrically a node is placed between its neighboring nodes from only ΔL . The node asymmetry parameters and node asymmetry signs of all repeater nodes together provide a complete parameterization of the locations of the nodes in the chain. Now, we define the *chain asymmetry parameter* $\mathcal{A}_{\text{chain}}$ to be the average value of \mathcal{A}_n over all repeaters,

$$\mathcal{A}_{\text{chain}} = \frac{1}{|\mathcal{R}|} \sum_{n \in \mathcal{R}} \mathcal{A}_n. \quad (4.30)$$

While the node asymmetry parameter \mathcal{A}_n quantifies how asymmetrically one specific node is placed between its neighboring nodes, the chain asymmetry parameter $\mathcal{A}_{\text{chain}}$ aims to capture how asymmetric the chain is as whole.

We aim to address the research questions posed in Section 4.2.2 by investigating how the repeater-chain performance varies as a function of $\mathcal{A}_{\text{chain}}$. However, for a repeater chain with a given total length and given number of nodes, there are many different possible repeater placements for which the chain asymmetry parameter takes the same value. Therefore, in order to avoid ambiguity, we here introduce a specific class of repeater chains for which the parameter $\mathcal{A}_{\text{chain}}$ (together with the total length and number of nodes) uniquely defines the locations of all the repeaters. These are repeater chains for which \mathcal{A}_n is the same for every repeater in the chain and S_n alternates between nodes (such that no two neighboring repeaters have the same sign). It then holds that $\mathcal{A}_{\text{chain}} = \mathcal{A}_n$ for all $n \in \mathcal{R}$. See Figure 4.5 for an example of what such a repeater chain looks like for different values of $\mathcal{A}_{\text{chain}}$. Our reason for choosing this class of chains is that the chains are relatively regular and easy to understand, while at the same time increasing $\mathcal{A}_{\text{chain}}$ clearly increases the disparity between long and short links, allowing us to study the effect of different entangling rates between different nodes as we set out to do.

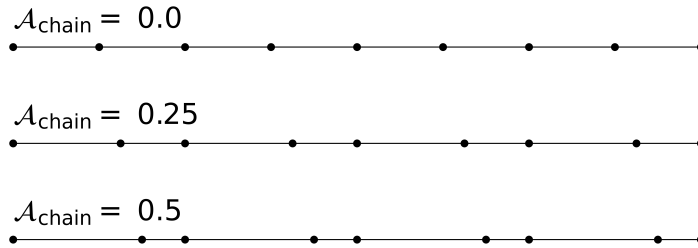


Figure 4.5: Locations of nodes in a chain with 7 repeaters for which $\mathcal{A}_n = \mathcal{A}_{\text{chain}}$ is the same for all nodes and S_n alternates between nodes (see definitions in Equations (4.28), (4.29) and (4.30)). The chain asymmetry parameter $\mathcal{A}_{\text{chain}}$ then quantifies the amount of asymmetry.

4.2.5 Model for Repeater Chain

We consider a simplified model for the repeater nodes as well as for heralded entanglement generation between neighboring nodes. In this model, the midpoint stations studied in Section 4.1 are abstracted away, such that we can focus on the placement of the repeater nodes only. We then take the cycle time for performing one attempt at generating an entangled state between two neighboring nodes to be given by

$$T_{\text{cycle}} = \frac{L}{c}, \quad (4.31)$$

where L is the distance between the neighboring nodes and c is again the speed of light in fiber (here taken to be 200,000 km/s). We note that this is equivalent to the cycle time when entanglement between neighboring nodes is generated using a symmetrically placed midpoint (see Equation (4.4)). We model the success probability of each attempt as

$$P_{\text{succ}} = e^{-\frac{L}{L_{\text{att}}}}, \quad (4.32)$$

where $L_{\text{att}} \approx 22$ km is the attenuation length corresponding to attenuation losses of 0.2 dB/km. This model has been chosen both for simplicity and for not being overly specific to one particular protocol for heralded entanglement generation. It reflects the exponential scaling of the success probability common to both the double-click and single-click protocols, and also to protocols based on the direct transmission of photons between neighboring nodes [67–69] (assuming dark counts do not contribute significantly). Therefore it is expected to adequately capture, at least on a qualitative level, how uneven entangling rates arise due to asymmetric node placement in repeater chains based on heralded entanglement generation.

We model the states created by heralded entanglement generation to be noiseless. More precisely, whenever an attempt is successful, a pure Bell state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is created. We consider the repeater nodes to be largely perfect devices at which entanglement swapping can be performed noiselessly and deterministically. The only imperfection modeled at both repeater nodes and end nodes is that while qubits are stored in quantum memory, they undergo memory decoherence. For simplicity, we model memory decoherence as depolarizing noise according to

$$\rho \rightarrow e^{-\frac{t}{T_{\text{coh}}}} \rho + (1 - e^{-\frac{t}{T_{\text{coh}}}}) \frac{\mathbb{1}}{2}. \quad (4.33)$$

Here t is the storage time and T_{coh} the coherence time, which we take to be one second here (as demonstrated with nitrogen-vacancy centers in Ref. [70]). Given these assumptions, noise in end-to-end entangled states produced by the repeater chain has only two sources. The first of these is repeaters storing entangled states in quantum memory until entanglement swapping takes place. The second is end nodes storing entangled states until all entanglement swaps have been completed and the measurements required by the BB84 protocol are performed. These are exactly the sources of noise that may be affected by uneven entangling rates in a repeater chain.

4.2.6 Numerical results

Now, we are ready to address the research questions outlined in Section 4.2.2. For concreteness, we consider a repeater chain with a length of 1000 km that contains 21 nodes

(including two end nodes). The nodes are thus, in the symmetric case, spaced 50 km apart. A distance of 1000 km can be thought of as a typical pan-continental one, corresponding to, e.g., roughly the distance between Paris and Berlin. In order to estimate the values of the generation duration and the QBER, we employ numerical simulations using the quantum-network simulator NetSquid [7]. These simulations are based on the code introduced in Ref. [54] and make use of a number of open-source libraries [71–77]. All simulation code and data can be found in our repository [78]. After the generation duration and QBER have been estimated, an estimate for the secret-key rate is computed using Equation (4.27). The simulations are performed for different values of the chain asymmetry parameter $\mathcal{A}_{\text{chain}}$, and both for asymmetric chains and chains that have been symmetrized again using the extended-fiber method. The results of these simulations are shown in Figure 4.6. It can be directly seen that using the extended-fiber method does not improve the performance of the repeater chain, but instead reduces it significantly. Simulation results demonstrating that the same conclusion holds for other numbers of repeaters, other chain lengths and other coherence times can be found in our repository [78]. This suggests that the question whether the extended-fiber method can be used to mitigate the adverse effects of uneven entangling rates due to asymmetric repeater placement must be answered in the negative.

It can be observed that the performance of the repeater chain exhibits some resilience against small amounts of asymmetry. At $\mathcal{A}_{\text{chain}} = 0.1$ the secret-key rate has only fallen by about 10%, and at $\mathcal{A}_{\text{chain}} = 0.2$ by about 50%. For the specific repeater chain we consider, this corresponds to all the even nodes in the chain being displaced by 5 km and 10 km respectively as compared to their position in a symmetric chain, while the odd nodes remain in place (see also Figure 4.5). This resilience seems to be a consequence of the fact that both the generation duration and the QBER have a vanishing first derivative at $\mathcal{A}_{\text{chain}} = 0$ in Figure 4.6. We note furthermore that the first derivatives not only appear to vanish for the parameters considered in Figure 4.6, but also for different numbers of nodes, chain lengths and coherence times, as demonstrated by data that can be found in our repository [78].

4.2.7 Reflection on numerical results

It may be surprising that the first derivatives in Figure 4.6 appear to vanish. After all, when \mathcal{A}_n is nonzero, the resultant longer links may be expected to form bottlenecks. However, we need to take into account that while the longer links become slower at generating entanglement, the shorter links become faster. It would appear that for small values of \mathcal{A}_n the negative effect of the slower links is mostly compensated by the positive effect of the faster links. To foster an intuitive understanding, let us introduce the following hand-waving argument that reinforces the interpretation that first-order effects on the fast and slow links cancel each other. Consider a single repeater node $n \in \mathcal{R}$. This repeater is connected to its two neighbors by fibers of lengths $\frac{1}{2}L_{\text{tot}}(1 \pm \mathcal{A}_n)$, where L_{tot} is the sum of the two lengths. Therefore, from combining Equations (4.1), (4.31) and (4.32), we find that

the average rates at which entanglement is generated with the two different neighbors are

$$\begin{aligned}
 R_{\pm} &= \frac{c \exp\left(-\frac{L_{\text{tot}}}{2L_{\text{att}}}(1 \pm \mathcal{A}_n)\right)}{L_{\text{tot}}(1 \pm \mathcal{A}_n)} \\
 &= \frac{c e^{-\frac{L_{\text{tot}}}{2L_{\text{att}}}}}{L_{\text{tot}}} \left(1 \mp \left(\frac{L_{\text{tot}}}{2L_{\text{att}}} + 1\right)\mathcal{A}_n\right) + \mathcal{O}(\mathcal{A}_n^2).
 \end{aligned} \tag{4.34}$$

Initially, entanglement generation is continuously attempted with both neighbors simultaneously. This can be thought of as entanglement being created on one side with rate R_+ and with rate R_- on the other side, resulting in a “total rate” at which entanglement is produced at this node of

$$R_{\text{sum}} = R_+ + R_- = 2 \frac{c e^{-\frac{L_{\text{tot}}}{2L_{\text{att}}}}}{L_{\text{tot}}} + \mathcal{O}(\mathcal{A}_n^2). \tag{4.35}$$

Abusively treating the time required to generate entanglement on either side as being exponentially distributed (while they are really geometrically distributed), we then have that the time required until the first entangled state is created takes time $1/R_{\text{sum}}$. This time is invariant with respect to the node asymmetry parameter at first order.

Before entanglement swapping can take place, the second entangled state still needs to be generated. Now, entangling attempts are only made on one side, and therefore the “total rate” is no longer R_{sum} but only R_+ or R_- , depending on with which of the two neighbors entanglement has been established already. The probability that the longer link is generated first (once more treating the times required to generate entanglement as being exponentially distributed) is given by R_+/R_{sum} , in which case it on average still takes a time $1/R_-$ to generate the second entangled state. Similarly, with probability R_-/R_{sum} it still takes a time $1/R_+$. Therefore, the average time until entanglement is swapped at repeater n is

$$\begin{aligned}
 T_{\text{swap}} &= \frac{1}{R_{\text{sum}}} \left(1 + \frac{R_+}{R_-} + \frac{R_-}{R_+}\right) \\
 &= \frac{3}{2} \frac{c e^{-\frac{L_{\text{tot}}}{2L_{\text{att}}}}}{L_{\text{tot}}} + \mathcal{O}(\mathcal{A}_n^2),
 \end{aligned} \tag{4.36}$$

which is just the well-known “three-over-two” approximation for symmetric repeaters [79, 80]. Furthermore, the average time during which the first entangled state is stored in quantum memory is then given by $T_{\text{swap}} - 1/R_{\text{sum}}$, which also does not contain any linear terms in \mathcal{A}_n . This is consistent with the fact that not only the generation duration of the repeater chain appears to be independent of the chain asymmetry parameter to linear order, but also the QBER.

While the above argument can help understand why the performance of the repeater chain studied here has a vanishing first derivative with respect to the asymmetry parameter, we stress that it is not a complete or accurate treatment. For one, we have approximated geometrically-distributed random variables as being exponentially distributed. Moreover, we neglected the fact that in order to calculate the QBER we would need to calculate the expected value of the exponential function occurring in Equation (4.33), which

is not the same as the exponential function evaluated at the expected value. But perhaps most importantly, the different repeaters cannot be considered in isolation. After the repeater has performed entanglement swapping, it can only start entanglement generation again with neighbors that have themselves also performed entanglement swapping (otherwise their qubit is still occupied). This complex interdependence is one of the main reasons why we have turned to numerical simulations here.

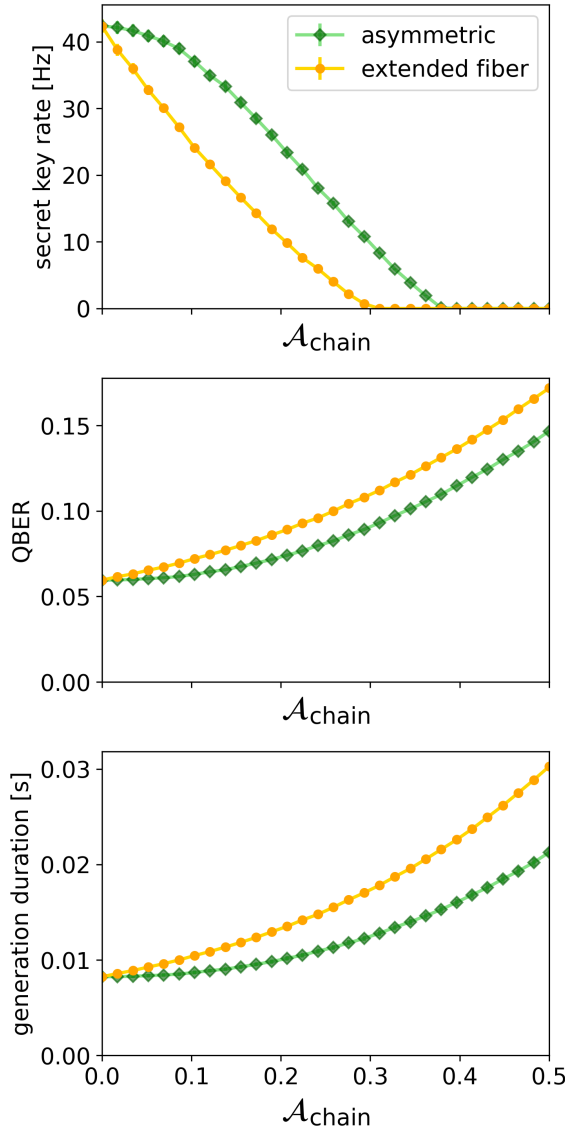


Figure 4.6: Effect of the chain asymmetry parameter $\mathcal{A}_{\text{chain}}$ in a repeater chain of the type illustrated in Figure 4.5 on the asymptotic secret-key rate of entanglement-based BB84. Additionally, the QBER and average entanglement-generation duration are shown, from which the secret-key rate is derived according to Equation (4.27). When using the “extended-fiber method”, spooled fiber is deployed to make all links in the network equally long, resulting in an effectively symmetric network with an increased total fiber length. The total length of the repeater chain considered here is 1000 km and it contains 21 nodes (including 2 end nodes). Depolarizing memory decoherence (see Equation (4.33)) with a coherence time of $T_{\text{coh}} = 1\text{ s}$ is the only source of noise included. Error bars represent the standard error in the estimates and are smaller than the marker size. Each data point is based on 20,000 simulated end-to-end entangled states.

4.3 Conclusion

We have investigated how the asymmetric placement of nodes in a quantum network can affect network performance. Specifically, we have studied the effect of asymmetric midpoint placement on heralded entanglement generation and of asymmetric repeater placement on SWAP-ASAP repeater chains in which repeaters can generate entanglement with both neighboring nodes in parallel. In both cases we have observed a remarkable resilience against small amounts of asymmetry, even though performance can be expected to degrade significantly as asymmetry is increased further. While for the midpoint placement the cycle time will be directly affected when asymmetry is introduced, the success probability and fidelity have a vanishing first derivative. Similarly, for repeater chains, both the generation duration and QBER appear to have vanishing first derivatives with respect to asymmetry in repeater placement. Whether the first derivatives also vanish for repeater chains in which parallel entanglement generation is not possible remains an open question. The same is true for repeater chains that do not execute a SWAP-ASAP protocol but instead, for example, execute a protocol that includes entanglement distillation.

We have also observed that asymmetry in midpoint placement can significantly affect the indistinguishability of photons used in heralded entanglement generation because of chromatic dispersion. Chromatic dispersion can potentially cause a bad fidelity even for small amounts of asymmetry. The size of the effect, however, depends on the temporal length of the photons, and we have found that as long as the photons are long enough (on the order of nanoseconds) the effect of chromatic dispersion can be negligible even for large asymmetries (percent level for an asymmetry of 40 km, see Figure 4.3). We have furthermore found that Gaussian wave packets are much more resilient against chromatic dispersion than Lorentzian wave packets which have long tails in their frequency distribution. By making the shape of a wave packet to be more Gaussian than Lorentzian (e.g., by filtering out long tails), the effects of chromatic dispersion can be mitigated.

From all this, we conclude that while asymmetry degrades quantum-network performance and should therefore be avoided where possible, small amounts of asymmetry are not expected to have a large effect. This may alleviate some of the pressure in selecting the perfect locations for nodes in a quantum network, and makes it more plausible that existing fiber infrastructure can provide fertile ground for a future quantum internet.

4.4 Code availability

The code that was used to perform the simulations and generate the plots in this chapter has been made available at <https://gitlab.com/GuusAvis/reproduction-code-for-asymmetric-node-placement-in-fiber-based-quantum-networks> [78].

4.5 Single-click and double-click expressions

In this section we derive the success probability and fidelity of the single- and double-click protocols in terms of the parameter ΔL (to first order). These derivations are based on the expressions given in Sections 3.10 and 3.8. For both protocols, our derivation hinges on having a set of probabilities $\{p_i\}$ and a set of states $\{\rho_i\}$ such that

$$P_{\text{succ}} = \sum_i p_i \quad (4.37)$$

is the success probability and

$$\rho = \frac{1}{P_{\text{succ}}} \sum_i p_i \rho_i \quad (4.38)$$

is the mixed state upon success. The fidelity can then be written as

$$F = \frac{1}{P_{\text{succ}}} \sum_i p_i F_i \quad (4.39)$$

where F_i is the fidelity corresponding to ρ_i . p_i and F_i depend on P_{left} and P_{right} , which we then rewrite in terms of $P_{\text{tot}} = P_{\text{left}} + P_{\text{right}}$ and $P_{\text{sum}} = P_{\text{left}} + P_{\text{right}}$ (see Equation (4.6)).

4.5.1 Double click

For the double-click protocol we have, using the results from Section 3.8,

$$\begin{aligned} p_T &= \frac{1}{2} P_{\text{tot}} V (1 - p_{\text{dc}}^{2r}), \\ p_{F_1} &= \frac{1}{2} P_{\text{tot}} (1 - V) (1 - p_{\text{dc}}^{2r}), \\ p_{F_2} &= \frac{2-r}{2} P_{\text{tot}} (1 + V) p_{\text{dc}} (1 - p_{\text{dc}})^{r+1}, \\ p_{F_3} &= 2(P_{\text{sum}} - 2P_{\text{tot}}) p_{\text{dc}} (1 - p_{\text{dc}})^{r+1}, \\ p_{F_4} &= 4(1 - P_{\text{sum}} + P_{\text{tot}}) p_{\text{dc}}^2 (1 - p_{\text{dc}})^2, \end{aligned} \quad (4.40)$$

such that we have the sets $\{p_i\}$, $\{\rho_i\}$ and $\{F_i\}$ with $p_1 = q_{\text{em}} p_T$, $\rho_1 = |\Psi^\pm\rangle\langle\Psi^\pm|$ (where $|\Psi^\pm\rangle = \frac{1}{2}(|01\rangle \pm |10\rangle)$ is the target Bell state, with the sign depending on which detector clicked), $F_1 = 1$, $p_2 = q_{\text{em}} p_{F_1}$, $\rho_2 = \frac{1}{2}(|01\rangle\langle 01| + |10\rangle\langle 10|)$, $F_2 = \frac{1}{2}$, $p_3 = q_{\text{em}} p_{F_2}$, $\rho_3 = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)$, $F_3 = 0$, $p_4 = (1 - q_{\text{em}})(p_T + p_{F_1} + p_{F_2}) + p_{F_3} + p_{F_4}$, $\rho_4 = \frac{1}{4}$, and $F_4 = \frac{1}{4}$. From this, it follows that we can write

$$\begin{aligned} P_{\text{succ}} &= a + b P_{\text{sum}}, \\ F &= \frac{c + \frac{1}{4} b P_{\text{sum}}}{a + b P_{\text{sum}}}, \end{aligned} \quad (4.41)$$

with

$$\begin{aligned} a &= \frac{1}{2} P_{\text{tot}} (1 - p_{\text{dc}})^{2r} + p_{\text{dc}} P_{\text{tot}} (1 - p_{\text{dc}})^{r+1} \left[\frac{2-r}{2} (1 + V) - 4 \right] + 4 p_{\text{dc}}^2 (1 + P_{\text{tot}}) (1 - p_{\text{dc}})^2, \\ b &= 2 p_{\text{dc}} (1 - p_{\text{dc}})^{r+1} - 4 p_{\text{dc}}^2 (1 - p_{\text{dc}})^2, \\ c &= \frac{1}{4} q_{\text{em}} P_{\text{tot}} (1 + V) (1 - p_{\text{dc}})^{2r} + (1 - q_{\text{em}}) \left(\frac{1}{8} P_{\text{tot}} (1 - p_{\text{dc}})^{2r} + \frac{2-r}{8} p_{\text{dc}} (1 - p_{\text{dc}})^2 P_{\text{tot}} (1 + V) \right) \\ &\quad - p_{\text{dc}} P_{\text{tot}} (1 - p_{\text{dc}})^{r+1} + p_{\text{dc}}^2 (1 + P_{\text{tot}}) (1 - p_{\text{dc}})^2. \end{aligned} \quad (4.42)$$

Taking a first-order expansion in p_{dc} of the success probability and the fidelity gives the double-click results presented in Section 4.1.2.

4.5.2 Single click

For the single-click protocol we can rewrite the expressions in Section 3.8 by substituting the bright-state parameters by q (see Equation (4.12)) such that we have the sets $\{p_i\}$, $\{\rho_i\}$ and $\{F_i\}$ with

$$\begin{aligned}
 p_1 &= \frac{q^2}{P_{\text{tot}}} (1 - p_{\text{dc}}) \left\{ 2p_{\text{dc}} + P_{\text{tot}} \left(-2(1 - p_{\text{dc}})^{r-1} + 2p_{\text{dc}} + \frac{1}{2}(2 - r)(1 + V) \right) \right\} \\
 &\quad + q^2 \frac{P_{\text{sum}}}{P_{\text{tot}}} \left((1 - p_{\text{dc}})^r - 2p_{\text{dc}}(1 - p_{\text{dc}}) \right) \\
 p_2 &= t_1 + t_2, \\
 t_1 &= q \left(1 - q \frac{P_{\text{left}}}{P_{\text{tot}}} \right) \left\{ (1 - p_{\text{dc}})^r + 2 \left(\frac{P_{\text{right}}}{P_{\text{tot}}} - q \right) (1 - p_{\text{dc}}) p_{\text{dc}} \right\}, \\
 t_2 &= q \left(1 - q \frac{P_{\text{right}}}{P_{\text{tot}}} \right) \left\{ (1 - p_{\text{dc}})^r + 2 \left(\frac{P_{\text{left}}}{P_{\text{tot}}} - q \right) (1 - p_{\text{dc}}) p_{\text{dc}} \right\}, \\
 p_3 &= 2p_{\text{dc}}(1 - p_{\text{dc}}) \left(1 + \frac{q^2}{P_{\text{tot}}} - q \frac{P_{\text{sum}}}{P_{\text{tot}}} \right)
 \end{aligned} \tag{4.43}$$

$$\rho_1 = |00\rangle\langle 00|, \rho_3 = |11\rangle\langle 11|, F_1 = F_3 = 0,$$

$$\begin{aligned}
 \rho_2 &= \frac{1}{p_2} \left(t_1 |01\rangle\langle 01| + t_2 |10\rangle\langle 10| \pm \sqrt{V t_1 t_2} (|01\rangle\langle 01| + |10\rangle\langle 10|) \right), \\
 F_2 &= \frac{1}{2} + \sqrt{V} \frac{\sqrt{t_1 t_2}}{p_2}.
 \end{aligned} \tag{4.44}$$

We note that while P_{left} and P_{right} cannot be eliminated in favor of P_{sum} and P_{tot} in the expressions for t_1 and t_2 , they can be eliminated in $p_2 = t_1 + t_2$, giving

$$\begin{aligned}
 p_2 &= 2q(1 - p_{\text{dc}})^r - 4qp_{\text{dc}}(1 - p_{\text{dc}}) \left(1 + \frac{q}{P_{\text{tot}}} \right) \\
 &\quad + \frac{P_{\text{sum}}}{P_{\text{tot}}} q \left(2p_{\text{dc}}(1 - p_{\text{dc}}) - q \left\{ (1 - p_{\text{dc}})^r - 2(1 - p_{\text{dc}}) p_{\text{dc}} \right\} \right)
 \end{aligned} \tag{4.45}$$

The success probability is then given by

$$P_{\text{succ}} = p_1 + p_2 + p_3. \tag{4.46}$$

We refrain from writing out the exact success probability explicitly here, but note that it can be readily verified that the terms proportional to P_{sum} cancel out. Therefore, we conclude that the success probability is independent of P_{sum} , and hence the asymmetry. To leading order we have $p_1 = 0$, $p_2 = 2q$ and $p_3 = 2p_{\text{dc}}$, and by adding these up the leading-order result for the success probability in Equations (4.13) is found.

As both F_1 and F_3 are zero, the fidelity is given by

$$F = \frac{p_2}{P_{\text{succ}}} F_2 = \frac{1}{2} \frac{p_2}{P_{\text{succ}}} + \sqrt{V} \frac{\sqrt{t_1 t_2}}{P_{\text{succ}}}. \tag{4.47}$$

The product $t_1 t_2$ cannot be written in terms of solely P_{tot} and P_{sum} instead of P_{left} and P_{right} . However, the troublesome terms in this product are higher order. Therefore, we can eliminate P_{left} and P_{right} from F as long as we stick to leading order. Here, we consider both q and p_{dc} to be of the same order, i.e., $p_{\text{dc}} = \mathcal{O}(q)$. We note that under realistic settings $p_{\text{dc}} < q$ as otherwise more successes would be caused by dark counts than by actual photons, which is a regime in which no useful entanglement can be created. Evaluating F at leading order requires evaluating p_2 , P_{succ} and $\sqrt{t_1 t_2}$ up to second order, giving

$$\begin{aligned} p_2 &= 2q \left(1 - (2+r)p_{\text{dc}} + \frac{P_{\text{sum}}}{P_{\text{tot}}} \left(p_{\text{dc}} - \frac{1}{2}q \right) \right) + \mathcal{O}(q^3), \\ P_{\text{succ}} &= 2(q + p_{\text{dc}}) \left(1 - q - p_{\text{dc}} + \frac{q}{q + p_{\text{dc}}} \left[\frac{1}{4}(2-r)(1+V)q - 2p_{\text{dc}} \right] \right) + \mathcal{O}(q^3), \\ \sqrt{t_1 t_2} &= q \left(1 - (2+r)p_{\text{dc}} - \frac{1}{2}(q - 2p_{\text{dc}}) \frac{P_{\text{sum}}}{P_{\text{tot}}} \right) + \mathcal{O}(q^3). \end{aligned} \quad (4.48)$$

The leading-order expression for the fidelity given in Equation (4.13) can now be obtained by substituting these quantities into the equation for the fidelity above and disregarding higher-order terms.

4.6 Calculating photon indistinguishability

In this section we derive the formulas for indistinguishability of Gaussian and Lorentzian photons presented in the main text.

4.6.1 Gaussian

For the Gaussian wave packets given in Equation (4.20), μ as defined in Equation (4.19) becomes

$$\mu = \frac{1}{\sqrt{2\pi}} e^{-\left(\frac{\delta\omega}{\sigma}\right)^2} \int dx \exp \left(i\delta t \sigma x - \frac{1}{2} [1 - i\Delta L \beta_2 \sigma^2] x^2 + \frac{1}{6} i\Delta L \beta_3 \sigma^3 x^3 \right). \quad (4.49)$$

By Taylor expanding in the TOD parameter β_3 we can rewrite this as

$$\mu = \frac{1}{\sqrt{2\pi}} e^{-\left(\frac{\delta\omega}{\sigma}\right)^2} \sum_{n=0}^{\infty} \frac{i^n (\Delta L \beta_3 \sigma^3)^n}{n! 6^n} \int dx x^{3n} \exp \left(i\delta t \sigma x - \frac{1}{2} [1 - i\Delta L \beta_2 \sigma^2] x^2 \right). \quad (4.50)$$

This allows us to evaluate the indistinguishability at different orders of $\Delta L \beta_3 \sigma^3$ by evaluating the moments of a Gaussian distribution. The $n=0$ term, which corresponds to $\beta_3=0$, is a simple Gaussian integral for which it holds that

$$\int_{-\infty}^{\infty} e^{-ax^2+bx+c} dx = e^{\frac{b^2}{4a}+c} \sqrt{\frac{\pi}{a}}. \quad (4.51)$$

Therefore,

$$\mu|_{\beta_3=0} = e^{-\left(\frac{\delta\omega}{\sigma}\right)^2} \frac{1}{\sqrt{1 - i\Delta L \beta_2 \sigma^2}} e^{-\frac{(\sigma\delta t)^2}{2(1 - i\Delta L \beta_2 \sigma^2)}}. \quad (4.52)$$

The result in Equation (4.21) is then obtained through

$$V|_{\beta_3=0} = |\mu|_{\beta_3=0}|^2. \quad (4.53)$$

To evaluate higher-order terms one can use

$$\int_{-\infty}^{\infty} x^n e^{-ax^2+bx+c} dx = e^{\frac{b^2}{2a}+c} \sqrt{\frac{\pi}{a}} \left[\left(\frac{b}{2a} \right)^n + \sum_{j=1}^{\lfloor \frac{n}{2} \rfloor} \binom{2j}{n} \left(\frac{b}{2a} \right)^{n-2j} \frac{(2j-1)!!}{(2a)^j} \right]. \quad (4.54)$$

In fact, this allows for determining the indistinguishability to arbitrary order in the TOD. Here, we only calculate the first order. By recognizing that the expression before the square brackets in the equation above is equation to the result of the regular Gaussian integral, we can then write

$$\mu = \mu|_{\beta_3=0} (1 + iA\Delta L\beta_3\sigma^3) + \mathcal{O}((\Delta L\beta_3\sigma^3)^2) \quad (4.55)$$

with

$$A = \frac{(i\delta t\sigma)^3 + 3i\delta t\sigma(1 - i\Delta L\beta_2\sigma^2)}{6(1 - i\Delta L\beta_2\sigma^2)^3}. \quad (4.56)$$

We then find

$$V = |\mu|^2 = V|_{\beta_3=0} (1 + 2\Delta L\beta_3\sigma^3 \text{Re}(iA)) + \mathcal{O}((\Delta L\beta_3\sigma^3)^2). \quad (4.57)$$

Evaluating this expression yields

$$V = V|_{\beta_3=0} \left[1 - \frac{\Delta L\beta_3\delta t\sigma^4}{(1 + \Delta L^2\beta_2^2\sigma^4)^2} \times \left(1 - 3\Delta L^2\beta_2^2\sigma^4 - \frac{\delta t^2\sigma^2(1 - \Delta L^2\beta_2^2\sigma^4)^2}{3(1 + \Delta L^2\beta_2^2\sigma^4)} \right) \right] + \mathcal{O}(\Delta L^2\beta_3^2\sigma^6). \quad (4.58)$$

Collecting the higher-order terms gives Equation (4.23).

4.6.2 Lorentzian

Using the Lorentzian wave forms defined in Equation (4.24) for $\delta\omega = \delta t = \beta_3 = 0$ we find

$$\mu = \frac{1}{\pi} \int_{-\infty}^{\infty} dx \frac{e^{\pm icx^2}}{1 + x^2} \quad (4.59)$$

where $\pm c = \frac{1}{2}\Delta L\beta_2\tau^{-2}$ and $c > 0$ is a real number (the sign \pm is the sign of $\Delta L\beta_2$). We rewrite this as

$$\mu = e^{\pm ic} I(\pm ic) \quad (4.60)$$

with

$$I(y) = \int_{-\infty}^{\infty} dx \frac{e^{-y(1+x^2)}}{1 + x^2}. \quad (4.61)$$

We can evaluate this integral by first differentiating it and then integrating it again. By the fundamental theorem of calculus, it holds that

$$I(y) = I(0) + \int_0^y \frac{dI(z)}{dz} dz. \quad (4.62)$$

Both terms are readily evaluated;

$$I(0) = \int_{-\infty}^{\infty} \frac{dx}{1+x^2} = \text{atan}(x)|_{-\infty}^{\infty} = \pi, \quad (4.63)$$

$$\begin{aligned} \int_0^y \frac{dI(z)}{dz} dz &= \int_0^y dz \int_{-\infty}^{\infty} -e^{-z(1+x^2)} dx \\ &= \int_0^y dz e^z \sqrt{\frac{\pi}{z}} \\ &= -2\sqrt{\pi} \int_0^{\sqrt{y}} e^{-u^2} du \\ &= -\pi \text{erf} \sqrt{y}, \end{aligned} \quad (4.64)$$

where erf is the error function. Here we have assumed $\text{Re}(z) \geq 0$ so that we could use Equation (4.51) (which is equivalent to assuming $\text{Re}(y) \geq 0$) and we made a change of variables $u = \sqrt{y}$, where \sqrt{y} is taken to mean the principal root of y . Therefore, we have (for $\text{Re}(y) \geq 0$)

$$I(y) = \pi(1 - \text{erf} \sqrt{y}). \quad (4.65)$$

In order to evaluate μ we need to evaluate the error function for a purely imaginary value. In that case we can rewrite

$$\int_0^{\sqrt{\pm ic}} e^{-u^2} du = \sqrt{\pm i} \int_0^{\sqrt{c}} e^{\mp iv^2} dv = \frac{1}{\sqrt{2}} ((1 \pm i)C(\sqrt{c}) + (1 \mp i)S(\sqrt{c})). \quad (4.66)$$

Here we made the change of variable $u = \sqrt{\pm i}v$ and we have introduced the Fresnel integrals $C(x) = \int_0^x \cos(t^2)dt$ and $S(x) = \int_0^x \sin(t^2)dt$. Therefore, we have

$$I(\pm ic) = \pi - \sqrt{2\pi} ((1 \pm i)C(\sqrt{c}) + (1 \mp i)S(\sqrt{c})). \quad (4.67)$$

We can then find the indistinguishability as given in Equation (4.26) as

$$V = |\mu|^2 = |I(\pm ic)|^2. \quad (4.68)$$

References

- [1] C. Cabrillo, J. I. Cirac, P. García-Fernández, and P. Zoller, *Creation of entangled states of distant atoms by interference*, Phys. Rev. A **59**, 1025 (1999).
- [2] S. D. Barrett and P. Kok, *Efficient high-fidelity quantum computation using matter qubits and linear optics*, Phys. Rev. A **71**, 060310 (2005).

- [3] S. Pirandola, *End-to-end capacities of a quantum communication network*, Commun Phys **2**, 1 (2019).
- [4] L. Jiang, J. M. Taylor, N. Khaneja, and M. D. Lukin, *Optimal approach to quantum communication using dynamic programming*, Proceedings of the National Academy of Sciences **104**, 17291 (2007).
- [5] D. Luong, L. Jiang, J. Kim, and N. Lütkenhaus, *Overcoming lossy channel bounds using a single quantum repeater node*, Appl. Phys. B **122**, 96 (2016).
- [6] F. Rozpędek, K. Goodenough, J. Ribeiro, N. Kalb, V. C. Vivoli, A. Reiserer, R. Hanson, S. Wehner, and D. Elkouss, *Parameter regimes for a single sequential quantum repeater*, Quantum Sci. Technol. **3**, 034002 (2018).
- [7] T. Coopmans, R. Knegjens, A. Dahlberg, D. Maier, L. Nijsten, J. de Oliveira Filho, M. Papendrecht, J. Rabbie, F. Rozpędek, M. Skrzypczyk, L. Wubben, W. de Jong, D. Podareanu, A. Torres-Knoop, D. Elkouss, and S. Wehner, *NetSquid, a NETwork Simulator for QUantum Information using Discrete events*, Commun Phys **4**, 1 (2021).
- [8] Á. G. Iñesta, G. Vardoyan, L. Scavuzzo, and S. Wehner, *Optimal entanglement distribution policies in homogeneous repeater chains with cutoffs*, npj Quantum Information **9**, 1 (2023).
- [9] P. C. Humphreys, N. Kalb, J. P. J. Morits, R. N. Schouten, R. F. L. Vermeulen, D. J. Twitchen, M. Markham, and R. Hanson, *Deterministic delivery of remote entanglement on a quantum network*, Nature **558**, 268 (2018), 1712.07567 .
- [10] M. Pompili, S. L. N. Hermans, S. Baier, H. K. C. Beukers, P. C. Humphreys, R. N. Schouten, R. F. L. Vermeulen, M. J. Tiggeleman, L. dos Santos Martins, B. Dirkse, S. Wehner, and R. Hanson, *Realization of a multinode quantum network of remote solid-state qubits*, Science **372**, 259 (2021).
- [11] H. Bernien, B. Hensen, W. Pfaff, G. Koolstra, M. S. Blok, L. Robledo, T. H. Taminiau, M. Markham, D. J. Twitchen, L. Childress, and R. Hanson, *Heralded entanglement between solid-state qubits separated by three metres*, Nature **497**, 86 (2013).
- [12] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, *Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres*, Nature **526**, 682 (2015).
- [13] L. J. Stephenson, D. P. Nadlinger, B. C. Nichol, S. An, P. Drmota, T. G. Ballance, K. Thirumalai, J. F. Goodwin, D. M. Lucas, and C. J. Ballance, *High-Rate, High-Fidelity Entanglement of Qubits Across an Elementary Quantum Network*, Phys. Rev. Lett. **124**, 110501 (2020).
- [14] V. Krutyanskiy, M. Galli, V. Krcmarsky, S. Baier, D. A. Fioretto, Y. Pu, A. Mazloom, P. Sekatski, M. Canteri, M. Teller, J. Schupp, J. Bate, M. Meraner, N. Sangouard, B. P. Lanyon, and T. E. Northup, *Entanglement of trapped-ion qubits separated by 230 meters*, Phys. Rev. Lett. **130**, 050803 (2023).

- [15] L. Childress, J. M. Taylor, A. S. Sørensen, and M. D. Lukin, *Fault-tolerant quantum repeaters with minimal physical resources and implementations based on single-photon emitters*, Phys. Rev. A **72**, 052330 (2005).
- [16] Y.-R. Fan, C.-Z. Yuan, C.-Z. Yuan, R.-M. Zhang, S. Shen, P. Wu, H.-Q. Wang, H. Li, G.-W. Deng, H.-Z. Song, H.-Z. Song, L.-X. You, Z. Wang, Y. Wang, Y. Wang, G.-C. Guo, G.-C. Guo, Q. Zhou, Q. Zhou, and Q. Zhou, *Effect of dispersion on indistinguishability between single-photon wave-packets*, Photon. Res., PRJ **9**, 1134 (2021).
- [17] D.-G. Im, Y. Kim, and Y.-H. Kim, *Dispersion cancellation in a quantum interferometer with independent single photons*, Opt. Express, OE **29**, 2348 (2021).
- [18] F. Mitschke, *Fiber Optics: Physics and Technology* (Heidelberg ; New York, 2010).
- [19] T. Utsugi, A. Goban, Y. Tokunaga, H. Goto, and T. Aoki, *Gaussian wavepacket model for single-photon generation based on cavity QED in the adiabatic and nonadiabatic conditions*, Physical Review A **106**, 023712 (2022).
- [20] J.-F. Li, Y.-F. Wang, K.-Y. Su, K.-Y. Liao, S.-C. Zhang, H. Yan, and S.-L. Zhu, *Generation of Gaussian-Shape Single Photons for High Efficiency Quantum Storage**, Chinese Physics Letters **36**, 074202 (2019).
- [21] P. P. Rohde, T. C. Ralph, and M. A. Nielsen, *Optimal photons for quantum-information processing*, Phys. Rev. A **72**, 052332 (2005).
- [22] B. Kambs, *Quantum Frequency Conversion of Indistinguishable Photons from Independent Solid State Emitters*, doctoralThesis, Saarländische Universitäts- und Landesbibliothek (2019).
- [23] H. Vural, S. L. Portalupi, J. Maisch, S. Kern, J. H. Weber, M. Jetter, J. Wrachtrup, R. Löw, I. Gerhardt, and P. Michler, *Two-photon interference in an atom–quantum dot hybrid system*, Optica, OPTICA **5**, 367 (2018).
- [24] J. H. Weber, B. Kambs, J. Kettler, S. Kern, J. Maisch, H. Vural, M. Jetter, S. L. Portalupi, C. Becher, and P. Michler, *Two-photon interference in the telecom C-band after frequency conversion of photons from remote quantum emitters*, Nature Nanotech **14**, 23 (2019).
- [25] A. Stolk, K. L. van der Enden, M.-C. Roehsner, A. Teepe, S. O. J. Faes, S. Cadot, J. van Rantwijk, I. te Raa, R. Hagen, A. Verlaan, B. Biemond, A. Khorev, J. Morits, R. Vollmer, M. Markham, A. M. Edmonds, E. van Zwet, and R. Hanson, *Telecom-band quantum interference of frequency-converted photons from remote detuned NV centers*, PRX Quantum **3**, 020359 (2022).
- [26] *G.652 : Characteristics of a single-mode optical fibre and cable*, <https://www.itu.int/rec/T-REC-G.652> (2013).
- [27] M. B. Rota, T. M. Krieger, Q. Buchinger, M. Beccaceci, J. Neuwirth, H. Huet, N. Horová, G. Lovicu, G. Ronco, S. F. C. da Silva, G. Pettinari, M. Moczała-Dusanowska, C. Kohlberger, S. Manna, S. Stroj, J. Freund, X. Yuan, C. Schneider, M. Ježek, S. Höfling, F. B. Basset, T. Huber-Loyola, A. Rastelli, and R. Trotta, *A source*

of entangled photons based on a cavity-enhanced and strain-tuned GaAs quantum dot, (2022), arXiv:2212.12506 .

- [28] Y.-M. He, Y. He, Y.-J. Wei, D. Wu, M. Atatüre, C. Schneider, S. Höfling, M. Kamp, C.-Y. Lu, and J.-W. Pan, *On-demand semiconductor single-photon source with near-unity indistinguishability*, *Nature Nanotech* **8**, 213 (2013).
- [29] P. Schnauber, A. Singh, J. Schall, S. I. Park, J. D. Song, S. Rodt, K. Srinivasan, S. Reitzenstein, and M. Davanco, *Indistinguishable Photons from Deterministically Integrated Single Quantum Dots in Heterogeneous GaAs/Si₃N₄ Quantum Photonic Circuits*, *Nano Lett.* **19**, 7164 (2019).
- [30] M. L. Goldman, M. W. Doherty, A. Sipahigil, N. Y. Yao, S. D. Bennett, N. B. Manson, A. Kubanek, and M. D. Lukin, *State-selective intersystem crossing in nitrogen-vacancy centers*, *Phys. Rev. B* **91**, 165201 (2015).
- [31] N. Kalb, P. C. Humphreys, J. J. Slim, and R. Hanson, *Dephasing mechanisms of diamond-based nuclear-spin memories for quantum networks*, *Phys. Rev. A* **97**, 062330 (2018).
- [32] C. Crocker, M. Lichtman, K. Sosnova, A. Carter, S. Scarano, and C. Monroe, *High purity single photons entangled with an atomic qubit*, *Opt. Express*, OE **27**, 28143 (2019).
- [33] T. Chakraborty, H. van Brug, A. Das, O. Pietx-Casas, P.-C. Wang, G. C. do Amaral, A. L. Tchebotareva, and W. Tittel, *Frequency multiplexed photon pairs and detection for quantum repeaters*, (2022), arXiv:2205.10028 .
- [34] M. Businger, L. Nicolas, T. S. Mejia, A. Ferrier, P. Goldner, and M. Afzelius, *Non-classical correlations over 1250 modes between telecom photons and 979-nm photons stored in 171Yb³⁺:Y₂SiO₅*, *Nature Communications* **13**, 6438 (2022).
- [35] D. A. Fioretto, *Towards a Flexible Source for Indistinguishable Photons Based on Trapped Ions and Cavities*, Ph.D. thesis, Innsbruck (2020).
- [36] M. Keller, B. Lange, K. Hayasaka, W. Lange, and H. Walther, *Continuous generation of single photons with controlled waveform in an ion-trap cavity system*, *Nature* **431**, 1075 (2004).
- [37] E. N. Knall, C. M. Knaut, R. Bekenstein, D. R. Assumpcao, P. L. Stroganov, W. Gong, Y. Q. Huan, P.-J. Stas, B. Machielse, M. Chalupnik, D. Levonian, A. Suleymanzade, R. Riedinger, H. Park, M. Lončar, M. K. Bhaskar, and M. D. Lukin, *Efficient Source of Shaped Single Photons Based on an Integrated Diamond Nanophotonic System*, *Physical Review Letters* **129**, 053603 (2022).
- [38] O. Morin, M. Körber, S. Langenfeld, and G. Rempe, *Deterministic Shaping and Reshaping of Single-Photon Temporal Wave Functions*, *Phys. Rev. Lett.* **123**, 133602 (2019).
- [39] P. B. R. Nisbet-Jones, J. Dille, D. Ljunggren, and A. Kuhn, *Highly efficient source for indistinguishable single photons of controlled shape*, *New J. Phys.* **13**, 103036 (2011).

- [40] Y. Shi, S. Moe Thar, H. S. Poh, J. A. Grieve, C. Kurtsiefer, and A. Ling, *Stable polarization entanglement based quantum key distribution over a deployed metropolitan fiber*, Appl. Phys. Lett. **117**, 124002 (2020).
- [41] G.653: *Characteristics of a dispersion-shifted, single-mode optical fibre and cable*, <https://www.itu.int/rec/T-REC-G.653-201007-I/en> (2010).
- [42] S. Fasel, N. Gisin, G. Ribordy, and H. Zbinden, *Quantum key distribution over 30 km of standard fiber using energy-time entangled photon pairs: A comparison of two chromatic dispersion reduction methods*, Eur. Phys. J. D **30**, 143 (2004).
- [43] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, *Inside Quantum Repeaters*, IEEE Journal of Selected Topics in Quantum Electronics **21**, 78 (2015).
- [44] K. Azuma, S. E. Economou, D. Elkouss, P. Hilaire, L. Jiang, H.-K. Lo, and I. Tzitrin, *Quantum repeaters: From quantum networks to the quantum internet*, (2022), arXiv:2212.10820 .
- [45] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, Physical Review Letters **70**, 1895 (1993).
- [46] V. Krutyanskiy, M. Canteri, M. Meraner, J. Bate, V. Krcmarsky, J. Schupp, N. Sangouard, and B. P. Lanyon, *A telecom-wavelength quantum repeater node based on a trapped-ion processor*, (2023), arXiv:2210.05418 .
- [47] N. Sangouard, R. Dubessy, and C. Simon, *Quantum repeaters based on single trapped ions*, Physical Review A **79**, 042340 (2009).
- [48] S. Santra, S. Muralidharan, M. Lichtman, L. Jiang, C. Monroe, and V. S. Malinovsky, *Quantum repeaters based on two species trapped ions*, New Journal of Physics **21**, 073002 (2019), 1811.10723 .
- [49] P. Dhara, N. M. Linke, E. Waks, S. Guha, and K. P. Seshadreesan, *Multiplexed quantum repeaters based on dual-species trapped-ion systems*, Physical Review A **105**, 022623 (2022).
- [50] M. Ruf, N. H. Wan, H. Choi, D. Englund, and R. Hanson, *Quantum networks based on color centers in diamond*, Journal of Applied Physics **130**, 070901 (2021).
- [51] F. Rozpędek, R. Yehia, K. Goodenough, M. Ruf, P. C. Humphreys, R. Hanson, S. Wehner, and D. Elkouss, *Near-term quantum-repeater experiments with nitrogen-vacancy centers: Overcoming the limitations of direct transmission*, Physical Review A **99**, 052330 (2019).
- [52] S. Langenfeld, P. Thomas, O. Morin, and G. Rempe, *Quantum Repeater Node Demonstrating Unconditionally Secure Key Distribution*, Phys. Rev. Lett. **126**, 230506 (2021).
- [53] A. Reiserer and G. Rempe, *Cavity-based quantum networks with single atoms and optical photons*, Reviews of Modern Physics **87**, 1379 (2015).

- [54] G. Avis, F. F. da Silva, T. Coopmans, A. Dahlberg, H. Jirovská, D. Maier, J. Rabbie, A. Torres-Knoop, and S. Wehner, *Requirements for a processing-node quantum repeater on a real-world fiber grid*, (2022), arXiv:2207.10579 .
- [55] B. Li, T. Coopmans, and D. Elkouss, *Efficient Optimization of Cutoffs in Quantum Repeater Chains*, IEEE Transactions on Quantum Engineering **2**, 1 (2021).
- [56] S. Khatri, *Policies for elementary links in a quantum network*, Quantum **5**, 537 (2021).
- [57] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, *Mixed-state entanglement and quantum error correction*, Physical Review A **54**, 3824 (1996).
- [58] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, *Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels*, Physical Review Letters **76**, 722 (1996).
- [59] W. Dür and H. J. Briegel, *Entanglement purification and quantum error correction*, Reports on Progress in Physics **70**, 1381 (2007), 0705.4165 .
- [60] K. Goodenough, D. Elkouss, and S. Wehner, *Optimizing repeater schemes for the quantum internet*, Physical Review A **103**, 032610 (2021).
- [61] F. Rozpędek, T. Schiet, L. P. Thinh, D. Elkouss, A. C. Doherty, and S. Wehner, *Optimizing practical entanglement distillation*, Physical Review A **97**, 062333 (2018).
- [62] S. Krastanov, V. V. Albert, and L. Jiang, *Optimized Entanglement Purification*, Quantum **3**, 123 (2019).
- [63] S. Haldar, P. J. Barge, S. Khatri, and H. Lee, *Fast and reliable entanglement distribution with quantum repeaters: Principles for improving protocols using reinforcement learning*, (2023), arXiv:2303.00777 .
- [64] C. H. Bennett, G. Brassard, and N. D. Mermin, *Quantum cryptography without Bell's theorem*, Phys. Rev. Lett. **68**, 557 (1992).
- [65] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, Theoretical Computer Science Theoretical Aspects of Quantum Cryptography – Celebrating 30 Years of BB84, **560**, 7 (2014).
- [66] P. W. Shor and J. Preskill, *Simple Proof of Security of the BB84 Quantum Key Distribution Protocol*, Phys. Rev. Lett. **85**, 441 (2000).
- [67] M. K. Bhaskar, R. Riedinger, B. Machielse, D. S. Levonian, C. T. Nguyen, E. N. Knall, H. Park, D. Englund, M. Lončar, D. D. Sukachev, and M. D. Lukin, *Experimental demonstration of memory-enhanced quantum communication*, Nature **580**, 60 (2020).
- [68] S. Langenfeld, S. Welte, L. Hartung, S. Daiss, P. Thomas, O. Morin, E. Distant, and G. Rempe, *Quantum Teleportation between Remote Qubit Memories with Only a Single Photon as a Resource*, Phys. Rev. Lett. **126**, 130502 (2021), 2105.04338 .
- [69] G. W. Lin, X. B. Zou, X. M. Lin, and G. C. Guo, *Heralded quantum memory for single-photon polarization qubits*, EPL **86**, 30006 (2009).

- [70] C. E. Bradley, S. W. de Bone, P. F. W. Möller, S. Baier, M. J. Degen, S. J. H. Loenen, H. P. Bartling, M. Markham, D. J. Twitchen, R. Hanson, D. Elkouss, and T. H. Taminiau, *Robust quantum-network memory based on spin qubits in isotopically engineered diamond*, npj Quantum Inf **8**, 1 (2022).
- [71] *NetSquid-Magic*, <https://gitlab.com/softwarequtech/netsquid-snippets/netsquid-magic> (2022).
- [72] *NetSquid-NetConf*, <https://gitlab.com/softwarequtech/netsquid-snippets/netsquid-netconf> (2022).
- [73] *NetSquid-QRepChain*, <https://gitlab.com/softwarequtech/netsquid-snippets/netsquid-qrepchain> (2023).
- [74] *NetSquid-SimulationTools*, <https://gitlab.com/softwarequtech/netsquid-snippets/netsquid-simulationtools> (2022).
- [75] *NetSquid-Driver*, <https://gitlab.com/softwarequtech/netsquid-snippets/netsquid-driver> (2022).
- [76] *NetSquid-EntanglementTracker*, <https://gitlab.com/softwarequtech/netsquid-snippets/netsquid-entanglementtracker> (2022).
- [77] *NetSquid-PhysLayer*, <https://gitlab.com/softwarequtech/netsquid-snippets/netsquid-physlayer> (2022).
- [78] G. Avis, *Reproduction code for Asymmetric node placement in fiber-based quantum networks*, <https://gitlab.com/GuusAvis/reproduction-code-for-asymmetric-node-placement-in-fiber-based-quantum-networks>.
- [79] T. Coopmans, S. Brand, and D. Elkouss, *Improved analytical bounds on delivery times of long-distance entanglement*, Phys. Rev. A **105**, 012608 (2022).
- [80] L. Jiang, J. M. Taylor, and M. D. Lukin, *Fast and robust approach to long-distance quantum communication with atomic ensembles*, Phys. Rev. A **76**, 012301 (2007).

5

Requirements for upgrading trusted nodes to a repeater chain over 900 km of optical fiber

5

Guus Avis*, Francisco Ferreira da Silva*, Joshua A. Slater and Stephanie Wehner.

We perform a numerical study of the distribution of entanglement on a real-world fiber grid connecting the German cities of Bonn and Berlin. The connection is realized using a chain of processing-node quantum repeaters spanning roughly 900 kilometers. We investigate how minimal hardware requirements depend on the target application, as well as on the number of repeaters in the chain. We find that requirements for blind quantum computing are markedly different than those for quantum key distribution, with the required coherence time being around two and a half times larger for the former. Further, we observe a trade-off regarding how target secret-key rates are achieved when using different numbers of repeaters: comparatively low-quality entangled states generated at a high rate are preferred for higher numbers of repeaters, whereas comparatively high-quality states generated at a lower rate are favored for lower numbers of repeaters. To obtain our results we employ an extensive simulation framework implemented using NetSquid, a discrete-event simulator for quantum networks. These are combined with an optimization methodology based on genetic algorithms to determine minimal hardware requirements.

5.1 Introduction

In Chapter 3 we have determined hardware requirements for a single quantum repeater on a real-world fiber grid. In this chapter, we extend these results in a number of key ways. First, instead of only considering a single quantum repeater, we study chains of

*These authors contributed equally.

This chapter is based on the preprint arXiv:2303.03234.

up to seven processing-node quantum repeaters. We do so using a fiber grid that will be used to construct a trusted-node network; upgrading such a network (which can be used for QKD albeit without end-to-end security) by replacing trusted nodes by repeaters may prove a particularly natural way of realizing early quantum-repeater networks [1]. Second, we investigate how the requirements on the quantum hardware change depending on how many repeaters are placed in the network. Finally, we also address the question whether the required hardware quality depends on the application that needs to be executed. Specifically, we consider two applications: QKD and VBQC, as discussed in Section 2.3.

5.1.1 Setup

We consider the quantum-network path depicted in Figure 5.1, with two end nodes situated in Bonn and Berlin separated by 917.1 km of optical fiber corresponding to 214.7 dB of attenuation (at a telecom wavelength of 1550 nm). There are a total of sixteen locations be-

5

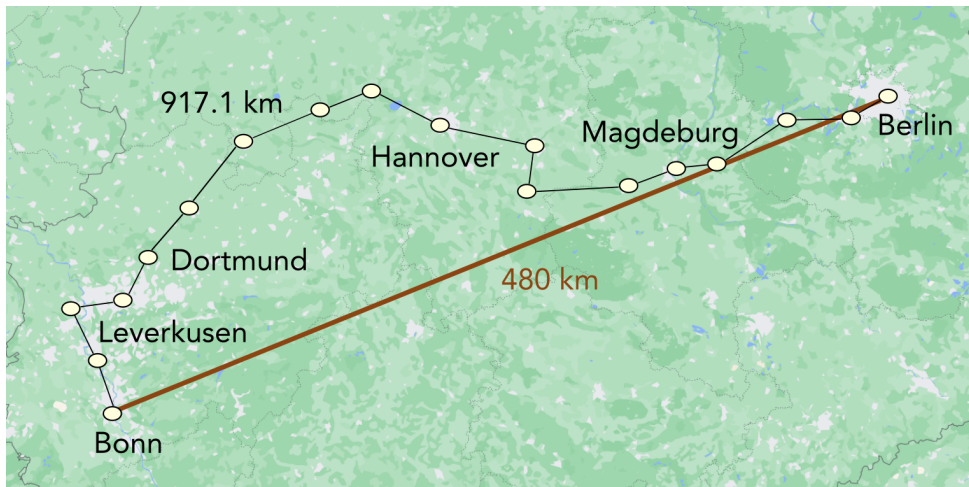


Figure 5.1: Map of Germany overlaid with a depiction of the fiber path connecting the German cities of Bonn and Berlin that we investigate, provided by Deutsche Telekom (DT). The white circles represent locations where DT plans to install trusted nodes and where, when building a repeater chain, processing nodes or heralding stations could be placed. These locations are connected to each other through fiber drawn in black. The maximum number of repeaters that can be placed between Bonn and Berlin in this fiber network is seven. We consider all possible repeater placements, assuming that the heralding stations are placed as symmetrically as possible (there are 986 such placements). The distance between Bonn and Berlin is 917.1 km via fiber, and approximately 480 km as the crow flies. The reason for such a large difference between the two values is that other major German cities, such as Hannover and Dortmund, are connected through the fiber link as well.

tween the end nodes where equipment can be placed, namely repeater nodes and heralding stations. Throughout this paper we assume that such a heralding station must be placed between every pair of neighboring network nodes (i.e., end nodes or repeater nodes), as these are required when entanglement is generated between those nodes through the interference and measurement of entangled photons [2–9]. This data has been provided to us by Deutsche Telekom (DT), Germany’s largest telecommunications provider, which plans to install trusted nodes in the locations depicted in Figure 5.1.

We assume neighboring nodes perform heralded entanglement generation [10, 11]. That is, entanglement consists of a series of attempts, and at the end of each attempt the partaking nodes learn whether an entangled state was successfully created or not. Examples of protocols for heralded entanglement generation are the double-click protocol [3, 6–9, 12], where photons are interfered and measured at a heralding station and success is declared in case two detectors click, the single-click protocol [2, 4, 5, 13, 14], where photons are also interfered but success is only declared in case one detector clicks, and direct transmission of an entangled photon from one node to the next where it is stored in heralded quantum memory [15–17]. Here, we employ a simplified model for heralded entanglement generation. We do this so that the protocol and its interplay with other components of the repeater chain can be readily understood and our modelling is not overly platform specific. First of all, we assume that each node can perform heralded entanglement generation with two neighbours in parallel, which is not currently possible for all quantum-repeater platforms [18]. Second, we model the elementary-link states ρ that are created upon the completion of a successful attempt as depolarized Bell states, i.e.,

$$\rho = W |\phi^+\rangle\langle\phi^+| + \frac{1-W}{4} \mathbb{1}, \quad (5.1)$$

where W is related to the fidelity F to the ideal Bell state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ as $F = (1+3W)/4$ and $\mathbb{1}$ is the four-dimensional identity matrix. We note that real entangled states generated in quantum-repeater chains are often not depolarized states [19] (see also Chapter 3). Yet, as depolarized Bell states represent a worst-case type of noise [20], using a depolarizing model ensures that we will not find hardware requirements that are artificially low due to this simplification. Third, we take the time t_{attempt} required to perform one attempt to be given by

$$t_{\text{attempt}} = \frac{L}{c}, \quad (5.2)$$

where L is the fiber distance between the two nodes and $c = 200,000$ km/s is the speed of light in fiber. That is, it corresponds to the communication time associated with sending photons to a heralding station that is exactly in the center between two nodes and then receiving a message with the measurement outcome. This is equivalent to the time required to directly transmit a photon from one node to the next. In reality it may be longer, as the attempt time could be further limited by the rate of the photon source, local operations or the synchronization of emission times [5, 21]. Finally, we take the success probability p_{el} of each attempt to be

$$p_{\text{el}} = p_{\text{det}} \times 10^{-\frac{\alpha_{\text{att}}}{10} L}. \quad (5.3)$$

Here, p_{det} is the probability that an emitted photon that is led through fiber to a detector is detected, given that it is not lost while travelling in fiber. This parameter combines multiple sources of loss, such as the detector's efficiency, the probability of emitting the photon in the right mode and the probability of successfully sending the photon into the fiber, but not the fiber's attenuation losses. α_{att} is the fiber's attenuation coefficient (in dB/km). Therefore, the success probability corresponds to the success probability of directly transmitting a photon between the nodes and measuring it there. We note that for the double-click protocol the scaling with length would be the same, although the prefactor would be different (p_{det}^2 instead of p_{det} , as two photons must be detected). For the

single-click protocol the scaling would be more gentle (roughly replacing L by $L/2$ in the exponential), and while the prefactor would be linear in p_{det} , there would also be a factor that depends on the device settings (specifically on the bright-state parameters chosen at both nodes, which tune a trade-off between success probability and state fidelity [5, 22]). Additionally, we allow also for the possibility of multiplexed heralded entanglement generation [23–25]. This essentially consists of performing multiple attempts of generating the same elementary-link state in parallel. Multiplexing can be done across multiple degrees of freedom, such as frequency, time or space. We remain agnostic regarding how the multiplexing is performed, including it in our model as one parameter corresponding to the number of multiplexing modes used, n . The probability of successfully generating an elementary link assuming the use of multiplexing is then the probability that at least one of the multiplexing modes succeeds:

$$p_{\text{multiple modes}} = 1 - (1 - p_{\text{el}})^n. \quad (5.4)$$

5

The nodes implement a swap-asap protocol [26, 27]. That is, as soon as a node holds two entangled states, one shared with each of its neighbours, it performs an entanglement swap in order to create an entangled state spanning a larger distance. We assume this swap is realized deterministically, since we are modelling processing nodes that can implement a swap using quantum gates and measurements on their processors. It may however introduce noise, which we model as depolarizing. We quantify how well the swap can be performed using the swap-quality parameter s_q . The d -dimensional depolarizing noise channel of parameter p acts on a state ρ as follows,

$$\rho \rightarrow p\rho + (1 - p)\frac{\mathbb{1}}{d}. \quad (5.5)$$

This means that, with probability p , ρ is left unchanged, and with probability $1 - p$ it is mapped to the maximally-mixed state, i.e., all information is lost. Then, we model entanglement swapping as a two-qubit depolarizing channel (i.e., $d = 4$) with parameter $p = s_q$ followed by a perfect entanglement-swapping operation (i.e., a measurement in the Bell basis [28]). We assume that the gates and measurements applied by the end nodes when executing QKD and VBQC are noiseless and instantaneous. States stored in memory undergo decoherence, which we model as exponential depolarizing noise, i.e.,

$$\rho \rightarrow e^{-t/T}\rho + (1 - e^{-t/T})\frac{\mathbb{1}}{d}, \quad (5.6)$$

where t is the time for which the state ρ has been held in memory and T is the memory's coherence time. To combat the effects of memory decoherence, entangled states are discarded after a local cut-off time. The cut-off time is defined as follows: a timer starts once a state is created in memory through the successful generation of an elementary link. If the timer reaches the local cut-off time, the state is discarded. That is, the qubit holding the state is reset. Additionally, the node sends a classical message along the chain so that the qubit with which the first qubit was entangled can also be reset. As a result, a number of elementary links in the chain must be regenerated (with the exact number depending on how far away the entangled qubit was).

5.1.2 Applications

Having discussed our modelling of the entanglement generation process between Bonn and Berlin, we turn to the applications that will make use of the entanglement, QKD and VBQC. We investigate the BB84 QKD protocol [29] (in its entanglement-based form [30]) between the end nodes situated in Bonn and Berlin. We record the entanglement generation rate and estimate the quantum bit error rate (QBER) that would have been obtained when measuring the generated state in order to estimate the achievable asymptotic secret-key rate (SKR) as per the following equation [31]:

$$\text{SKR} = E_R \cdot \max\left(0, (1 - 2H(Q))\right), \quad (5.7)$$

where E_R is the entanglement-generation rate, $H(p) = -p \log_2(p) - (1-p) \log_2(1-p)$ is the binary entropy function and Q is the QBER. We note that all the noise sources we consider are depolarizing, hence the entangled states generated will be of the form of the state shown in Equation 5.5. Therefore, the QBER is the same irrespective of the measurement basis. The end nodes do not wait until end-to-end entanglement is established before measuring their qubits. Instead, they measure them as soon as they have established entanglement with their nearest neighbours, as this minimizes the amount of time states spend in memory, resulting in laxer hardware requirements.

We also investigate a two-qubit version of the VBQC protocol introduced in [32]. In such protocols, a client wishes to delegate a computation to a powerful remote server in a secure and verifiable fashion [33]. In particular, we investigate the repeated execution of test rounds of the protocol, which consist of the server performing a controlled-Z gate followed by a measurement. In these rounds the client knows the computation's expected outcome, and can therefore compare them to the observed outcomes. Under the assumption of an honest server, wrong outcomes are a result of noise. We call this the *BQC test protocol*. The fraction of successful BQC test protocol rounds is therefore a metric for the quality of the entanglement used for transmitting qubits. We define the success rate as the number of rounds of the protocol that can be executed with a successful result per time unit. More concretely, if p_s is the success probability of a test round and R_{rounds} is the rate at which rounds can be executed, the BQC-test-protocol success rate is given by:

$$R_{\text{BQC}} = R_{\text{rounds}} \cdot p_s. \quad (5.8)$$

While the BQC test protocol is in and of itself not an interesting application of a quantum network, it can be considered a benchmark for how well the network is suited to VBQC and possibly other multi-qubit applications. The fact that, in contrast with QKD, it requires the distribution of multiple entangled states and the storage of qubits between rounds makes it a more meaningful benchmark for quantum-network applications that require multiple live qubits contemporaneously. Further details on the BQC test protocol can be found in Section 5.10.

The two applications we have just introduced define our performance targets.

5.1.3 Minimal hardware requirements

We wish to find the *minimal hardware requirements* that are needed to realize different target SKRs and BQC-test-protocol success rates. These correspond to the minimal improvements over state-of-the-art hardware parameters that enable meeting the targets.

We phrase the problem of finding minimal hardware requirements as a constrained optimization problem. Namely, we wish to minimize the hardware improvement while ensuring that the constraint induced by the performance target is met. This constraint is relaxed through a process known as scalarization [34, 35], resulting in a single-objective optimization problem, in which the quantity to be minimized is the sum of the cost associated to the hardware improvement and a penalty term for the rate target. The resulting cost function is given by:

$$C = w_1 \left(1 + (R_{target} - R_{real})\right)^2 \cdot \Theta(R_{target} - R_{real}) + w_2 H_C(x_1, \dots, x_N), \quad (5.9)$$

where H_C is the hardware improvement cost associated to parameter set $\{x_1, \dots, x_N\}$, w_i are the weights assigned to the objectives, Θ is the Heaviside step function, R_{target} is the rate target and R_{real} is the rate of application execution achieved by the parameter set. We note that R_{real} and R_{target} can be either a SKR or a BQC-test-protocol success rate. H_C maps sets of hardware parameters to a number, the cost, which represents how large of an improvement over the state-of-the-art they represent. In order to compute this cost consistently across different parameters, we use no-imperfection probabilities as done in Chapter 3. By no-imperfection probability, we mean the probability that there is no error or loss associated to a given parameter. For example, the no-error probability associated to a photon detection probability p_{det} (defined in Section 7.2) of 0.1 is 0.1. For the no-error probabilities associated to the other hardware parameters, see Section 5.9.1. We say that a parameter is improved by a factor of k if its no-imperfection probability becomes $\sqrt[k]{p_{ni}}$, with p_{ni} being the state-of-the-art no-imperfection probability. For example, improving the no-imperfection probability of 0.1 associated to $p_{det} = 0.1$ by a factor of 5, we get a no-imperfection probability of ≈ 0.63 , corresponding to $p_{det} \approx 0.63$. The hardware cost associated to a set of parameters is given by the sum of the improvement factors of the parameters. The weights w_i are chosen such that the term of the overall cost function corresponding to meeting the rate target is always larger than the one corresponding to the hardware cost, ensuring that even though we have relaxed the constraints by scalarizing, we are still effectively requiring that the minimal hardware requirements are such that the performance target is met. To ensure this, we picked $w_1, w_2 \gg w_3$, such that $w_1(1 + (R_{target} - R_{real})^2) \Theta(R_{target} - R_{real}) \gg w_2 H_C(x_1, \dots, x_N)$. Specifically, we set $w_1 = 1 \times 10^{100}$ and $w_2 = 1$. No particular heuristic was used to select these numbers.

We note that the hardware cost is meant only to represent a measure of the hardness of improving the hardware to a certain level, and not any form of monetary cost. At present quantum repeater systems are research setups, with commercial solutions only starting to emerge. Therefore, assigning any specific commercial cost numbers would be too speculative at this point, and would require an in-depth study outside the scope of this project.

5.1.4 State-of-the-art parameters

Computing minimal hardware requirements as described in Section 5.1.3 is done with respect to a baseline over which we are improving. In this work, this baseline consists of parameters measured for color centers in diamond, as they are physical systems using

which various quantum-networking primitives have been demonstrated. These include long-lived quantum memories [36], remote entanglement generation [6, 7], quantum teleportation [12], entanglement distillation [13], entanglement swapping [37] and a three-node network [5]. We do not impose that all parameters must have been demonstrated in the same experiment or even with the same color center. The parameters we consider are shown in Table 5.1. Details on how these parameters were determined can be found

Parameter	Value
Coherence time	1 s [38]
Number of multiplexing modes	1
Fidelity of elementary links	0.83 [7]
Photon detection probability	0.255 [15]
Swap quality	0.83 [13, 39]

Table 5.1: State-of-the-art color-center parameters. We note that not all of these parameter values have been realized in a single experiment. We have number of modes as 1 without reference because to the best of our knowledge multiplexed entanglement generation has not been demonstrated using color centers.

in Section 5.7.

5

5.1.5 Determining minimal hardware requirements

In order to determine minimal hardware requirements, we need to (i) be able to evaluate how a given set of hardware parameters performs and (ii) optimize over the parameter space to find the parameters that minimize the requirements while still performing adequately (i.e., the parameters that minimize the cost function defined in Equation (5.9)).

We evaluate the performance of hardware parameters using general processing-node repeater-chain simulations developed in NetSquid, a discrete-event based quantum-network simulator [26]. The simulations are general in the sense that they can be used to investigate swap-asap repeater chains of arbitrary size and spacing (i.e., nodes and heralding stations need not be equidistant). They take into account time-dependent noise, classical control communication and the constraints imposed by a real-world fiber network. The code for executing such simulations has been made publicly available at [40] and is largely based on the simulations presented in Chapter 3. Our code that utilizes these simulations to produce the results here presented can be found at [41] (and the corresponding data at [42]).

Given that we can evaluate the performance of any parameter set on the Bonn-Berlin path, we perform parameter optimization using a genetic algorithm [43] to minimize the cost function defined in Section 5.1.3 using the high-performance computing cluster Snelius. For further details, see Section 5.9.

5.2 Impact of number of repeaters on hardware requirements

In this section we answer the question of how hardware requirements are affected by the number of repeaters deployed in a quantum network. Specifically, we investigate the minimal hardware requirements for performing BB84 between the German cities of Bonn and Berlin at a key rate of 10 Hz. We assume the cities are connected by the network path

shown in Figure 5.1. We determine what these minimal requirements are in two cases: (i) optimizing over the number of repeaters and (ii) restricting the number of repeaters to specific values. In both cases we optimize over the placement of the repeaters.

5.2.1 Absolute minimal number of multiplexing modes

Before determining minimal requirements, we aim to answer the question of what are the absolute minimal number of multiplexing modes required to perform QKD between the German cities of Bonn and Berlin at rates of 1, 10 and 100 Hz. By *absolute minimal* number of multiplexing modes, we mean the minimum number of multiplexing modes that is required if the only source of imperfection in the setup is fiber attenuation. This provides a lower bound on the number of multiplexing modes in the minimal hardware requirements, as the introduction of other hardware imperfections can only lead to more stringent demands on the number of modes. We emphasize that for the purposes of answering this question we are temporarily setting aside the real-world fiber path introduced in Figure 5.1. Instead, we are going to consider a *symmetrized* version of that path. By this we mean a path with the same total length and attenuation, but in which nodes and heralding stations are placed equidistantly, and where the attenuation is evenly distributed throughout the path, i.e., all elementary links have the same attenuation. The reason for doing so is that the minimal number of modes for this path is a lower bound for the same quantity on any other path with the same total length and attenuation. To see this, we note that it has been shown in Chapter 4 that repeater chains of the type studied here perform best when all nodes are positioned as symmetrically as possible. This implies that such a chain will have less stringent hardware requirements to attain a given performance target in comparison to chains which are subject to real-world restrictions such as the ones imposed by the fiber path shown in Figure 5.1, and, therefore, also less stringent requirements on the number of multiplexing modes.

Determining the absolute minimal number of multiplexing modes serves two purposes. First, it allows us to limit the search space of the optimization we run for finding minimal hardware requirements. Second, it gives us a general idea of how many repeaters might be required to achieve the target with reasonable hardware demands. For example, if for a specific number of repeaters hundreds of thousands of multiplexing modes are required to meet the target without any noise sources, that may indicate that using that number of repeaters is not practically feasible.

In Figure 5.2 we show the absolute minimal number of modes required to distribute secret key at rates of 1, 10 and 100 Hz using BB84 in the symmetrized Bonn - Berlin path. We find that more multiplexing modes are required for higher rate targets, and that this number grows superexponentially as the number of repeaters decreases, so as to counteract the effects of photon loss in fiber. Further, we find that achieving a SKR of 10 Hz with fewer than 3 repeaters requires hundreds of thousands of multiplexing modes even in the absence of any sources of noise. As the hardware cost (defined in Section 5.1.3) associated with so many multiplexing modes far outweighs typical values for the minimal total hardware cost found for three or more repeaters we limit the rest of our investigation to configurations with three or more repeaters.

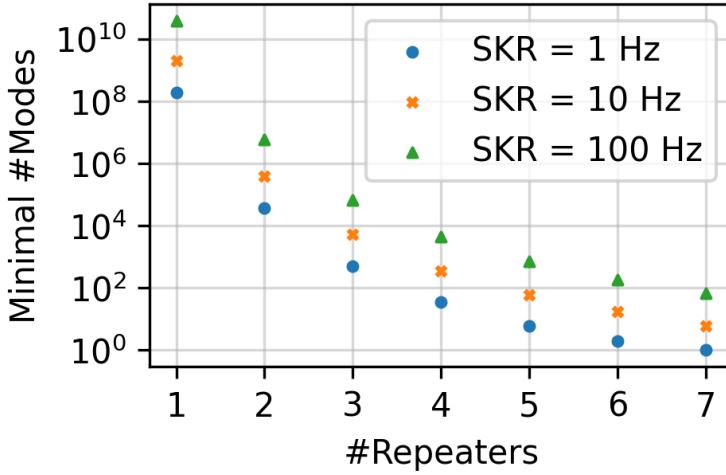


Figure 5.2: Minimal number of multiplexing modes required to achieve 1, 10 and 100 Hz of SKR over 917.1 km of fiber with a total of 214.7 dB of attenuation, corresponding to a symmetrized version of the path between Bonn and Berlin that we investigate. That is, for N repeaters, the symmetrized path has $N + 1$ elementary links, each of length $917.1/(N + 1)$ km and of attenuation $214.7/(N + 1)$ dB. We assume that there are no hardware imperfections, and that repeaters are uniformly spaced.

5.2.2 Minimal hardware requirements for quantum-key distribution

We now turn our attention to the minimal hardware requirements for performing quantum-key distribution at a rate of 10 Hz using the BB84 protocol. In particular, we investigate them along the path connecting Bonn and Berlin depicted in Figure 5.1. As Figure 5.2 illustrates, the number of repeaters used can have a considerable impact on the hardware requirements. Further, it is expected that the same is true for the placement of repeaters and heralding stations (see Chapters 3 and 4). With this in mind, we ask two questions: (i) what are the minimal hardware requirements when allowing for the placement of up to the largest number of repeaters that fits in the fiber path (seven) and (ii) what are the minimal hardware requirements when restricting the maximum number of repeaters to five. We expect that this will lead to different parameter regimes, illustrating two possible directions towards achieving the target performance.

In Figure 5.3 we show the directions along which hardware must be improved for distributing secret key at rates of 10 Hz using BB84 in the network path connecting Bonn and Berlin. The corresponding minimal hardware requirements can be found in Table 5.2. In each case we find that the hardware requirements are minimized when the number of repeaters used is maximized. That is, for seven repeaters in case (i) and five repeaters in case (ii). Hardware requirements are more stringent in case fewer repeaters are used. In particular, the overall photon detection probability excluding attenuation in fiber must be improved to a much larger degree (0.79 vs 0.36) if only five repeaters are used. This is needed to overcome the increased attenuation losses associated with the longer elementary links. The coherence time required when using five repeaters is also larger than the time required when using seven repeaters (4.2 s vs 3.1 s). This can be explained by the fact that keeping the entanglement-generation rate high is more costly in case of five repeaters.

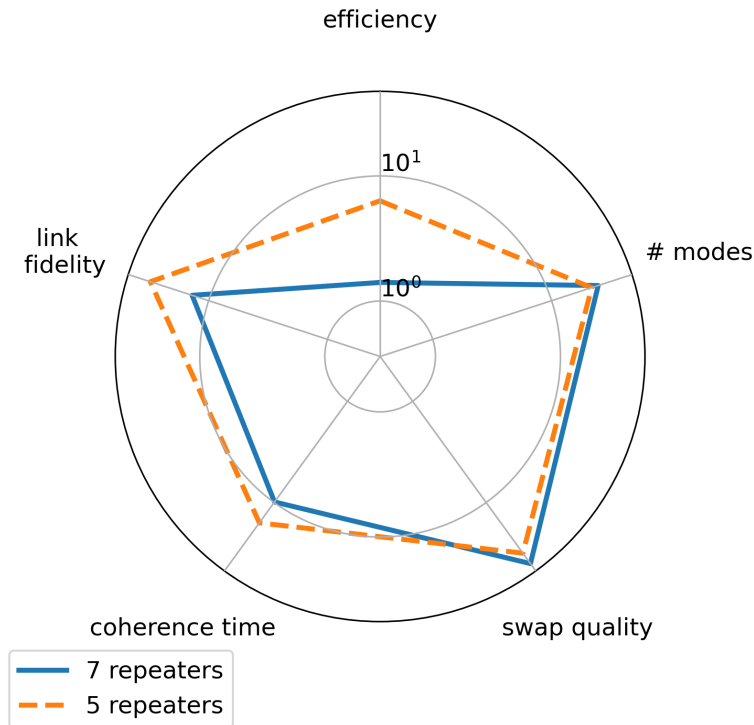


Figure 5.3: Directions along which hardware must be improved to enable attaining a secret-key rate of 10 Hz between the German cities of Bonn and Berlin. The blue (orange) line was obtained by performing an optimization in which the algorithm was allowed to use a maximum of seven (five) repeaters. The further away the line is from the center of the plot towards a given parameter, the more that parameter must be improved with respect to the current state-of-the-art. Improvement is depicted for the following parameters, clockwise from the top: overall photon detection probability excluding attenuation in fiber, number of multiplexing modes, fidelity of entanglement swap, coherence time of memory qubits and fidelity of elementary links. Note the use of a logarithmic scale.

Application	QKD				BQC
Rate (Hz)	1	10		100	10
Number of repeaters	7	Max 5	Max 7	7	7
Coherence time (s)	1.81	4.23	3.14	10.1	7.99
Number of multiplexing modes	175	544	592	799	172
Fidelity of elementary links	0.989	0.995	0.987	0.996	0.845
Photon detection probability p_{det}	0.604	0.785	0.360	0.804	0.552
Swap quality	0.996	0.996	0.997	0.997	0.881

Table 5.2: Minimal hardware requirements to achieve 1, 10 and 100 Hz of secret-key rate and 10 Hz of blind quantum computing test protocol success rate between the German cities of Bonn and Berlin. The photon detection probability p_{det} is the probability of a photon being detected given that it is not lost in fiber. It combines multiple sources of loss, such as the detector's efficiency, the probability of emitting the photon in the right mode and the probability of successfully sending the photon into the fiber. More details can be found in Section 7.2 and 5.7.

Therefore keeping the QBER small to extract as many secret bits as possible from each entangled state is more valuable. Furthermore, since the entanglement-generation rate is smaller for five repeaters, qubits are stored for longer times before they can be swapped and hence a larger coherence time is required to achieve the same QBER. We study this interplay further in Section 5.2.3. Finally, we notice that while the requirements on most hardware parameters are more stringent for five repeaters as compared to seven repeaters, this is not the case for the requirement on the swap quality. In fact, the requirement on the swap quality is even slightly looser for five repeaters (0.996 vs 0.997). This is explained by the fact that when there are more repeaters, there are more entanglement swaps associated with every end-to-end entangled state. Therefore, when there are more repeaters the final error rate is more sensitive to noise in the swaps, creating a larger incentive to improve the associated parameter in the seven-repeater case as compared to the five-repeater case.

5

5.2.3 Secret-key rate: quantum-bit error rate and entanglement generation rate

A specific value for the SKR can be obtained through many different pairs of values for the entanglement-generation rate and the QBER, as follows from Equation (5.7). This opens up a trade-off between the entanglement generation rate and the QBER, as briefly discussed in Section 5.2.2. Here, we investigate this trade-off more deeply by repeating our process for determining minimal hardware requirements to achieve an SKR of 10 Hz while keeping the number of repeaters a fixed parameter. We did this for 4, 5, 6 and 7 repeaters. For each case, we still optimize over all possible placements of the repeaters in the fiber grid. In Figure 5.4 we show the QBER and entanglement-generation rate achieved with the minimal hardware requirements for the best setup found by our optimization procedure for varying number of repeaters. We observe two different regimes. For 4 and 5 repeaters, which we name the ‘few-repeater’ regime, we find a low QBER ($\sim 5\%$) and an entanglement-generation rate of 20 - 30 Hz. On the other hand, for 6 and 7 repeaters, i.e., the ‘many-repeater’ regime, we find a comparatively higher QBER ($\sim 9\%$) and an entanglement generation rate of almost 80 Hz. In other words, in the many-repeater regime, distributing many entangled pairs of comparatively lower quality requires less hardware improvement. On the other hand, in the few-repeater regime it seems to be more feasible

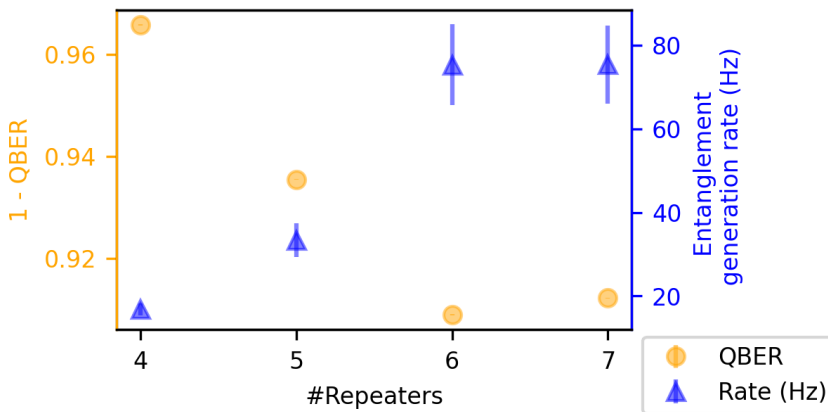


Figure 5.4: QBER and entanglement generation rate obtained with the minimal hardware requirements to achieve 10 Hz of SKR in the Bonn - Berlin setup with different numbers of repeaters, up to seven, the maximum allowed in the setup we study. The error bars are given by the standard error of the mean. Each data point corresponds to 2000 simulations of an entanglement-based BB84 protocol.

5

to distribute fewer pairs of comparatively higher quality. As the number of repeaters used decreases, it becomes harder to overcome the effect of fiber attenuation, which makes improving the quality of the entangled states delivered a more attractive option for increasing the SKR.

We finalize by remarking that, perhaps surprisingly, the variance in the time it takes to distribute one entangled state appears to grow as the number of repeaters in the chain increases (as shown by the increasing error bar on the rate in Figure 5.4). While interesting, further investigation is beyond the scope of this work.

We show the repeater placement corresponding to the minimal hardware requirements found when optimizing over the number of repeaters and their placement in Section 5.8.

5.3 Impact of target on hardware requirements

We now turn our attention to the impact of the performance target on the hardware requirements. We approach this from two angles: (i) the impact of varying the SKR target and (ii) the impact of holding the required rate constant but changing the target quantum-network application. It is clear that, given the same repeater chain, increasing the target rate will lead to more stringent requirements. However, it is not *a priori* obvious if the relative importance of the different parameters will change as the target rate is increased. It is further not obvious how changing the target application impacts the hardware requirements. These are questions of practical relevance: given that one wishes to build a repeater chain capable of distributing entanglement to perform QKD at a rate of 100 Hz, it seems crucial to know whether building a repeater chain for performing QKD at a rate of 1 Hz is a step in the right direction. In other words, this investigation can shed light on whether the process of improving hardware for quantum-repeater chains should be approached incrementally. The same question holds for the different target applications. It is likely that quantum repeaters will initially be used for QKD as they begin to replace

their trusted-node predecessors, and only progressively start to be used for applications that require multiple live qubits. We would then like to know whether the hardware improvements necessary to perform QKD using quantum repeaters are similar to the ones for multi-qubit applications.

5.3.1 Requirements for different secret-key-rate targets

In Figure 5.5 we show the directions along which hardware must be improved for distributing secret key at rates of 1, 10 and 100 Hz using BB84 in the network path connecting Bonn and Berlin. The corresponding minimal hardware requirements can be found in Table 5.2.

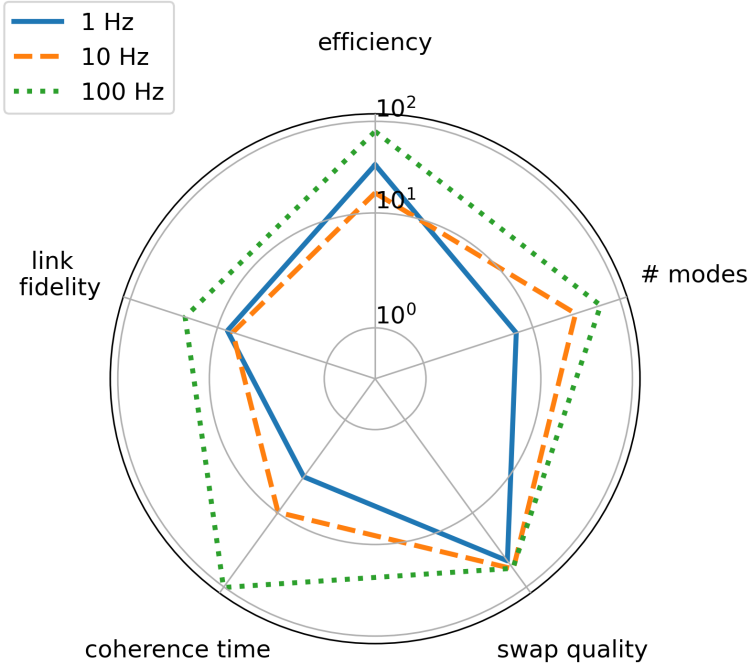


Figure 5.5: Directions along which hardware must be improved to enable attaining secret-key rates of 1 (blue, full), 10 (orange, dashed) and 100 Hz (green, dotted) between the German cities of Bonn and Berlin. The further away the line is from the center of the plot towards a given parameter, the more that parameter must be improved with respect to the current state-of-the-art. Improvement is depicted for the following parameters, clockwise from the top: overall photon detection probability excluding attenuation in fiber, number of multiplexing modes, fidelity of entanglement swap, coherence time of memory qubits and fidelity of elementary links. Note the use of a logarithmic scale.

The hardware requirements become more stringent as the SKR target grows. Further, the coherence time requires significantly less improvement in the 1 Hz case when compared to 10 and 100 Hz. This comes as something of a surprise, given that we expect qubits to spend less time in memory for higher SKR values, as these should correspond to higher entanglement-generation rates (and hence lower waiting times). In order to further investigate why this happens, we show in Figure 5.6 the QBER and entanglement generation rate achieved with the minimal hardware requirements for the best setup found by our optimization procedure for different SKR targets. We find that both the entanglement gen-

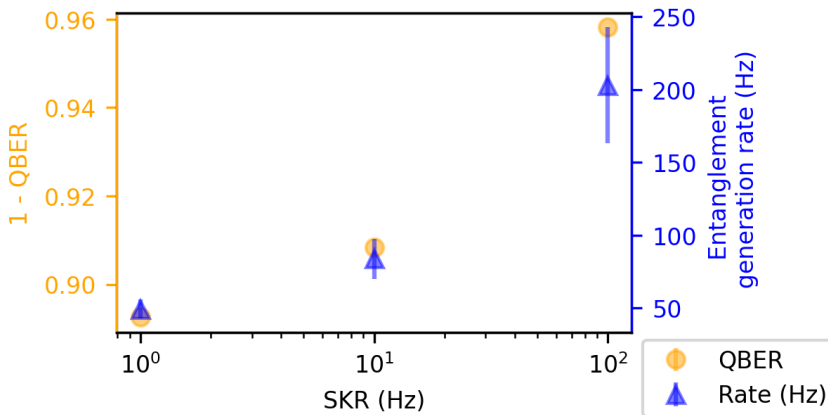


Figure 5.6: QBER and entanglement generation rate obtained with the minimal hardware requirements to achieve 1, 10 and 100 Hz of SKR in the Bonn - Berlin setup using the configuration found to be optimal for 10 Hz. The error bars are given by the standard error of the mean. Each data point corresponds to 2000 simulations of an entanglement-based BB84 protocol.

5

eration rate and $1 - \text{QBER}$ increase with the target SKR. We conjecture that the increase in coherence time observed for higher SKR targets is due to the necessary entanglement generation rate being very high. In fact, it is so high that it requires a huge number of multiplexing modes, which in turn imply a very high cost. This makes it comparatively less costly to extract more key from each entangled state than to generate states faster.

5.3.2 Requirements for secret-key and blind-quantum-computing success rates

In Figure 5.7 we show the directions along which hardware must be improved for performing QKD and BQC at a rate of 10 Hz in the network path connecting Bonn and Berlin. The corresponding minimal hardware requirements can be found in Table 5.2. It is plain to see that the two applications require improvements in distinct parameters. In particular, we emphasize the much larger coherence time required for BQC, corresponding to roughly a factor of 2.5 difference (7.99 vs 3.14 seconds). This can be explained by the fact that BQC, unlike QKD, requires two entangled pairs to be alive at the same time, implying that one entangled pair must be stored at the end nodes while the second one is generated. Further, the fact that the minimal coherence time required for BQC is high means that comparatively less noise will be caused by decoherence. This, in turn, means that in order to achieve the same state quality, the swap quality and the elementary link fidelity need not be as good.

We have also observed that there is a significant difference in the entanglement generation rates achieved by the parameter sets corresponding to the improvements shown in Figure 5.7. The minimal hardware requirements for QKD achieve an entanglement generation rate of almost 80 Hz, whereas the ones for the BQC-test-protocol result in an entanglement generation rate of around 20 Hz. In the same vein as what was discussed in Section 5.2.3, this is a result of the SKR and the BQC test protocol success rate being

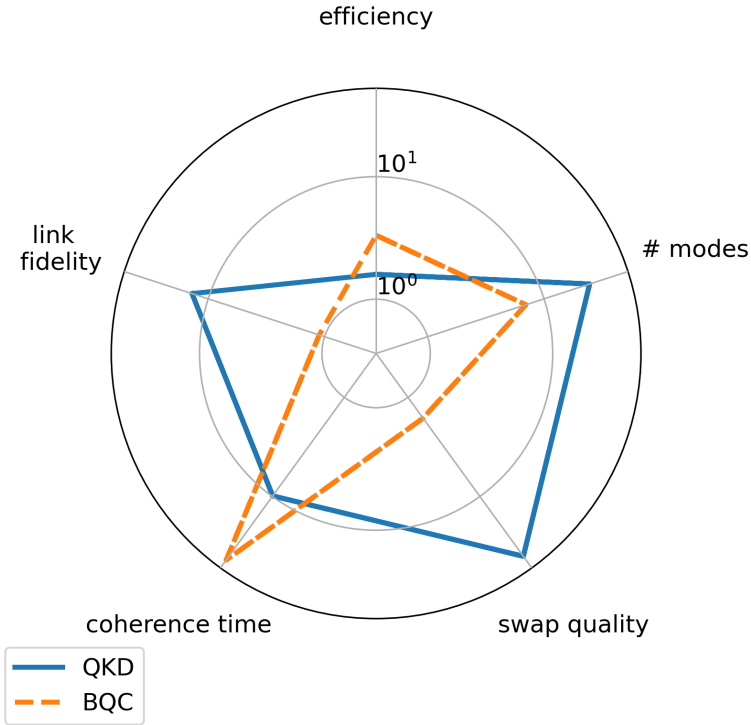


Figure 5.7: Directions along which hardware must be improved to enable attaining secret-key (QKD, blue) and blind quantum computing (BQC, orange) test protocol rates of 10 Hz between the German cities of Bonn and Berlin. The further away the line is from the center of the plot towards a given parameter, the more that parameter must be improved with respect to the current state-of-the-art. Improvement is depicted for the following parameters, clockwise from the top: overall photon detection probability excluding attenuation in fiber, number of multiplexing modes, fidelity of entanglement swap, coherence time of memory qubits and fidelity of elementary links. Note the use of a logarithmic scale.

composite quantities, depending not only on the rate at which entangled states are delivered, but also on the quality of these states. We believe that the difference observed in entanglement generation rate between the two applications is due to the fact that there is a threshold state quality to obtain non-zero secret-key ($\sim 11\%$ QBER or equivalently ~ 0.84 fidelity, both under the assumption of depolarizing noise). Such a threshold does not exist for the BQC test protocol. This fundamental difference means that the state quality requirements are more stringent in the QKD case, making improving the entanglement generation rate a more attractive possibility. We do however note that even though the BQC test protocol does not impose a threshold on state quality, the complete VBQC protocol proposed in [32] does.

5.4 Conclusion

We have determined minimal hardware requirements for generating entanglement between two nodes separated by roughly 900 km of real-world optical fiber using a chain

of processing-node quantum repeaters. We investigated both how such requirements depend on how many repeaters are employed and on the quantum-network application for which the entanglement is used. Notably, we have found that the hardware requirements for performing quantum key distribution and a simplified form of blind quantum computing are qualitatively different, with blind quantum computing requiring a coherence time which is roughly a factor of 2.5 larger for the same target rate in the setup we investigated. We further observed that given that most metrics one is interested in when evaluating quantum-network performance depend on both the rate at which entanglement is generated and its quality, there is room for trade-offs: for example, we found that when employing a large number of repeaters to achieve a given secret-key rate in the setup we studied it is easier to generate many entangled pairs of comparatively lower quality, with the opposite being true if fewer repeaters are used.

The blind-quantum-computing requirements we determined were obtained for a simplified form of the protocol, which is useful as a benchmark for quantum-network performance but is not an interesting application in and of itself. It would be interesting to learn how the results presented would change if instead a complete verified blind quantum computing protocol such as the one introduced in [32] were studied.

5

5.5 Data availability

The data presented in this work have been made available at <https://doi.org/10.4121/22193539> [42].

5.6 Code availability

The code that was used to perform the simulations and generate the plots in this paper has been made available at <https://gitlab.com/softwarequtech/simulation-code-for-requirements-for-upgrading-trusted-nodes-to-a-repeater-chain-over-900-km-of-optical-fiber> [41].

5.7 Baseline parameters

Here we discuss how we determined the baseline hardware parameters shown in Table 5.1. We did so by following two steps: (i) finding state-of-the-art color-center hardware parameters in the literature and (ii) converting these to the hardware model we employ. In Table 5.3 we show the relevant state-of-the-art color center parameters we have identified and provide their respective references. We now discuss how these are converted to the parameters shown in Table 5.1. The elementary-link fidelity and number of modes can be used directly without conversion. Color-center memories have both an electron qubit (also known as communication qubits due to their optical interface) and possibly multiple carbon qubits (also known as memory qubits due to being long-lived). We assume a ‘best-of-both-worlds’ situation, in which the qubits in our model are both endowed with an optical interface that allows them to generate entanglement and a long (1s baseline) memory lifetime. This simplification allows us to treat all qubits in the nodes equally. As explained in Section 7.2 we combine all photon-related inefficiencies, with the exception of fiber attenuation, into one parameter, p_{det} . This is done as follows:

$$p_{\text{det}} = p_{\text{photon interface}} \cdot p_{\text{conv}}, \quad (5.10)$$

Parameter	State-of-the-art value
Number of modes	1
Carbon coherence time	1 s [38]
Elementary-link fidelity	0.83 [7]
Electron initialization fidelity	0.995 [5]
Carbon initialization fidelity	0.99 [38]
Electron-carbon two-qubit gate fidelity	0.97 [13]
Electron single-qubit gate fidelity	0.995 [5]
Carbon single-qubit gate fidelity	0.999 [39]
Electron readout fidelity	0.93(0) 0.995(1) [37]
Photonic interface efficiency	0.855 [15]
Frequency conversion efficiency	0.3 [44]

Table 5.3: State-of-the-art color center parameters. We have number of modes as 1 without reference because to the best of our knowledge multiplexed entanglement generation has not been demonstrated using color centers.

where $p_{\text{photon interface}}$ is the photonic interface efficiency and p_{conv} is the frequency-conversion efficiency. This results in the 0.255 number reported in Table 5.1. We note that the experiment reported in [15] does not consist of entanglement generation through a heralding station, as we assume in this paper. We have made a best guess of how the parameters reported there would translate to a scheme where entangled photons are interfered and measured at a heralding station. An entanglement swap in a color center (this concrete example was demonstrated using a nitrogen-vacancy center) consists of single-qubit gates on both carbon and electron, two-qubit gates and measurement and initialization of the electron (see Figure 17 in Supplementary Note 5 of [26] for an image of the circuit). We make the simplifying assumption that all errors are depolarizing. First, we convert each of the initialization and gate fidelities in Table 5.3 to depolarizing parameters (in accordance with Equation (5.5)), and then multiply the depolarizing parameters corresponding to all the operations in the circuit together to obtain the swap quality (which parametrizes a depolarizing channel as detailed in Section 7.2), i.e.,

$$s_q = (1 - p_{\text{carbon}})^2 \cdot (1 - p_{\text{electron-carbon}}) \cdot (1 - p_{\text{electron}})^2 \cdot (1 - p_{\text{electron init}}) \cdot (1 - p_{\text{electron meas}})^2 \cdot (1 - p_{\text{retrieve}}), \quad (5.11)$$

where p_{carbon} is the depolarizing parameter of the carbon single-qubit gate, $p_{\text{electron-carbon}}$ of the two-qubit gate, p_{electron} of the electron single-qubit gate, $p_{\text{electron init}}$ of the electron initialization, $p_{\text{electron meas}}$ of the electron measurement and p_{retrieve} of the retrieve operation (maps the carbon state to the electron, see Figure 17 (b) in Supplementary Note 5 of [26]).

5.8 Repeater placement chosen by optimization method

As described in Section 5.2.2, we determined minimal hardware requirements for performing QKD at a rate of 10 Hz over the network path depicted in Figure 5.1. In doing so, we optimized over the number of repeaters used and their placement. We then used the placement our optimization method found to perform best for determining minimal hardware requirements for other performance targets, as described in Section 5.3. In Figure 5.8 we

show this placement. In Table 5.4 we show the lengths and attenuations of the elementary



Figure 5.8: Map of Germany overlaid with a depiction of the fiber path connecting the German cities of Bonn and Berlin that we investigated. The white circles represent end nodes, in Bonn and Berlin, and repeater nodes elsewhere. This placement corresponds to the best found by our optimization method, in the sense that it allowed for minimization of hardware requirements for a target secret-key rate of 10 Hz.

5

links defined by the repeater placement.

Link	Length (km)	Attenuation (dB)
Bonn - Wuppertal	138.9	32.8
Wuppertal - Münster	133.2	31.4
Münster - Warmsen	126.2	29.6
Warmsen - Hannover	97.2	22.7
Hannover - Liebenburg	122.0	28.4
Liebenburg - Magdeburg	115.5	26.9
Magdeburg - Havel	103.9	24.3
Havel - Berlin	80.2	18.6

Table 5.4: Length and attenuation of elementary links depicted in Figure 5.8.

In order to optimize over the number of repeaters and their placement, we have first generated all the 986 possible ways repeaters can be placed in the network (such that there is still space for the required heralding stations between repeaters and end nodes). To each configuration we assigned a number r corresponding to the number of repeaters in the network. Then, for each configuration we computed the chain asymmetry parameter defined as (see Chapter 4)

$$\mathcal{A}_{\text{chain}} = \frac{1}{r} \sum_{i=1}^r \frac{|L_{\text{left},i} - L_{\text{right},i}|}{L_{\text{left},i} + L_{\text{right},i}}, \quad (5.12)$$

where $L_{\text{left},i}$ ($L_{\text{right},i}$) is the distance between repeater node i and its left- (right-) hand neighboring node. Next, we ordered all the configurations with the same value of r by their values of $\mathcal{A}_{\text{chain}}$, and label their position in this ordering as n . This number is then an identifier for how asymmetric (as quantified by the chain asymmetry parameter) a configuration is relative to the other configurations with the same number of repeaters. $n = 0$

corresponds to the most symmetric setup and $n = m_r - 1$ corresponds to the most asymmetric setup, where m_r is the number of configurations with r repeaters. All configurations are then stored in a table by their values for r and n .

Then, when we optimize over the hardware parameters, we also optimize over two additional parameters. These are r (the number of repeaters) and a , which is a number between zero and one. Given a pair (r, a) , the configuration that is used is chosen as follows. First, the number a is mapped to a value of n using

$$n = \text{round}(a(m_r - 1)), \quad (5.13)$$

(where round denotes rounding to the closest integer) i.e., it uses $n = 0$ for $a = 0$ and $n = m_r - 1$ for $a = 1$. Second, the unique configuration defined by the values of r and n is taken from the table and used in the simulation. The reason why we optimize over a instead of over n directly is that a quantifies how asymmetric the chosen configuration is in a way that is independent of r (the range is always between 0 and 1, instead of between 0 and $m_r - 1$). This makes it easier to vary r and a independently compared to r and n .

5

5.9 Optimization method

In this section we provide more details regarding our optimization methodology. This methodology is based on genetic algorithms, which come in several different flavors. Our particular implementation is heavily based on the one introduced in [43] and used in [45, 46] and Chapter 3, to which we refer the interested reader. There are two things that we do discuss in this section. First, as the parameter set we use here is different than in [43, 45, 46] and Chapter 3, we explain in Section 5.9.1 how we define the probability of no imperfection for each of these, as required by the definition of the hardware cost function H_c in Section 5.1.3. Second, we have employed a simple local optimization performed on the best solution found by the genetic algorithm. This local optimization method has been used and described in [45], but has not yet appeared in a peer-reviewed publication. We therefore explain it below in Section 5.9.2. Additionally, we also give the details of the machine used to perform the actual optimizations in Section 5.9.3. Finally we would like to remark that the code for our implementation, together with the tools required for integration with NetSquid simulations, is publicly accessible at [47].

5.9.1 No-imperfection probabilities

We show in Table 5.5 the probability of no-imperfection for all parameters considered in our hardware models.

We start by defining the quantity $p_{\text{surv baseline}}$ that appears in this table more rigorously. It is computed as follows,

$$p_{\text{surv baseline}} = 10^{-\overline{\alpha_{\text{att}}}/10}, \quad (5.14)$$

with $\overline{\alpha_{\text{att}}}$ given by,

$$\overline{\alpha_{\text{att}}} = \frac{2}{N} \sum_{i=1}^N \alpha_{\text{att},i} L_i. \quad (5.15)$$

Here, L_i is the length of fiber segment i in the fiber path under consideration, $\alpha_{\text{att},i}$ is the attenuation coefficient of fiber segment i (i.e., the amount of attenuation per unit length),

Parameter	Probability of no-imperfection
Photon detection probability p_{det}	p_{det}
Coherence time T	$e^{-1/T}$
Swap quality s_q	s_q
Elementary link fidelity F_{el}	F_{el}
Number of multiplexing modes N	$1 - (1 - p_{\text{surv baseline}})^N$

Table 5.5: Probabilities of no-imperfection for hardware parameters we optimized over in this work. $p_{\text{surv baseline}}$ (defined in Equation (5.14)) is the probability of one photon (i.e., no multiplexing) surviving traveling an elementary link made up out of two times the average fiber segment in the fiber path we study (shown in Figure 5.1).

5

and N is the total number of fiber segments in the path. For the fiber path considered in this paper (i.e., the one depicted in Figure 5.1), $N = 17$. An elementary link between two neighboring nodes must consist of at least two fiber segments to allow for the installation of a heralding station. $\overline{\alpha}_{\text{att}}$ can then be thought of as the total amount of attenuation on an elementary link made up of two times the average fiber segment. This means $p_{\text{surv baseline}}$ is the probability of a photon surviving traveling through this average elementary link. The reason for constructing this quantity is that it provides a baseline for the photon survival probability in fiber, which can then be improved upon by increasing the number of multiplexing modes, thereby enabling us to associate a cost function.

The coherence time T represents a timescale for depolarization, with the probability of the state becoming maximally mixed over a period of time t being given by $1 - e^{-t/T}$, with the respective probability of no-imperfection then being $e^{-t/T}$. In this case, improving T by a factor of k is equivalent to multiplying it by k .

For the swap quality, s_q is the probability that the two-qubit state before the Bell-state measurement is not replaced with a maximally mixed state, and therefore s_q is the corresponding probability of no imperfection. Finally, for the elementary-link fidelity we take the fidelity itself to be the probability of no imperfection.

5.9.2 Local optimization

Genetic algorithms are derivative-free optimization algorithms that are particularly useful when applied to functions whose cost landscape is largely unknown but is assumed to have many local minima [48]. Through a balancing act of exploration (i.e., investigation of many different areas of parameter space) and exploitation (i.e., investigation of local optima) they often manage to avoid being trapped in local optima as gradient-based methods are wont to. Nevertheless, use of a genetic algorithm does not guarantee that one can find the global optimum. Further, one can not even be sure that one has maximally exploited the best optimum found. For this reason, we complement the exploration performed by the genetic algorithm with a deterministic local optimization method which we apply to the best parameter set found by the genetic algorithm. The algorithm used is a variation of an iterative local search algorithm [49]. It consists of iteratively making small changes on a parameter and evaluating the cost associated to the resulting parameter set. In case it has decreased, it is kept and we again make a small change on the same parameter. If the cost increases, we discard the change and move on to another parameter. This process is repeated for all parameters being optimized over. We must however emphasize that this still does not guarantee that the global optimum will be found.

More details on this method can be found in Chapter 4.2 of [45].

5.9.3 Performing the optimization

Each optimization run was executed on a thin node of the Snellius supercomputer [50]. Each of these nodes is endowed with 2 AMD Rome 7H12 CPUs (2.6 GHz), for a total of 128 cores and a total of 256 GiB of memory.

5.10 BQC test protocol

In this section we describe the BQC test protocol that is used as a performance metric in this paper. This protocol consists of repeated execution of test rounds as required by the VBQC protocol presented in [32]. In each round of the VBQC protocol, a server is tasked by a client to execute a quantum computation on qubits transmitted by the client and then send the classical result of that computation back to the client. In test rounds, the client has prepared the transmitted qubits in such a way that it knows the correct outcome of the computation.

Therefore, executing test rounds allows the client to verify whether the server is honest. However, noise in the quantum hardware can also lead to failed test rounds. The more often test rounds fail due to noise, the harder it is for the client to verify the server's honesty.

The BQC test protocol that we consider is not itself a VBQC protocol. In fact, its only purpose is to benchmark how suited a quantum network could be to perform BQC protocols (and perhaps other applications that require multiple live qubits simultaneously). The performance metric that we consider for this protocol is the success rate, defined as the average number of successful test rounds that can be executed per time unit (i.e., the product of the rate R and success probability p_s , as in Equation (5.8)). We specifically consider an entanglement-based two-qubit version of the protocol. In that case, the protocol is as follows:

1. The client chooses d and r uniformly at random from $\{0, 1\}$ and θ from $\{j\pi/4\}_{0 \leq j \leq 7}$, and then defines two quantum states, $|\text{dummy}\rangle = |i\rangle$ and $|\text{trap}\rangle = |+\theta\rangle$, where $|\pm\phi\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle \pm e^{i\phi}|1\rangle)$. Additionally, it uniformly at random designates $|\phi_1\rangle$ to be $|\text{dummy}\rangle$ or $|\text{trap}\rangle$. $|\phi_2\rangle$ is designated to be the option that was not chosen.
2. When an entangled state shared between the client and server becomes available, the client uses quantum teleportation to transmit the state $|\phi_1\rangle$ to the server. The server stores the received state in quantum memory.
3. When a second entangled state becomes available, the client uses quantum teleportation to transmit the state $|\phi_2\rangle$ to the server.
4. The server performs a CZ gate between its two qubits.
5. The server measures the qubit that was used to receive the state $|\text{trap}\rangle$ in the basis $\{|+\theta+r\pi\rangle, |-\theta+r\pi\rangle\}$ and transmits the result back to the client.
6. The client declares the test round a success if it receives measurement result matching its expectation (i.e., if the outcome is equal to $d \oplus r$, where \oplus is addition modulo two), and a failure otherwise.

7. The client and server go back to Step 1 to start the next test round.

Alternatively, remote state preparation [51] could be used to prepare the required states at the server, which may be easier to execute on real hardware than quantum teleportation. In fact, we have proven in Chapter 3 that using remote state preparation for the VBQC protocol in [32] is equivalent to using quantum teleportation in case the client and server implement gates noiselessly. Therefore the success rate will, under these assumptions, be the same whether quantum teleportation or remote state preparation is used.

We here assume that classical communication between the client and the server happens instantaneously and that both the client and server are able to perform gates and measurements noiselessly and instantly. However we do not assume they are able to store qubits indefinitely; the first teleported state undergoes depolarizing noise as described in Equation (5.6), where the coherence time T is the same as the coherence time of the repeater nodes (i.e., it is varied by the optimizations performed in this paper). Under these assumptions, R_{rounds} is simply half the rate at which entanglement can be distributed when entanglement is being generated continuously, as one test round can be performed for every two entangled states that are produced. In order to calculate the success probability, we use the following result from Chapter 3:

$$1 - p_s = e^{-\frac{\Delta t}{T}} \left[F_{\text{dummy}}(1 - F_{\text{trap}}) + F_{\text{trap}}(1 - F_{\text{dummy}}) \right] + \frac{1}{2} \left(1 - e^{-\frac{\Delta t}{T}} \right). \quad (5.16)$$

Here, Δt is the time between the transmission of the first qubit and the second qubit. For the fidelities F_{trap} and F_{dummy} , let the density matrices for the state $|\text{dummy}\rangle$ after transmission to the server be ρ_{dummy} and ρ_{trap} for $|\text{trap}\rangle$. Then $F_{\text{dummy}} = \langle \text{dummy} | \rho_{\text{dummy}} | \text{dummy} \rangle$ and $F_{\text{trap}} = \langle \text{trap} | \rho_{\text{trap}} | \text{trap} \rangle$.

We then determine the success rate as follows. First, we simulate continuous entanglement generation between the end nodes of a repeater chain. Each time an end-to-end entangled state is generated it is removed from the simulation and stored as raw data, together with the time at which it was generated. Then, after the simulation has finished, we process the raw data to determine what the success rate would have been if the entangled states had been consumed by the BQC test protocol. To this end, we divide the data into single test rounds, each consisting of two entangled states that were generated in succession. We assign each test round a duration t , which is the amount of time between the start of the round and the end of the round (i.e., when the second state was generated), and a storage time Δt , which is the time between when the first entangled state and the second entangled state were generated. We furthermore calculate the p_s of that round using Equation (5.16), where we average over the two possible choices in the protocol for how $|\phi_1\rangle$ and $|\phi_2\rangle$ are designated (i.e., whether the first entangled state is used to transmit the dummy and the second to transmit the trap or vice versa). Then we calculate the rate as

$$R = \frac{1}{\langle t \rangle}, \quad (5.17)$$

where $\langle t \rangle$ is the average value of t over all the test rounds. Finally, we use R and the average value of p_s to calculate the success rate according to Equation (5.8). The processing code that realizes this calculation has been made publicly available at [52].

References

- [1] S. Wehner, D. Elkouss, and R. Hanson, *Quantum internet: A vision for the road ahead*, *Science* **362** (2018).
- [2] C. Cabrillo, J. I. Cirac, P. Garcia-Fernandez, and P. Zoller, *Creation of entangled states of distant atoms by interference*, *Physical Review A* **59**, 1025 (1999).
- [3] S. D. Barrett and P. Kok, *Efficient high-fidelity quantum computation using matter qubits and linear optics*, **71**, 060310, publisher: American Physical Society.
- [4] P. C. Humphreys, N. Kalb, J. P. Morits, R. N. Schouten, R. F. Vermeulen, D. J. Twitchen, M. Markham, and R. Hanson, *Deterministic delivery of remote entanglement on a quantum network*, *Nature* **558**, 268 (2018).
- [5] M. Pompili, S. L. Hermans, S. Baier, H. K. Beukers, P. C. Humphreys, R. N. Schouten, R. F. Vermeulen, M. J. Tiggeleman, L. dos Santos Martins, B. Dirkse, *et al.*, *Realization of a multinode quantum network of remote solid-state qubits*, *Science* **372**, 259 (2021).
- [6] H. Bernien, B. Hensen, W. Pfaff, G. Koolstra, M. S. Blok, L. Robledo, T. H. Taminiau, M. Markham, D. J. Twitchen, L. Childress, *et al.*, *Heralded entanglement between solid-state qubits separated by three metres*, *Nature* **497**, 86 (2013).
- [7] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenbergh, R. F. Vermeulen, R. N. Schouten, C. Abellán, *et al.*, *Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres*, *Nature* **526**, 682 (2015).
- [8] L. J. Stephenson, D. P. Nadlinger, B. C. Nichol, S. An, P. Drmota, T. G. Ballance, K. Thirumalai, J. F. Goodwin, D. M. Lucas, and C. J. Ballance, *High-Rate, High-Fidelity Entanglement of Qubits Across an Elementary Quantum Network*, *Physical Review Letters* **124**, 110501 (2020).
- [9] V. Krutyanskiy, M. Galli, V. Krcmarsky, S. Baier, D. A. Fioretto, Y. Pu, A. Mazloom, P. Sekatski, M. Canteri, M. Teller, J. Schupp, J. Bate, M. Meraner, N. Sangouard, B. P. Lanyon, and T. E. Northup, *Entanglement of trapped-ion qubits separated by 230 meters*, *Phys. Rev. Lett.* **130**, 050803 (2023).
- [10] K. Azuma, S. E. Economou, D. Elkouss, P. Hilaire, L. Jiang, H.-K. Lo, and I. Tzitrin, *Quantum repeaters: From quantum networks to the quantum internet*, (2022), arXiv:2212.10820 .
- [11] T. E. Northup and R. Blatt, *Quantum information transfer using photons*, *Nature Photon* **8**, 356 (2014), arxiv:1708.00424 .
- [12] W. Pfaff, B. J. Hensen, H. Bernien, S. B. van Dam, M. S. Blok, T. H. Taminiau, M. J. Tiggeleman, R. N. Schouten, M. Markham, D. J. Twitchen, *et al.*, *Unconditional quantum teleportation between distant solid-state quantum bits*, *Science* **345**, 532 (2014).
- [13] N. Kalb, A. A. Reiserer, P. C. Humphreys, J. J. Bakermans, S. J. Kamerling, N. H. Nickerson, S. C. Benjamin, D. J. Twitchen, M. Markham, and R. Hanson, *Entanglement distillation between solid-state quantum network nodes*, *Science* **356**, 928 (2017).

- [14] L. Slodička, G. Hétet, N. Röck, P. Schindler, M. Hennrich, and R. Blatt, *Atom-Atom Entanglement by Single-Photon Detection*, Phys. Rev. Lett. **110**, 083603 (2013).
- [15] M. K. Bhaskar, R. Riedinger, B. Machielse, D. S. Levonian, C. T. Nguyen, E. N. Knall, H. Park, D. Englund, M. Lončar, D. D. Sukachev, *et al.*, *Experimental demonstration of memory-enhanced quantum communication*, Nature **580**, 60 (2020).
- [16] S. Langenfeld, S. Welte, L. Hartung, S. Daiss, P. Thomas, O. Morin, E. Distanté, and G. Rempe, *Quantum Teleportation between Remote Qubit Memories with Only a Single Photon as a Resource*, Phys. Rev. Lett. **126**, 130502 (2021), 2105.04338 .
- [17] G. W. Lin, X. B. Zou, X. M. Lin, and G. C. Guo, *Heralded quantum memory for single-photon polarization qubits*, EPL **86**, 30006 (2009).
- [18] M. Ruf, N. H. Wan, H. Choi, D. Englund, and R. Hanson, *Quantum networks based on color centers in diamond*, Journal of Applied Physics **130**, 070901 (2021).
- [19] S. Hermans, M. Pompili, L. dos Santos Martins, A. Rodriguez-Pardo Montblanch, H. Beukers, S. Baier, J. Borregaard, and R. Hanson, *Entangling remote qubits using the single-photon protocol: an in-depth theoretical and experimental study*, New Journal of Physics (2023).
- [20] M. Horodecki, P. Horodecki, and R. Horodecki, *General teleportation channel, singlet fraction, and quasidistillation*, Physical Review A **60**, 1888 (1999), publisher: American Physical Society.
- [21] M. Pompili, C. Delle Donne, I. te Raa, B. van der Vecht, M. Skrzypczyk, G. Ferreira, L. de Kluijver, A. J. Stolk, S. L. N. Hermans, P. Pawełczak, W. Kozłowski, R. Hanson, and S. Wehner, *Experimental demonstration of entanglement delivery using a quantum network stack*, npj Quantum Inf **8**, 1 (2022).
- [22] L. Childress, J. M. Taylor, A. S. Sørensen, and M. D. Lukin, *Fault-tolerant quantum repeaters with minimal physical resources and implementations based on single-photon emitters*, Phys. Rev. A **72**, 052330 (2005).
- [23] M. F. Askarani, K. Chakraborty, and G. C. Do Amaral, *Entanglement distribution in multi-platform buffered-router-assisted frequency-multiplexed automated repeater chains*, New Journal of Physics **23**, 063078 (2021).
- [24] S. B. van Dam, P. C. Humphreys, F. Rozpędek, S. Wehner, and R. Hanson, *Multiplexed entanglement generation over quantum networks using multi-qubit nodes*, Quantum Science and Technology **2**, 034002 (2017).
- [25] N. Sinclair, E. Saglamyurek, H. Mallahzadeh, J. A. Slater, M. George, R. Ricken, M. P. Hedges, D. Oblak, C. Simon, W. Sohler, *et al.*, *Spectral multiplexing for scalable quantum photonics using an atomic frequency comb quantum memory and feed-forward control*, Physical review letters **113**, 053603 (2014).
- [26] T. Coopmans, R. Knegjens, A. Dahlberg, D. Maier, L. Nijsten, J. de Oliveira Filho, M. Papendrecht, J. Rabbie, F. Rozpędek, M. Skrzypczyk, *et al.*, *Netsquid, a network simulator for quantum information using discrete events*, Communications Physics **4**, 1 (2021).

- [27] Á. G. Iñesta, G. Vardoyan, L. Scavuzzo, and S. Wehner, *Optimal entanglement distribution policies in homogeneous repeater chains with cutoffs*, (2022), arxiv:arXiv:2207.06533 .
- [28] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels*, Physical review letters **70**, 1895 (1993).
- [29] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, Theoretical Computer Science Theoretical Aspects of Quantum Cryptography – Celebrating 30 Years of BB84, **560**, 7 (2014).
- [30] C. H. Bennett, G. Brassard, and N. D. Mermin, *Quantum cryptography without bell’s theorem*, Physical review letters **68**, 557 (1992).
- [31] P. W. Shor and J. Preskill, *Simple proof of security of the bb84 quantum key distribution protocol*, Physical review letters **85**, 441 (2000).
- [32] D. Leichtle, L. Music, E. Kashefi, and H. Ollivier, *Verifying bqp computations on noisy devices with minimal overhead*, PRX Quantum **2**, 040302 (2021).
- [33] A. Broadbent, J. Fitzsimons, and E. Kashefi, *Universal blind quantum computation*, in *2009 50th Annual IEEE Symposium on Foundations of Computer Science* (IEEE, 2009) pp. 517–526.
- [34] A. Pascoletti and P. Serafini, *Scalarizing vector optimization problems*, Journal of Optimization Theory and Applications **42**, 499 (1984).
- [35] J. D. Schaffer, *Some experiments in machine learning using vector evaluated genetic algorithms*, Tech. Rep. (Vanderbilt Univ., Nashville, TN (USA), 1985).
- [36] C. Bradley, S. de Bone, P. Möller, S. Baier, M. Degen, S. Loenen, H. Bartling, M. Markham, D. Twitchen, R. Hanson, *et al.*, *Robust quantum-network memory based on spin qubits in isotopically engineered diamond*, npj Quantum Information **8**, 122 (2022).
- [37] S. Hermans, M. Pompili, H. Beukers, S. Baier, J. Borregaard, and R. Hanson, *Qubit teleportation between non-neighbouring nodes in a quantum network*, Nature **605**, 663 (2022).
- [38] C. Bradley, J. Randall, M. Abobeih, R. Berrevoets, M. Degen, M. Bakker, M. Markham, D. Twitchen, and T. Taminiau, *A ten-qubit solid-state spin register with quantum memory up to one minute*, Physical Review X **9**, 031045 (2019).
- [39] T. H. Taminiau, J. Cramer, T. van der Sar, V. V. Dobrovitski, and R. Hanson, *Universal control and error correction in multi-qubit spin registers in diamond*, Nature nanotechnology **9**, 171 (2014).
- [40] *NetSquid-QRepChain*, <https://gitlab.com/softwarequtech/netsquid-snippets/netsquid-qrepchain> (2023).

- [41] G. Avis and F. Ferreira da Silva, *Simulation code for Requirements for upgrading trusted nodes to a repeater chain over 900 km of optical fiber*, <https://gitlab.com/softwarequtech/simulation-code-for-requirements-for-upgrading-trusted-nodes-to-a-repeater-chain-over-900-km-of-optical-fiber>.
- [42] F. Ferreira da Silva, G. Avis, and S. Wehner, *Replication data for: Requirements for upgrading trusted nodes to a repeater chain over 900 km of optical fiber*, <https://doi.org/10.4121/22193539> (2023).
- [43] F. F. da Silva, A. Torres-Knoop, T. Coopmans, D. Maier, and S. Wehner, *Optimizing entanglement generation and distribution using genetic algorithms*, Quantum Science and Technology (2021).
- [44] S. Zaske, A. Lenhard, C. A. Keßler, J. Kettler, C. Hepp, C. Arend, R. Albrecht, W.-M. Schulz, M. Jetter, P. Michler, *et al.*, *Visible-to-telecom quantum frequency conversion of light from a single quantum emitter*, Physical review letters **109**, 147404 (2012).
- [45] A. Labay Mora, *Genetic algorithm-based optimisation of entanglement distribution to minimise hardware cost*, (2021).
- [46] A. Labay Mora, F. Ferreira da Silva, and S. Wehner, In preparation.
- [47] A. Torres-Knoop, T. Coopmans, D. Maier, and F. Silva, *smart-stopos*, <https://gitlab.com/aritoka/smart-stopos> (2020).
- [48] D. E. Goldberg, *Genetic Algorithms in Search, Optimization and Machine Learning*, 1st ed. (Addison-Wesley Longman Publishing Co., Inc., USA, 1989).
- [49] S. Luke, *Essentials of metaheuristics*, Vol. 2 (Lulu Raleigh, 2013).
- [50] *Snellius*, <https://www.surf.nl/en/dutch-national-supercomputer-snellius>.
- [51] C. H. Bennett, D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, and W. K. Wootters, *Remote state preparation*, Physical Review Letters **87**, 077902 (2001).
- [52] *NetSquid-SimulationTools*, <https://gitlab.com/softwarequtech/netsquid-snippets/netsquid-simulationtools> (2022).

6

Designing Quantum Networks Using Preexisting Infrastructure

Julian Rabbie, Kaushik Chakraborty*, Guus Avis* and Stephanie Wehner.

6

We consider the problem of deploying a quantum network on an existing fiber infrastructure, where quantum repeaters and end nodes can only be housed at specific locations. We propose a method based on integer linear programming (ILP) to place the minimal number of repeaters on such an existing network topology, such that requirements on end-to-end entanglement-generation rate and fidelity between any pair of end-nodes are satisfied. While ILPs are generally difficult to solve, we show that our method performs well in practice for networks of up to 100 nodes. We illustrate the behavior of our method both on randomly-generated network topologies, as well as on a real-world fiber topology deployed in the Netherlands.

In this chapter we address the question of how repeaters can best be allocated in an existing fiber grid in order to build a quantum network, while keeping the total number of repeaters as small as possible. In doing so we focus less on the precise devices and protocols used to realize the quantum repeaters or their exact performance. Rather, we focus on how a sufficient service level can be guaranteed for a large number of end nodes in the network and search for an efficient algorithm for choosing repeater locations correspondingly.

We model a classical fiber network which forms the basis of a quantum network as an undirected, weighted graph $G = (\mathcal{N}, \mathcal{F}, \mathcal{L})$. The nodes \mathcal{N} are partitioned into a set of *end nodes* $\mathcal{C} \subset \mathcal{N}$ and a set of *potential repeater locations* $\mathcal{R} = \mathcal{N} \setminus \mathcal{C}$. The goal of the quantum network is to enable quantum communication between end nodes. Potential repeater locations are any location in the network where a quantum repeater could be placed. Such a location could, for example, be a hub in the classical network with the facilities required to run a quantum repeater. The edges of the graph are the fibers of the network, \mathcal{F} , where

*These authors contributed equally.

This chapter is based on the publication npj Quantum Inf 8, 5 (2022)

$\mathcal{L}(f)$ is the length of fiber $f \in \mathcal{F}$. In case a quantum repeater is installed at a potential repeater location, the potential repeater location becomes a *quantum-repeater node*. When deploying a quantum network based on a classical fiber network, it is essential to determine which potential repeater locations should be turned into quantum-repeater nodes.

In order to have an operational quantum network, nodes must be connected by elementary links. For many quantum-repeater schemes (such as those using heralded entanglement generation as discussed in Section 2.1), elementary links consist of fibers with active elements measuring qubits. Therefore, when deploying a quantum network based on a classical fiber network, it must also be determined which fibers to convert into elementary links. Here, we consider that elementary links can be constructed from any number of consecutively-adjacent fibers in the graph G (passing through potential repeater locations). Both fibers and potential repeater locations can be part of multiple elementary links, which is motivated by the fact that fibers are typically constructed in bundles (meaning that each elementary link could, in fact, use the same fiber bundle but a different fiber). Additionally, multiplexing over different wavelengths could be used to enable the use of a single fiber in multiple elementary links. For an example of how a (very) small classical fiber network can be used to create a quantum network, see Figure 6.1.

Here, we introduce the problem of determining how to construct a quantum network using a preexisting classical fiber network as the repeater-allocation problem. We define it as follows:

Repeater-Allocation Problem: Given a classical fiber network corresponding to the undirected, weighted graph $G = (\mathcal{N}, \mathcal{F}, \mathcal{L})$ with end nodes $\mathcal{E} \subset \mathcal{N}$. Which of the potential repeater locations $\mathcal{R} = \mathcal{N} \setminus \mathcal{E}$ should be turned into quantum-repeater nodes, and which fibers should be converted into elementary links, such that a quantum network is obtained which satisfies a set of network requirements, while the associated costs are minimized?

In this paper we present, to the best of our knowledge for the first time, a method which solves the repeater-allocation problem. Here, we only consider the costs associated to installing quantum repeaters, as we expect that the first practical quantum repeaters will come at a high cost. Furthermore, the set of network requirements that we consider are the following:

1 Rate and fidelity.

The quantum network must be able to distribute bipartite entangled quantum states between any pair of end nodes at some minimum rate, which we denote R_{\min} . Furthermore, the states must have some minimum fidelity to a maximally entangled

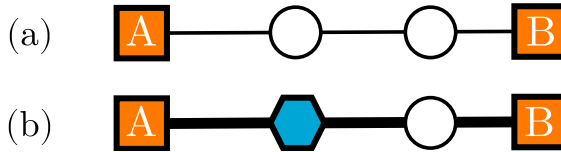


Figure 6.1: Example of how a quantum network can be constructed. (a) Graph representing a simple fiber network. Nodes A and B are end nodes, while the other two nodes are potential repeater locations. (b) Quantum network that is constructed using the pre-existing fiber network. The first node from A is used as a quantum-repeater node (blue hexagon) and there are two elementary links. One elementary link is made from A to the quantum-repeater node, while the other starts at the quantum-repeater node and ends at B.

state, which we denote F_{\min} . The network must be able to do this for every pair of end nodes simultaneously.

In a quantum-repeater chain with fixed hardware, the rate of entanglement distribution is limited by loss and noise in elementary links and in quantum repeaters. Therefore, it is generally possible to lower bound the rate by upper bounding the number of quantum repeaters (and thereby the number of elementary links), and the length of each elementary link (assuming the photon loss probability per unit length is constant). Similarly, fidelity is limited by noisy operations in quantum repeaters, while it can also be a decreasing function of the elementary link length (this can be, for example, due to dark counts in detectors). Therefore, fidelity too can be lower bounded by upper bounding the number of quantum repeaters and the elementary link length.

We use these bounds to assess whether the rate and fidelity between a pair of end nodes is sufficient. For any R_{\min} and F_{\min} , we can find N_{\max} and L_{\max} such that a repeater chain of N_{\max} repeaters and elementary links of length L_{\max} can deliver entangled states at rate R_{\min} with fidelity F_{\min} . Then, we consider two end nodes capable of receiving entangled states with at least rate R_{\min} and at least fidelity F_{\min} if there is a free path between them which contains at most N_{\max} repeaters and of which each elementary link is at most L_{\max} long.

How exactly N_{\max} and L_{\max} can be determined from R_{\min} and F_{\min} is specific to the quantum-repeater architecture and depends on various performance parameters. We give a toy-model calculation in Section 6.3.2 as an example. Note that when considering a quantum-repeater architecture which is not based on entanglement distribution, the method presented in this paper is still applicable if a performance metric like rate and fidelity can be determined which can be lower bounded by upper bounding the number of repeaters and the elementary link lengths of a repeater chain.

2 Robustness.

When a part of a quantum network breaks down, all other requirements should still be met. We quantify this using the minimum number of quantum-repeater nodes or elementary links (it can be any combination) that need to break down before one of the other requirements can no longer be met. Here, we use the symbol K to refer to this number.

3 Repeater capacity.

Quantum-repeater nodes should never be required to operate above their capacity in order to meet all other network requirements. We define the capacity of a quantum-repeater node as the maximum number of quantum-communication sessions it can facilitate simultaneously. In an entanglement-based network, this could be directly related to the number of entangled states that can be stored in memory or the number of Bell-state measurements that can be performed simultaneously. Here, we use the symbol D to refer to the capacity of the quantum-repeater nodes.

6.1 Results

6

In this section we present a method, detailed in Box 6.1, which aids in the design of a quantum network using existing classical infrastructure. Specifically, given a fiber network, our method makes it possible to choose at which locations quantum repeaters should be installed. This is done such that entangled states can be distributed between all pairs of end nodes simultaneously with a minimum rate and fidelity. Furthermore, our method guarantees that the resulting quantum network is robust against failure of quantum repeaters and elementary links, and can take finite capacity of quantum repeaters into account. At the same time, our method minimizes the total number of quantum repeaters that need to be installed. We dub the problem that our method solves the repeater-allocation problem.

Box 6.1: Method to solve the repeater-allocation problem.**Input**

- Fiber network graph $G = (\mathcal{N}, \mathcal{F}, \mathcal{L})$.
- Set of end nodes $\mathcal{C} \subset \mathcal{N}$.
- Minimum rate R_{\min} and fidelity F_{\min} required by end nodes.*
- Required robustness parameter K (number of quantum-repeater nodes and elementary links that must be incapacitated before network operation is compromised).
- Capacity parameter D (number of quantum-communication sessions that one quantum repeater can facilitate simultaneously).

Method

1. Determine values for the parameters L_{\max} and N_{\max} such that a quantum-repeater chain consisting of N_{\max} repeaters and elementary links of length L_{\max} is able to deliver entangled states at rate R_{\min} with fidelity F_{\min} to a maximally entangled state.
2. Construct the set of potential repeater locations

$$\mathcal{R} = \mathcal{N} \setminus \mathcal{C}. \quad (6.1)$$

3. Construct the set

$$\mathcal{Q} = \left\{ (s, t) \mid (s, t) \in_R \{(i, j), (j, i)\}, i, j \in \mathcal{C}, i \neq j \right\}, \quad (6.2)$$

where \in_R implies picked uniformly at random.

4. For every $(s, t) \in \mathcal{Q}$, construct the set

$$\mathcal{E}_{(s,t)} = \left\{ (n_1, n_2) \mid n_1 \in \mathcal{R} \cup \{s\}, n_2 \in \mathcal{R} \cup \{t\}, n_1 \neq n_2 \right\}, \quad (6.3)$$

and then construct the set

$$\mathcal{E} = \bigcup_{q \in \mathcal{Q}} \mathcal{E}_q. \quad (6.4)$$

5. For every $(u, v) \in \mathcal{E}$, determine the shortest path from u to v in the fiber-network graph G . Store the length of the path as $L((u, v))$ and the fibers making it up as $F((u, v))$.

6. Solve the link-based formulation in Box 6.3 using an ILP solver. Store the values of the variables $x_{uv}^{q,k}$ and y_u .
7. Apply the path extraction algorithm, i.e. Algorithm 1, to obtain the set \mathcal{P}^* . For every $(u, v) \in \mathcal{E}$, set $x_{uv}^{q,k} = 0$ if there is no $p \in \mathcal{P}^*$ such that $(u, v) \in p$.

Solution

- Every potential repeater location $u \in \mathcal{R}$ for which $y_u = 1$ should be used as a quantum-repeater node.
- For every $(u, v) \in \mathcal{E}$ for which $x_{uv}^{q,k} = 1$ for some value of q and k , an elementary link should be constructed using the fibers $F((u, v))$.

Key to our method is integer linear programming (ILP), which can be used to obtain the optimal repeater placement with an optimization solver such as Clp [1], Gurobi [2] or CPLEX [3]. Our method has been tested both using a real fiber network and a large number of randomized graphs, on which we report in Sections 6.2.1 and 6.2.2 respectively. The real network contains four end nodes and 50 potential repeater locations, and a solution was found in 74 seconds using a computer running a quad-core Intel Xeon W-2123 processor at 3.60 GHz and 16 GB of RAM, demonstrating that the method is feasible for realistically-sized networks.

Here, we put forward two different ILP formulations. The first, which we call the *path-based formulation* (see Box 6.2), is based on enumerating and then choosing paths between end nodes of the quantum network. It is relatively easy to show and understand that this formulation indeed solves the repeater-allocation problem (see Section 6.3.1). However, it is not efficient, as the number of variables and constraints in the formulation grows exponentially with the size of the network. The second formulation is the *link-based formulation* (see Box 6.3). This formulation is much more efficient than the path-based formulation, as it only grows polynomially with the size of the network. Therefore, our method as described in Box 6.1 uses the link-based formulation. It is, however, harder to see that the link-based formulation can be used to solve the repeater-allocation problem. Yet, the link-based formulation is equivalent to the path-based formulation, as we show in Section 6.3.3.

The structure of the paper is as follows. In the remainder of this section, we present our method for solving the repeater-allocation problem and introduce both the intuitive path-based formulation and the efficient link-based formulation. Next, in Section 6.2, we first give an example of the use of our method on a real fiber network in the Netherlands. We also study the behaviour and performance of the method on a large number of randomly-generated network graphs. Furthermore, we present ways in which our method can be extended, and we discuss its limitations. Finally, in Section 6.3, we argue that the path-based formulation can indeed be used to solve the repeater-allocation problem, we give an example of a rate-fidelity analysis, we sketch a proof of the equivalence of the path-

*Instead of a minimum rate and fidelity, one can also use the minimum value(s) for other performance metric(s), as long as these can be lower bounded by upper bounding the number of repeaters and elementary link lengths of a quantum-repeater chain.

based formulation and the link-based formulation, we explain how we generate random network graphs and we present the scaling of the two ILP formulations.

6.1.1 Path-Based Formulation

6

The main idea behind the path-based formulation, which is shown in Box 6.2, is to enumerate and then choose paths for every $(s, t) \in \mathcal{Q}$, where \mathcal{Q} is the set of all ordered pairs of end nodes as defined in Equation (6.2). A path between s and t is a sequence of elementary links that does not contain any loops and connects s and t . Quantum-repeater nodes are then allocated in such a way that they enable the chosen paths to be used. This can be considered an instance of the set cover problem [4]. To guarantee a minimum rate R_{\min} and fidelity F_{\min} , we require every chosen path to contain at most N_{\max} quantum-repeater nodes, and we require every elementary link in the path to be at most L_{\max} long. N_{\max} and L_{\max} are functions of R_{\min} and F_{\min} , and what these functions look like depends on the specific quantum-repeater implementation under consideration. For an example of how N_{\max} and L_{\max} can be derived from R_{\min} and F_{\min} , see Section 6.3.2. Furthermore, to guarantee the network is robust, we choose K different paths per end-node pair. They are chosen such that none of the K paths share a quantum-repeater node or an elementary link. Finally, to account for the finite capacity of quantum repeaters, we choose the paths such that every quantum-repeater node is only used by at most D different paths. It can be intuitively understood that any quantum network accommodating the use of all these paths, will satisfy all network requirements considered in this paper.

Box 6.2: Path-based formulation.

$$\min \sum_{u \in \mathcal{R}} y_u \quad (6.5)$$

$$\text{s.t.} \quad L((u, v))x_p \leq L_{\max} \quad \forall (u, v) \in \mathcal{P}, p \in \mathcal{P} \quad (6.6)$$

$$|p|x_p \leq N_{\max} + 1 \quad \forall p \in \mathcal{P} \quad (6.7)$$

$$\sum_{p \in \mathcal{P}_q} x_p = K \quad \forall q \in \mathcal{Q} \quad (6.8)$$

$$\sum_{p \in \mathcal{P}_q} r_{up}x_p \leq 1 \quad \forall u \in \mathcal{R}, q \in \mathcal{Q} \quad (6.9)$$

$$\sum_{p \in \mathcal{P}} r_{up}x_p \leq Dy_u \quad \forall u \in \mathcal{R} \quad (6.10)$$

$$x_p \in \{0, 1\} \quad \forall p \in \mathcal{P} \quad (6.11)$$

$$y_u \in \{0, 1\} \quad \forall u \in \mathcal{R} \quad (6.12)$$

$$\text{where} \quad (6.13)$$

$$r_{up} = \begin{cases} 1 & \text{if } p \text{ uses } u \text{ as a repeater} \\ 0 & \text{otherwise} \end{cases} \quad \forall u \in \mathcal{R}, p \in \mathcal{P} \quad (6.14)$$

Key to the path-based formulation are the binary decision variables x_p , which are defined for every path $p \in \mathcal{P} = \cup_{(s,t) \in \mathcal{Q}} \mathcal{P}_{(s,t)}$, where $\mathcal{P}_{(s,t)}$ is the set of all possible paths from end node s to end node t . The elementary links that can be contained by a path $p \in \mathcal{P}_{(s,t)}$ must all be in $\mathcal{E}_{(s,t)}$, which is defined in Equation (6.3). Each x_p has value 1 when p is considered part of the chosen set of paths, and 0 otherwise. Furthermore, there are the binary decision variables y_u for all $u \in \mathcal{R}$. y_u is 1 if a quantum repeater is placed at potential repeater location u , and 0 otherwise. Constraints (6.6) to (6.10) guarantee that these variables are chosen such that all network requirements are satisfied. The objective function (6.5) ensures that they are chosen such that the total number of quantum-repeater nodes is minimized. It is argued that solutions to the path-based formulation are indeed solutions to the repeater-allocation problem in Section 6.3.1.

The path-based formulation requires us to define one variable x_p corresponding to each path $p \in \mathcal{P}$. Hence, the total number of variables as well as the number of constraints are at least $|\mathcal{P}|$, which is $O(|\mathcal{N}|!)$. Therefore the size of the input to the ILP solver scales exponentially with the number of nodes. This makes the path-based formulation unsuitable for designing quantum networks based on large fiber networks. Our implementation of the path-based formulation in CPLEX can be found in the repository [5]. In the next section, we give a more efficient formulation.

6.1.2 Link-Based Formulation

Here we present the link-based formulation, which can be found in Box 6.3. This formulation is inspired by the capacitated facility location problem [4]. Instead of choosing which

paths to use, we choose which elementary links to use. Quantum repeaters can then be placed such that each chosen elementary link is enabled. To this end, for each end-node pair $q \in \mathcal{Q}$, for every elementary link $(u, v) \in \mathcal{E}_q$ and for $k = 1, 2, \dots, K$, we define the binary decision variable $x_{uv}^{q,k}$. It can be thought of as indicating whether elementary link (u, v) is used in the k^{th} path used to connect end node s to end node t , where $q = (s, t)$. Furthermore, we again use the variables y_u that indicate whether node $u \in \mathcal{R}$ is used as a quantum-repeater node.

Box 6.3: Link-based formulation.

$$\min \sum_{u \in \mathcal{R}} y_u \quad (6.15)$$

$$\text{such that} \quad (6.16)$$

$$\sum_{\substack{v \\ (u,v) \in \mathcal{E}_q}} x_{uv}^{q,k} - \sum_{\substack{v \\ (v,u) \in \mathcal{E}_q}} x_{vu}^{q,k} \quad (6.17)$$

$$= \begin{cases} 1, & \text{if } u = s \\ -1, & \text{if } u = t \\ 0, & \text{if } u \in \mathcal{R} \end{cases} \quad \forall u \in \mathcal{R} \cup \{s, t\}, q = (s, t) \in \mathcal{Q}, k = 1, 2, \dots, K \quad (6.18)$$

$$L((u, v)) x_{uv}^{q,k} \leq L_{\max} \quad \forall (u, v) \in \mathcal{E}_q, q \in \mathcal{Q}, k = 1, 2, \dots, K \quad (6.19)$$

$$\sum_{(u,v) \in \mathcal{E}_q} x_{uv}^{q,k} \leq N_{\max} + 1 \quad \forall q \in \mathcal{Q}, k = 1, 2, \dots, K \quad (6.20)$$

$$\sum_{\substack{v \\ (u,v) \in \mathcal{E}_q}} \sum_{k=1}^K x_{uv}^{q,k} \leq 1 \quad \forall u \in \mathcal{R}, q \in \mathcal{Q} \quad (6.21)$$

$$\sum_{k=1}^K x_{st}^{q,k} \leq 1 \quad \forall q \in \mathcal{Q} \quad (6.22)$$

$$\sum_{q \in \mathcal{Q}} \sum_{\substack{v \\ (u,v) \in \mathcal{E}_q}} \sum_{k=1}^K x_{uv}^{q,k} \leq D y_u \quad \forall u \in \mathcal{R} \quad (6.23)$$

$$x_{uv}^{q,k} \in \{0, 1\} \quad \forall (u, v) \in \mathcal{E}_q, q \in \mathcal{Q}, k = 1, 2, \dots, K \quad (6.24)$$

$$y_u \in \{0, 1\} \quad \forall u \in \mathcal{R} \quad (6.25)$$

Because the number of elementary links scales polynomially with the number of nodes, both the number of variables and the number of constraints also scale polynomially with the number of nodes $|\mathcal{N}|$. In particular, they are $O(|\mathcal{N}|^2)$ (see Section 6.3.5 for a derivation). Our implementation of the link-based formulation in CPLEX can be found in the

repository [5].

In Section 6.3.3, we sketch the proof of the equivalence of the path-based formulation and the link-based formulation. Furthermore, we sketch why the variables $x_{uv}^{q,k}$ and y_u still provide a solution to the link-based formulation after performing step 7 of Box 6.1. The reason this step is included in our method is because, otherwise, elementary links could be included in the solution which are not necessary to meet the network requirements. The detailed version of the proof can be found in the supplementary material. Since the link-based formulation scales much more favourably with the size of the fiber network under consideration, it is more efficient to use this formulation when solving the repeater-allocation problem for large networks.

6.2 Discussion

In this section we illustrate our method as implemented by the link-based formulation using the Python API of CPLEX version 12.9 [3]. The corresponding code can be found in the repository [5]. Furthermore, we investigate the effect of varying network-requirement parameters and discuss possible extensions and limitations of our method.

6.2.1 Example on a Real Network

Here, we demonstrate our method by solving the repeater-allocation problem for a real fiber network. The fiber network that we consider is the core network of SURFnet. The latter is a network provider for Dutch educational and research institutions and has provided us with the network data, which is available in the repository [5]. The network graph is depicted in Figure 6.2.

As end nodes of the network, we have chosen the cities of Delft, Enschede, Groningen and Maastricht. In this example, we consider an entanglement-based quantum network utilizing massive multiplexing as described in e.g. [6]. For the end nodes, we require a minimum rate of $R_{\min} = 1$ Hz (one entangled state per second) and a fidelity to a maximally entangled state $F_{\min} = 0.93$. Furthermore, we set the robustness parameter to $K = 2$ (thus requiring that any single quantum repeater or elementary link in the network can break down without compromising network functionality), and we set the capacity parameter to $D = 4$ (which, in this case, means that we assume each quantum repeater can perform four Bell-state measurements simultaneously).

The first step of our method requires us to calculate the L_{\max} and N_{\max} corresponding to the minimal rate and fidelity we have chosen. This requires us to study the behaviour of a quantum-repeater chain consisting of $N + 1$ elementary links of length L each. L_{\max} and N_{\max} then have to be chosen as the largest possible values for L and N respectively such that the repeater chain still achieves the required rate and fidelity. Here, we make a couple of simplifying assumptions to make the calculations more tractable. Particularly, we assume elementary links generate Werner states, and we assume that the only losses are due to fiber attenuation and probabilistic Bell-state measurements (which we take to have a 50% success probability). In Section 6.3.2, we perform the calculation and find that for an elementary-link fidelity $F_{\text{link}} = 0.99$, number of multiplexing modes $M = 1000$, speed of light in fiber $c_{\text{fiber}} = 200,000$ km/s and attenuation length $L_{\text{att}} = 22$ km, we have $N_{\max} = 6$ and $L_{\max} = 136$ km.

The rest of the steps of the method in Box 6.1 have been performed using a Python

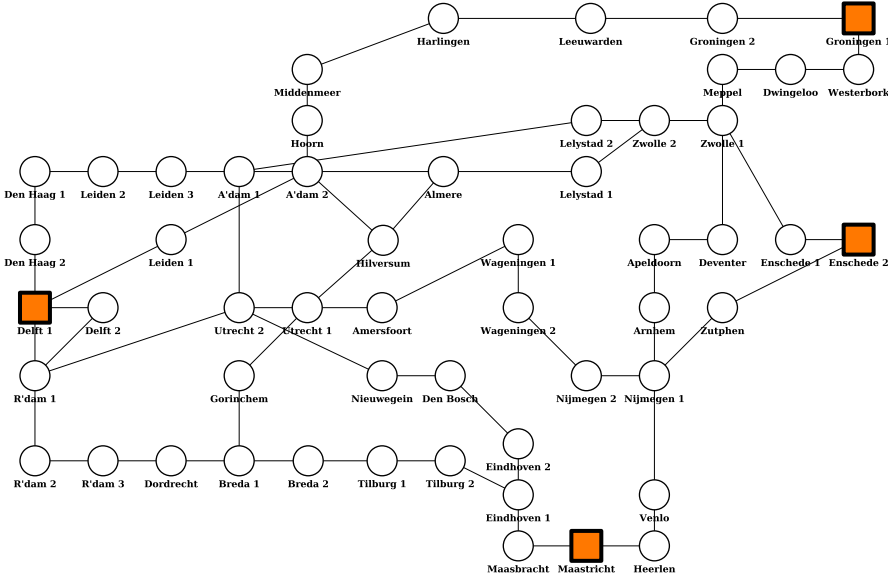


Figure 6.2: Graph representation of SURFnet core network. Node locations roughly correspond to geographical locations but have been adjusted for readability. Lengths of fibers connecting nodes are not shown. Nodes that are used as end nodes are shown as orange squares. Potential repeater locations are shown as white circles. A'dam and R'dam are used as abbreviations for Amsterdam and Rotterdam respectively.

script and CPLEX [5]. The resulting solution is shown graphically in Figure 6.3. All chosen repeater nodes are shown as blue hexagons, while all fibers that are used in elementary links are drawn as thick lines. We see that repeaters are placed around Groningen in order to bridge the large distance to the other end nodes without exceeding the maximum elementary-link length L_{\max} . Additionally, placing quantum-repeater nodes close to Groningen means they can be used for several of Groningen's outgoing connections. There are multiple such nodes close together because each only has a limited capacity ($D = 4$), and the redundancy increases the robustness of the network.

On our setup (see Section 6.1), it took us approximately 74 seconds to find the optimal solution to the link-based formulation for this network. Note that a feasible solution is a combination of decision variable values that satisfy all the constraints, while the optimal solution is a feasible solution that also minimizes the objective function.

6.2.2 Effect of Network-Requirement Parameters

Here, we demonstrate and investigate the effect of the different network-requirement parameters on the outcome of our method. The network-requirement parameters are, in principle, the minimum rate R_{\min} , the minimum fidelity F_{\min} , the robustness parameter K and the capacity parameter D . However, since R_{\min} and F_{\min} are translated into a maximum number of repeaters N_{\max} and a maximum elementary-link length L_{\max} in our

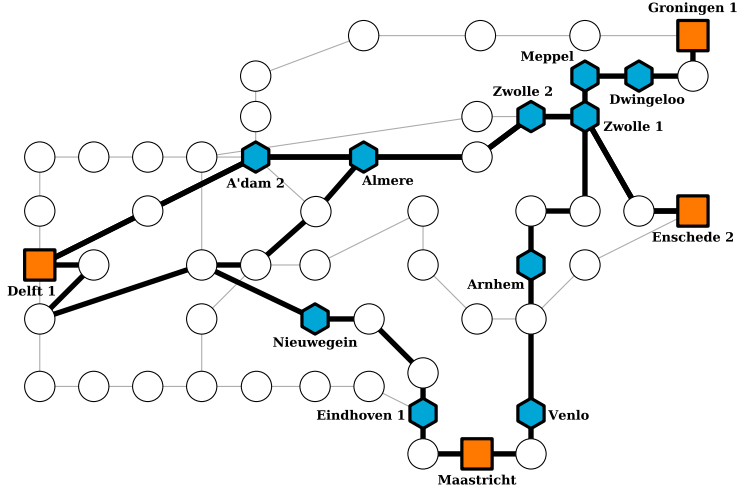


Figure 6.3: Solution to the repeater-allocation problem for $R_{\min} = 1$ Hz, $F_{\min} = 0.93$, $K = 2$ and $D = 4$. The network graph used as input corresponds to the SURFnet network, depicted in Figure 6.2. End nodes are shown as orange squares, quantum-repeater nodes are shown as blue hexagons and the fibers that are used in the elementary links are highlighted with thick lines.

6

method, we here consider the network-requirement parameters to be L_{\max} , N_{\max} , K and D . This way, we can keep our discussion agnostic about the exact hardware used to create a quantum network and how R_{\min} and F_{\min} are mapped to N_{\max} and L_{\max} .

First we give a visual demonstration on how the different network-requirement parameters affect the repeater placement. To this end, we have created a network graph with end nodes in the corners of the network and 10 possible repeater locations randomly distributed in between the end nodes. For details on how the graph was obtained, see Section 6.3.4. While keeping the network fixed, we vary the network-requirement parameters D , K and L_{\max} . In Figures 6.4a to 6.4c, we explore how the robustness parameter influences the total number of required quantum repeaters. Since each repeater has a capacity of $D = 6$ to distribute entanglement between the six end-node pairs, and because the network is set up in such a way that each path needs exactly one quantum-repeater node to connect end nodes without elementary links exceeding $L_{\max} = 0.9$, the optimal solution always contains K repeaters. In Figures 6.4d to 6.4f on the other hand, we see that as the capacity of quantum repeaters is varied from $D = 1$ to $D = 3$, the required number of quantum repeaters decreases when D increases. Note that since $K = 1$, the optimal solution here always happens to contain $\lceil Q/D \rceil$ repeaters. Finally, in Figures 6.4g to 6.4i we see that as we allow for longer elementary links to be used, the total number of repeaters is decreased. If we would increase L_{\max} even further, at a certain point every end node can be connected to another end node with a direct elementary link and hence the number of repeaters will drop to zero. The degeneracy of the optimal solution is visible from the fact that the solutions with two repeaters for $K = 2$ (Figure 6.4b), $D = 3$ (Figure 6.4f) and $L_{\max} = 0.75$ (Figure 6.4h) are not equal. In Section 6.2.4, it is discussed how this degeneracy can be lifted. We do not show the effect of N_{\max} . Since the total number of repeaters is

already minimized, changing the value of N_{\max} does not change the repeater allocation, but only determines whether a feasible solution exists at all.

Considering how the repeater placement on a single network varies with the network-requirement parameters can offer insight into how our method operates. However, it does not provide a general investigation into the properties of our method. In order to make more general and quantitative statements about our method, we will next consider the effect of varying network-requirement parameters on the repeater allocation for an ensemble of random networks. In this work, we construct random network graphs using random geometric graphs. That is, network graphs are constructed by scattering nodes randomly on a unit square. Edges are put only between nodes if the Euclidean distance separating them is smaller than some number, which is called the radius of the random geometric graph. The nodes which form the convex hull of the network are chosen as end nodes, so that the others are potential repeater locations. This choice is motivated by the fact that any potential-repeater locations that do not lie between end nodes would probably not play an important role anyway. For a more elaborate account of how we generate random network graphs, see Section 6.3.4.

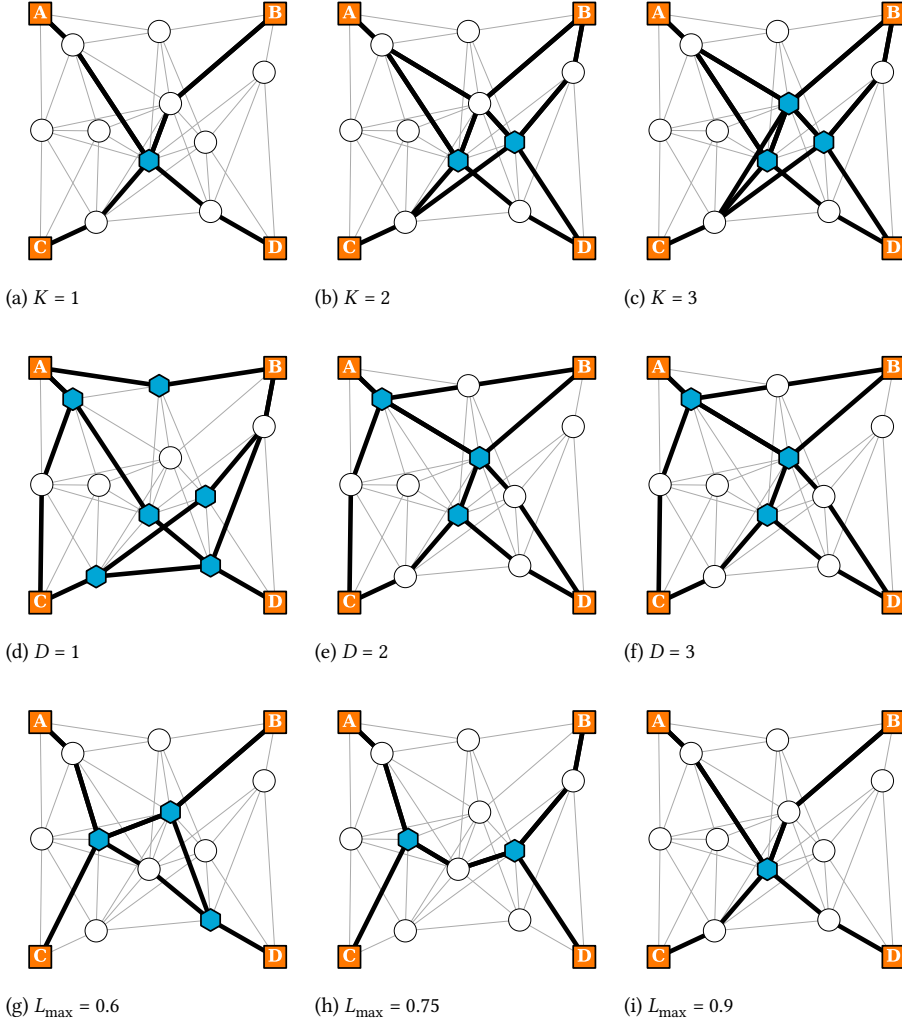


Figure 6.4: Solutions obtained using our method for an example network graph using the network-requirement parameters $L_{\max} = 0.9$, $N_{\max} = 3$, $K = 1$ and $D = 6$, unless noted otherwise in the caption of a specific solution. **(a)-(c)** Visualization of the effect of K . A higher robustness implies that we require more repeaters. **(d)-(f)** Visualization of the effect of D . As the capacity of quantum-repeater nodes increases, multiple paths can use the same repeater and hence the overall number of repeaters decreases. **(g)-(i)** Visualization of the effect of L_{\max} . When longer elementary-link lengths are allowed, less quantum-repeater nodes are required to bridge the distance between end nodes.

We here report how the number of placed repeaters and the (vertex) connectivity of quantum networks designed using our method vary as a function of the network-requirement parameters. The number of placed repeaters is interesting to consider since the aim of our method is to minimize this. On the other hand, the connectivity is interesting since it lower bounds the minimum number of quantum repeaters that need to break down before any pair of end nodes becomes disconnected, thereby giving an indication

of how robust a quantum network is. Note that connectivity is not the same as the robustness parameter K , which lower bounds the minimum number of quantum repeaters or elementary links that need to break down before end nodes can no longer distribute entanglement with a minimum rate and fidelity, while at the same time taking repeater capacity into account. We have first generated 1000 random network graphs for which our method was able to find solutions for the parameter values $L_{\max} = 0.9$, $N_{\max} = 6$, $K = 6$ and $D = 4$. Then, while keeping all other parameters constant, we have varied each of the parameters D , K and L_{\max} . This has been done in such a way that all considered values are less restrictive than the original values, such that we can be sure that a solution exists for each parameter value. Of each resulting quantum network, we determine the number of repeaters and the connectivity, and for each parameter value we determine the average number of repeaters and the average connectivity over all 1000 quantum networks.

In Figure 6.5 (a) and (b), we show the number of repeaters and the connectivity as a function of the repeater capacity D . We see that both the number of repeaters and the connectivity decrease as D increases, and they both accurately follow an exponential fit in the domain under consideration. In Figure 6.5 (c) and (d), we show how the number of repeaters and connectivity vary as a function of the robustness parameter K . We see that both increase linearly in the domain under consideration. For $D(K)$ the number of repeaters decreases (increases) following the same line of reasoning as we mentioned above for the visual demonstration. Generally, we expect the connectivity to follow the change in the number of repeaters, because a network with less quantum repeaters is easier to disconnect. Finally, in Figure 6.5, we investigate the effect of L_{\max} on the number of repeaters and connectivity. While the number of repeaters decreases, the connectivity increases, although they both flatten from $L_{\max} = 1.2$. The number of repeaters does not decrease to zero because $K = 6$. Therefore, even if L_{\max} is large enough to allow for paths between end nodes with zero quantum-repeater nodes, there are still at least five quantum-repeater nodes required to make the network robust against the breakdown of direct elementary links between end nodes. On the other hand, the connectivity increases since it also takes paths through other end nodes into account in its computation, and with an increasing value of L_{\max} , we expect more direct elementary links to appear.

6.2.3 Computation Times

Even though the link-based formulation has a scaling of $O(|\mathcal{N}|^2)$ in terms of the number of variables and constraints, it remains an ILP. In general, ILP's are NP-hard and thus generally require an exponential amount of time to solve. In order to investigate the performance of our method for varying network sizes, we determined the computation time for finding an optimal solution as a function of the number of nodes. The result is shown in Figure 6.6, in which we see that the computation time indeed increases exponentially. Nonetheless, instances on random geometric graphs with 100 nodes can be solved to optimality in about one minute on our setup (see Section 6.1).

The computation time can be strongly affected by the network topology and the chosen parameter values, since these can alter the difficulty of finding an optimal solution as well as the number of variables and constraints (see Section 6.3.5). However, the parameters that we use for Figure 6.6 are neither very strict nor loose and provide us with insight into the approximate scaling of the computation time, rather than the worst-case behavior. Note that we expect that, in practical use cases, the topology and the parameter values

will be determined once and remain more or less fixed, which implies that the repeater-allocation problem will not need to be solved repeatedly. This makes the increasingly large computation time for sizable graphs or stringent parameters less problematic.

6

6.2.4 Extensions

There are various ways in which our method can be extended. Here, we present two possible extensions. Such extensions change the ILP formulation in Box 6.3. The result of these is the generalized link-based formulation, which is presented in Box 6.4. To incorporate the extensions into the method in Box 6.1, the generalized link-based formulation must be used where otherwise the link-based formulation would be used.

Box 6.4: Generalized link-based formulation.

$$\min \sum_{u \in \mathcal{R}} \left(y_u + \alpha \sum_{q \in \mathcal{Q}} \sum_{(u,v) \in \mathcal{E}_q} \sum_{k=1}^{K^q} L((u,v)) x_{uv}^{q,k} \right) \quad (6.26)$$

$$\text{such that} \quad (6.27)$$

$$\begin{aligned} \sum_{\substack{v \\ (u,v) \in \mathcal{E}_q}} x_{uv}^{q,k} - \sum_{\substack{v \\ (v,u) \in \mathcal{E}_q}} x_{vu}^{q,k} \\ = \begin{cases} 1, & \text{if } u = s \\ -1, & \text{if } u = t \\ 0, & \text{if } u \in \mathcal{R} \end{cases} \quad \forall u \in \mathcal{R} \cup \{s, t\}, q = (s, t) \in \mathcal{Q}, k = 1, 2, \dots, K^q \end{aligned} \quad (6.28)$$

$$L((u,v)) x_{uv}^{q,k} \leq L_{\max}^q \quad \forall (u,v) \in \mathcal{E}_q, q \in \mathcal{Q}, k = 1, 2, \dots, K^q \quad (6.29)$$

$$\sum_{(u,v) \in \mathcal{E}_q} x_{uv}^{q,k} \leq N_{\max}^q + 1 \quad \forall q \in \mathcal{Q}, k = 1, 2, \dots, K^q \quad (6.30)$$

$$\sum_{\substack{v \\ (u,v) \in \mathcal{E}_q}} \sum_{k=1}^{K^q} x_{uv}^{q,k} \leq 1 \quad \forall u \in \mathcal{R}, q \in \mathcal{Q} \quad (6.31)$$

$$\sum_{k=1}^{K^q} x_{st}^{q,k} \leq 1 \quad \forall q \in \mathcal{Q} \quad (6.32)$$

$$\sum_{q \in \mathcal{Q}} \sum_{\substack{v \\ (u,v) \in \mathcal{E}_q}} \sum_{k=1}^{K^q} x_{uv}^{q,k} \leq D_u y_u \quad \forall u \in \mathcal{R} \quad (6.33)$$

$$x_{uv}^{q,k} \in \{0, 1\} \quad \forall (u,v) \in \mathcal{E}_q, q \in \mathcal{Q}, k = 1, 2, \dots, K^q \quad (6.34)$$

$$y_u \in \{0, 1\} \quad \forall u \in \mathcal{R} \quad (6.35)$$

The first extension we can make is solving the repeater-allocation problem in case of heterogeneous network requirements. So far, we have considered the network requirements to be homogeneous, i.e. the same throughout the network. However, it can be the case that some end nodes require a higher rate and fidelity, that some end nodes need access to more robust quantum communication, or that quantum repeaters with a larger capacity can be placed at some potential repeater locations than at other. Then, we can define the network-requirement parameters on a per-end-node-pair or per-node basis. Specifically, for every pair of end nodes $q \in \mathcal{Q}$, we define the minimum rate R_{\min}^q and fidelity F_{\min}^q of entanglement generation, and the required robustness parameter K^q (in order to break

communication between the end nodes q , at least K^q quantum repeaters or elementary links must be incapacitated). Furthermore, for every potential repeater location $u \in \mathcal{R}$, we define the quantum-repeater capacity D_u . To incorporate this into the method, the input parameters must be adapted accordingly, and the maximum number of repeaters and maximum elementary-link length must be calculated for every pair of end nodes separately (i.e. L_{\max}^q and N_{\max}^q must be determined from R_{\min}^q and F_{\min}^q for each $q \in \mathcal{Q}$).

A second extension has to do with the fact that the link-based formulation in Box 6.3 typically has a highly-degenerate optimal solution. That is, often there are multiple possible quantum-repeater placements for which all constraints are satisfied and the total number of quantum-repeater nodes is minimal. However, it might be the case that some solutions are more desirable than others. To pick out these solutions, one can define a secondary objective. This secondary objective can then be taken into account by defining a corresponding objective function, and adding it to the existing objective function, while scaling it such that it does not influence the optimal number of repeaters. In particular, the scale factor α should be chosen such that the secondary objective value does not exceed 1. This can be seen as a form of weighted goal programming [7]. As an example, in Box 6.4, we use as secondary objective to minimize the total length of all used elementary links. Other secondary objectives, such as minimizing the largest elementary-link length, could be implemented in a similar fashion.

6

6.2.5 Limitations

In this section we discuss some of the limitations of the method we present in this work. Each limitation represents a way that our method could be further extended, but is beyond the scope of this paper.

A first major limitation is the complexity of ILP's. While we provide an efficient ILP formulation, in which the number of variables and constraints scales polynomially with the network size, it remains an ILP. This cannot be helped, as choosing whether a repeater should be placed at a certain potential repeater location is inherently binary. In general, it is NP-hard to solve an ILP. While we indeed observe exponential scaling of the computation time in Section 6.2.3, we are able to find optimal solutions of realistically-sized networks within tractable time using CPLEX, which is also demonstrated using a real network in Section 6.2.1. Conceivably, one can use heuristics or approximation algorithms to obtain solutions faster, although the solutions then may no longer be optimal.

Another limitation that we consider here is the fact that our method is agnostic about how elementary links are constructed. We assume that any number of fibers can be combined to form an elementary link. However, quantum-repeater protocols relying on heralded entanglement generation typically require the presence of a midpoint station with the capability to perform Bell-state measurements [8]. If there are constraints on the placement of such stations, our method is insufficient. Conceivably, if such stations can only be placed at potential repeater locations, a modified version of our method could be used. Furthermore, we assume that an elementary link between two nodes is always constructed from the fibers which minimize the elementary-link length such that rate and fidelity are maximized. However, if one would like to incorporate the number of fibers (rather than elementary links) that need to be disabled before the quantum network is incapacitated as an additional network requirement (thereby guaranteeing more robustness), this may no longer be a useful assumption. It may then be better to try to construct different ele-

mentary links from different fibers as much as possible, such that individual fibers do not become too critical.

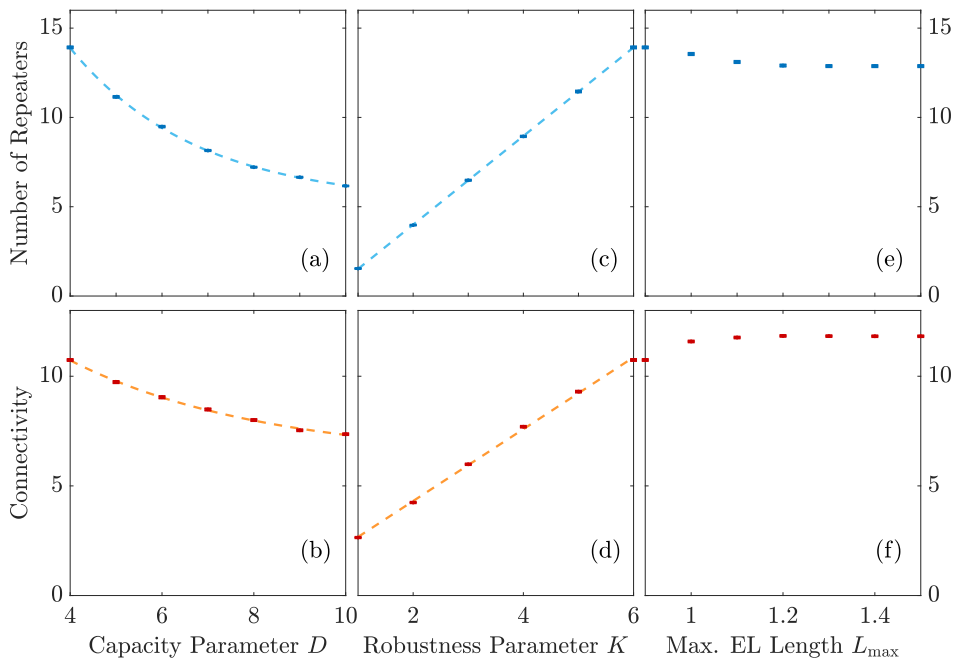


Figure 6.5: Simulation on 1000 random geometric graphs with a radius of 0.9 and $n = 25$ nodes for varying network parameters. We use $L_{\max} = 0.9$, $N_{\max} = 6$, $K = 6$ and $D = 4$, and except for the varied parameter. In the plots, each of the points represents the average number of placed repeaters or average connectivity over all samples for each value of (a)-(b) the capacity parameter D , (c)-(d) the robustness parameter K or (e)-(f) the maximum elementary-link length L_{\max} . We either use a linear or an exponential function for the fits. The error bars represent one standard deviation of the mean. Solving an instance to optimality requires approximately 30 seconds on average.

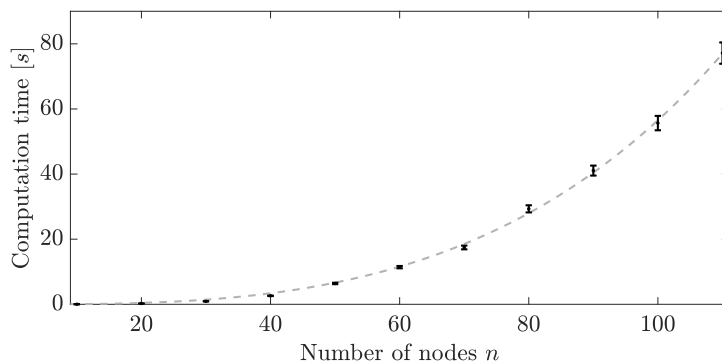


Figure 6.6: Computation time in seconds for 100 random geometric graphs with $L_{\max} = 1$, $N_{\max} = 6$, $K = 2$ and $D = 8$ for varying number of nodes n . The error bars represent one standard deviation of the mean. For the fit we have used an exponential function of the form $a(e^{bn^3} - 1)$, where a and b are free parameters.

6.3 Methods

6.3.1 Explanation of the Path-Based Formulation

In Section 6.1.1, we introduced the path-based formulation. This ILP formulation can be found in Box 6.2, and we claim that solutions to the path-based formulation can be used to construct solutions to the repeater-allocation problem. Here, we show how and why this can be done.

The idea behind the path-based formulation is to choose a combination of feasible paths that minimize the overall number of utilized repeaters. If a path is chosen that uses potential repeater location $u \in \mathcal{R}$ as a quantum-repeater node, a repeater should be placed at u . The binary variables x_p are used to parameterize the chosen paths, while the binary variables y_u are used to parameterize where quantum repeaters should be placed. A coupling between these variables is realized by Constraints (6.10): if a path $p \in \mathcal{P}$ is chosen in which a node $u \in \mathcal{R}$ is used as quantum-repeater node, the corresponding y_u variables must have value 1. Conversely, when $y_u = 1$ for a given repeater node $u \in \mathcal{R}$, up to D paths can use this repeater node in order for the corresponding constraint to hold, thereby also imposing a limit on the repeater capacity. After all, if $\sum_{p \in \mathcal{P}} r_{up} x_p > D$ then more than D paths are chosen in which node $u \in \mathcal{R}$ is used as a repeater, which renders the solution infeasible.

Paths are moreover only considered useful if they can be used to deliver entanglement between end nodes with the minimum required rate R_{\min} and fidelity F_{\min} . In the path-based formulation, this is implemented by requiring chosen paths to contain at most $N_{\max} + 1$ elementary links, each with a length of at most L_{\max} . The values of N_{\max} and L_{\max} can be determined from R_{\min} and F_{\min} as detailed in Box 6.1. These requirements are straightforwardly enforced by Constraints (6.6) and (6.7). Constraints (6.6) can only hold when $x_p = 0$ for all paths that contain an elementary link $((u, v) \in p)$ which is too long ($L((u, v)) > L_{\max}$). Similarly, Constraints (6.7) can only hold when $x_p = 0$ for all paths for which the number of elementary links ($|p|$) exceeds the maximum ($N_{\max} + 1$).

Furthermore, the choice of paths must be such that it is guaranteed that up to K potential repeater nodes or elementary links can break down before there is no path available between any pair of end nodes that can deliver entanglement at the required rate and fidelity. This is implemented by choosing, per pair of end nodes, K different paths. All of these paths are chosen such that none of them share a quantum-repeater node. Since elementary links connect quantum-repeater nodes, this automatically also means that none of the paths share an elementary link. Therefore, when a quantum-repeater node or elementary link becomes incapacitated, this can disrupt at most one path between a pair of end nodes. When there are K break downs, in the worst case, this can disrupt all paths between a pair of end nodes. But as long as there are fewer break downs, there will be at least one path available.

Since every chosen path can deliver entanglement at the required rate and fidelity, this guarantees robustness of the quantum network against up to K break downs. It is enforced by Constraints (6.8) that there are exactly K paths chosen between every pair of end nodes. Furthermore, Constraints (6.9) make sure that the number of chosen paths connecting a pair of end nodes using u as a quantum-repeater node ($\sum_{p \in \mathcal{P}_q} r_{up} x_p$) is at most one, thereby guaranteeing that all K paths are disjoint. Note that, when considering the quantum-repeater capacity, all chosen paths are taken into account. In other words,

Constraints (6.10) guarantee that the repeater capacity is not exceeded when all paths are used simultaneously. Therefore, if one path between a pair of end nodes is disrupted and they are forced to switch to another path, it is guaranteed that none of the quantum repeaters along that path are overloaded.

It is now easy to obtain a solution to the repeater-allocation problem from the solution to the path-based formulation. Every potential repeater location $u \in \mathcal{R}$ for which $y_u = 1$ in the solution to the path-based formulation should be used as a quantum-repeater node. Furthermore, each elementary link which is part of a chosen path $((u, v) \in p \text{ such that } x_p = 1)$ should be constructed. This is done using the fibers making it up $(F((u, v)))$. Then, the resulting quantum network will be such that all network requirements are satisfied. Furthermore, the number of quantum-repeater nodes will be minimal. This is because this number, which is exactly $\sum_{u \in \mathcal{R}} y_u$, is minimized by the objective function (6.5) of the path-based formulation. Therefore, the path-based formulation can indeed be used to solve the repeater-allocation problem.

6.3.2 Toy-Model Calculation of N_{\max} and L_{\max} from R_{\min} and F_{\min}

In this section we calculate the maximum number of repeaters and maximum elementary-link length from the minimum required rate R_{\min} and fidelity F_{\min} using a toy model of a quantum-repeater chain. The quantum-repeater architecture that we consider is of the massively-multiplexed type as described in e.g. [6]. The toy model that we consider here makes the following simplifying assumptions:

- the states distributed over elementary links are Werner states,
- the noise in the states distributed over elementary links is the only noise,
- the only sources of photon loss are fiber attenuation and non-deterministic Bell-state measurements,
- all processes except light traveling through fiber are instantaneous.

It is shown in the supplementary material that in this model, a repeater chain with N quantum repeaters, M entanglement-distribution attempts per round per elementary link, elementary-link length L , elementary-link fidelity F_{link} , speed of light in fiber c_{fiber} and a 50% Bell-state measurement success probability has the following end-to-end rate R and fidelity F :

$$R = \frac{c_{\text{fiber}}}{L} \left(\frac{1}{2} \right)^N \left[1 - \left(1 - \frac{1}{2} e^{-L/L_{\text{att}}} \right)^M \right]^{N+1}, \quad (6.36)$$

$$F = \frac{1}{4} \left[1 + 3 \left(\frac{4F_{\text{link}} - 1}{3} \right)^{N+1} \right]. \quad (6.37)$$

N_{\max} can now be obtained from the fidelity. Specifically, it is the lowest-integer solution to the equation

$$F > F_{\min}. \quad (6.38)$$

To find L_{\max} , we can put the resulting value of N_{\max} into the equation

$$R > R_{\min}. \quad (6.39)$$

The smallest value for L that solves Equation (6.39) is then L_{\max} . Note that the calculation here is somewhat simplified because the fidelity is not a function of L_{\max} . If both fidelity and rate would be functions of N and L , there would not exist a unique solution. In that case, there is some freedom in choosing N_{\max} and L_{\max} .

The calculation of N_{\max} and L_{\max} for the example parameters $F_{\min} = 0.93$, $R_{\min} = 1$ Hz, $F_{\text{link}} = 0.99$, $c_{\text{fiber}} = 200,000$ km/s, $M = 1000$ and $L_{\text{att}} = 22$ km results in $N_{\max} = 6$ and $L_{\max} = 136$ km (rounded down).

6.3.3 Proof of Equivalence

In this section we briefly outline the proof of why the path-based formulation and the link-based formulation are equivalent. The main idea is to use an optimal solution to the path-based formulation to construct a feasible solution to the link-based formulation and vice versa. We prove that this is always possible in such a way that the value of the objective function of the constructed feasible solution is the same as that of the original optimal solution. This can be used to show that the optimal objective values of both formulations are always the same. Therefore, the feasible solution to one formulation constructed from an optimal solution to another formulation is itself an optimal solution. We say that two ILP formulations are equivalent if optimal solutions to one can be obtained from the other and vice versa, and therefore we conclude that the path-based formulation and the link-based formulation are equivalent.

To construct a solution to the link-based formulation using a solution to the path-based formulation, we use the elementary links that appear in chosen paths. More specifically, for each $q = (s, t) \in \mathcal{Q}$ and $k = 1, 2, \dots, K$, we set $x_{uv}^{q,k} = 1$ if elementary link $(u, v) \in \mathcal{E}_q$ is in the k^{th} chosen path connecting s and t . Conversely, Constraints (6.18) guarantee that, for every $q = (s, t) \in \mathcal{Q}$ and $k = 1, 2, \dots, K$, the elementary links $(u, v) \in \mathcal{E}_q$ for which $x_{uv}^{q,k} = 1$ can be used to form exactly one path between s and t . These paths can be obtained by using Algorithm 1, which outputs the set \mathcal{P}^* that contains the extracted paths over all $q \in \mathcal{Q}$ and $k = 1, 2, \dots, K$. Thus, we can construct a solution to the path-based formulation from a solution to the link-based formulation by setting $x_p = 1$ for all $p \in \mathcal{P}^*$. Furthermore, the repeater-placement variables y_u are kept the same when translating between formulations.

By comparing the different constraints, it can be understood that if a solution to one formulation is feasible, the solution to the other formulation that can be obtained from it is also feasible. Constraints (6.6) and (6.19) both guarantee that elementary-link lengths do not exceed L_{\max} , while Constraints (6.7) and (6.20) both guarantee that each path includes N_{\max} quantum-repeater nodes at maximum. Constraints (6.8) and (6.18) make sure there are K paths between each pair of end nodes. These paths are guaranteed to be disjoint for the path-based formulation by Constraints (6.9) and for the link-based formulation by Constraints (6.21) and (6.22). Lastly, Constraints (6.10) and (6.23) couple the x variables to the y variables and make sure the quantum-repeater capacity is taken into account.

In step 7 of Box 6.1, we manually set $x_{uv}^{q,k} = 0$ for all elementary links $(u, v) \in \mathcal{E}$ which are not in one of the paths $p \in \mathcal{P}^*$. We do this because, on some occasions, the variables $x_{uv}^{q,k}$ are allowed to have value 1 in such a way that they form loops (which are disjoint from the path between s and t). For example, it could be the case that for some $q \in \mathcal{Q}$ and $k = 1, 2, \dots, K$, it holds that $x_{u_1 u_2}^{q,k} = x_{u_2 u_1}^{q,k} = 1$, which does not violate any of the constraints in

Box 6.3, and also does not influence the objective function (6.15). Since these loops do not connect end nodes, they do not contribute to realizing any of the network requirements. Therefore, any variable $x_{uv}^{q,k}$ with value 1 such that it is part of a loop can safely be set to 0 without violating any constraint. This is shown rigorously in the supplementary material. Only allowing for elementary links which are part of paths between end nodes realizes the removal of such loops. Since the method in Box 6.1 recommends the construction of elementary link $(u, v) \in \mathcal{E}$ if $x_{uv}^{q,k} = 1$, setting them to 0 whenever this is possible helps to prevent the construction of unnecessary elementary links. One way in which the appearance of loops in optimal solutions can be prevented in the first place by is to use the generalized link-based formulation in Box 6.4. In this formulation, the minimization of the total elementary-link length is used as secondary objective.

6.3.4 Generating Random Networks

Here, we describe how we generate random network graphs based on random geometric graphs. These networks are used to demonstrate our method and study the effect of different network-requirement parameters in Section 6.2.2.

The recipe for generating a random geometric graph on a two-dimensional Euclidean space with n nodes and radius d is as follows [9]. First, n points are distributed uniformly at random on a unit square, by sampling both their horizontal and vertical coordinates uniformly at random. To every two points p_1, p_2 we associate $r(p_1, p_2)$, which is the Euclidean distance between the two points. From this, an undirected weighted graph is constructed in which every node corresponds to one of the points, and edges between nodes corresponding to points p_1, p_2 are added if $r(p_1, p_2) \leq d$. The weight that is given to the edge is $r(p_1, p_2)$.

To turn a random geometric graph into a suitable network graph, it must be decided which of the nodes are end nodes, and which are potential repeater locations. To this end, we determine the convex hull of the graph. We choose to use nodes corresponding to vertices of the convex hull of the graph as end nodes, i.e. they make up the set \mathcal{E} . All other nodes are thus considered potential repeater locations, i.e. they make up the set \mathcal{R} . This method is used because it is expected that potential repeater locations lying outside of the area spanned by the end nodes will only rarely be chosen as quantum-repeater nodes. When the end nodes form the convex hull, there are no such potential repeater locations, and the number of nodes that are not of relevance to the repeater-allocation problem is minimized. We generate the random geometric graphs using NetworkX [10] and determine the convex hull using an algorithm [11] which is included in SciPy [12].

The random network graph used in Figure 6.4 has been based on a random geometric graph with $n = 10$ and $d = 0.6$, but has been further edited to be made suitable for demonstration purposes. Some nodes were displaced manually. Additionally, end nodes have been added at the corners of the unit square and connected to the three closest potential repeater locations.

6.3.5 Scaling of the Formulations

The path-based formulation relies on the enumeration of all the paths between two end nodes. For every pair $(s, t) \in \mathcal{Q}$ we must consider all possible permutations of intermediate nodes in which r repeaters are placed on a path. For $r = 0$, we get a single path directly

from s to t and for $r = 1$ we should consider all possible paths that utilize one repeater, which are $|\mathcal{R}|$ in total. Next, when $r = 2$ we must consider all paths that contain exactly two repeaters and additionally all permutations of the repeater placements in these paths, which gives $|\mathcal{R}|(|\mathcal{R}| - 1)$ paths in total, et cetera. The number of y_u variables is $|\mathcal{R}|$, so that the number of variables $n_{\text{var}}^{\text{pbf}}$ of the path-based formulation is given by

$$n_{\text{var}}^{\text{pbf}} = |\mathcal{R}| + |\mathcal{Q}||\mathcal{P}_q| \quad (6.40)$$

$$= |\mathcal{R}| + |\mathcal{Q}| \sum_{r=0}^{|\mathcal{R}|} \frac{|\mathcal{R}|!}{(|\mathcal{R}| - r)!}. \quad (6.41)$$

If $|\mathcal{R}| > 1$, this simplifies to [13]

$$n_{\text{var}}^{\text{pbf}} = |\mathcal{R}| + |\mathcal{Q}| \lceil e|\mathcal{R}|! \rceil, \quad (6.42)$$

where e denotes Euler's number and $\lceil \cdot \rceil$ represents the rounding operator. We assume that the number of end nodes $|\mathcal{E}|$, and therefore the number of end-node pairs $|\mathcal{Q}| = |\mathcal{E}|(|\mathcal{E}| - 1)/2$, is constant so that this does not scale with the total number of nodes $|\mathcal{N}|$ in our graph. This implies that the number of possible repeater locations $\mathcal{R} = \mathcal{N} \setminus \mathcal{E}$ scales linearly with the number of nodes. The number of variables, as well as the number of constraints, is thus $O(|\mathcal{N}|!)$.

One important detail of our implementation of the path-based formulation is that we take Constraints (6.6) and (6.7) into account while enumerating all the paths. If we encounter a path which contains an elementary link with a length that exceeds L_{max} or which uses more than N_{max} repeaters, we simply exclude it from the set \mathcal{P} . This can greatly reduce the total number of variables, although it will remain to scale exponentially with $|\mathcal{N}|$.

In the link-based formulation, we need to enumerate all the elementary links in the network. To this end, we need to count every elementary link from s to every node $v \in \mathcal{R} \cup \{t\}$, and from $u \in \mathcal{R}$ to t which results in $2|\mathcal{R}| + 1$ elementary links. Next, we also need to consider the elementary link from every node $u \in \mathcal{R}$ to $v \in \mathcal{R}$ and back, in order to allow for directional paths from s to t , which are $|\mathcal{R}|(|\mathcal{R}| - 1)$ in total. Additionally, since we use the index k for our $x_{uv}^{q,k}$ variables in order to keep track of the redundant paths that are required for the given level of robustness, we need to make a copy of these variables for every value of $k = 1, 2, \dots, K$. When we combine this with the $|\mathcal{R}|$ y_u variables, we get that the total number of variables of the link-based formulation is given by

$$n_{\text{var}}^{\text{lb}} = |\mathcal{R}| + K|\mathcal{Q}||\mathcal{E}_q| \quad (6.43)$$

$$= |\mathcal{R}| + K|\mathcal{Q}|(|\mathcal{R}|^2 + |\mathcal{R}| + 1), \quad (6.44)$$

which is $O(|\mathcal{N}|^2)$, if we assume that K is a fixed constant. Note that the link-based formulation therefore also has $O(|\mathcal{N}|^2)$ constraints.

Algorithm 1 Path extraction algorithm.

```

 $\mathcal{P}^* = \emptyset$ 
for  $q = (s, t) \in \mathcal{Q}$  do
  for  $k = 1, 2, \dots, K$  do
     $u_0 = s$ 
     $n = 0$ 
    while  $u_n \neq t$  do
      Find the unique node  $v \in \mathcal{R} \cup \{t\}$  for which  $x_{u_n v}^{q,k} = 1$ 
       $n = n + 1$ 
       $u_n = v$ 
    end while
     $p = ((s, u_1), (u_1, u_2), \dots, (u_{n-1}, t))$   $\mathcal{P}^* = \mathcal{P}^* \cup p$ 
  end for
end for

```

Data Availability

All the data and code we used for generating the results can be found in the Github repository [5].

Author Contributions

This work is based on the master thesis of J.R. which was devised by S.W. and supervised by S.W. and G.A.; K.C. introduced some key conceptual and proof ideas. J.R. proposed the use of linear programming and implemented both formulations with CPLEX and G.A. wrote most of the code for the simulations. All authors contributed to the manuscript.

6.4 Toy-Model Calculation of Rate and Fidelity

In this section, we calculate the rate and fidelity of a quantum-repeater chain using a toy model described in Section 6.3.2. The quantum-repeater architecture under consideration is of the massively-multiplexed type as described in e.g. [6]. In such a repeater chain, during every round of time, entanglement distribution is attempted a large number of times on each elementary link (using e.g. spectral multiplexing). If at the end of the round a quantum repeater has at least succeeded once at entanglement generation with each neighbour, a successfully-entangled state is selected from each side and entanglement swapping is performed between the two (through a Bell-state measurement). Otherwise, all entanglement is discarded and a new attempt is made during the next round. Our toy model of such a quantum-repeater chain is based on the following simplifying assumptions:

- the states distributed over elementary links are Werner states,
- the noise in the states distributed over elementary links is the only noise,
- the only sources of photon loss are fiber attenuation and non-deterministic Bell-state measurements,
- all processes except light traveling through fiber are instantaneous.

First, we investigate the final end-to-end fidelity of entangled quantum states created by a repeater chain. Let us consider a repeater chain with N quantum repeaters, M entanglement-distribution attempts per round per elementary link, elementary-link length L and elementary-link fidelity F_{link} . In the toy model, entangled states shared over elementary links are Werner states, which can be parametrized as

$$\rho_{p_{\text{link}}} = p_{\text{link}} |\Phi^+\rangle\langle\Phi^+| + \frac{1-p_{\text{link}}}{4} \mathbb{1}. \quad (6.45)$$

This state has fidelity to the maximally-entangled Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ of $F_{\text{link}} = \frac{1}{4}(1 + 3p_{\text{link}})$, and therefore $p_{\text{link}} = \frac{1}{3}(4F_{\text{link}} - 1)$.

Entanglement swapping between Werner states ρ_{p_1} and ρ_{p_2} is performed through a Bell-state measurement on one qubit from the first state and one qubit from the second state. The quantum state after this operation (after tracing out the measured qubits and ignoring possible Pauli corrections) is a new Werner state, $\rho_{p_{1,2}}$, with $p_{1,2} = p_1 p_2$. Repeated use of this equation reveals that, if entanglement distribution is successful at least once

in each of the $N + 1$ elementary links, and if all entanglement swaps are successful, the Werner state ρ_{p_f} is obtained with $p_f = p_{\text{link}}^{N+1}$. Thus, the final fidelity is

$$F = \frac{1 + 3p_{\text{link}}^{N+1}}{4} = \frac{1}{4} \left[1 + 3 \left(\frac{4F_{\text{link}} - 1}{3} \right)^{N+1} \right]. \quad (6.46)$$

Now we consider the rate at which end-to-end entanglement can be established. First, we calculate the probability that a single attempt at entanglement distribution in a single elementary link is successful. Entanglement is generated by sending entangled photons from both repeaters to a station in the center of the elementary link, where a probabilistic Bell-state measurement is performed with 50% success probability. In the toy model, the only other source of photon loss in the elementary link is attenuation in optical fiber, which we assume to be characterized by the attenuation length L_{att} . In that case, the probability that both photons reach the midpoint and the Bell-state measurement is successful is

$$\text{Pr}(\text{one attempt}) = \left(e^{-L/(2L_{\text{att}})} \right)^2 \times \frac{1}{2} = \frac{1}{2} e^{-L/L_{\text{att}}}. \quad (6.47)$$

Then, the probability that at least one of the M attempts in an elementary link in a single round is successful is

$$\text{Pr}(\text{elementary link}) = 1 - \left(1 - \text{Pr}(\text{one attempt}) \right)^M. \quad (6.48)$$

Finally, the end-to-end success probability is given by the probability that each link is successful, and that each entanglement swap in the repeaters is successful. Since entanglement swapping in repeaters has a 50% success probability, this gives

$$\text{Pr}(\text{repeater chain}) = \text{Pr}(\text{elementary link})^{N+1} \left(\frac{1}{2} \right)^N = \left(\frac{1}{2} \right)^N \left[1 - \left(1 - \frac{1}{2} e^{-L/L_{\text{att}}} \right)^M \right]^{N+1}. \quad (6.49)$$

To determine the rate, we now need to know how long every round takes. In the toy model, the only aspect of entanglement generation that takes any time is the photons traveling to the midpoints stations, and the messages heralding success or failure of the entanglement attempts traveling from the midpoint stations back to the repeaters. We assume both are light traveling through fiber. Thus, every round takes as long as it takes for light to travel the distance L through fiber. Denoting the speed of light in fiber c_{fiber} , this gives a round time of L/c_{fiber} , so that the repetition rate is c_{fiber}/L . The end-to-end entanglement distribution rate is obtained by multiplying the repetition rate with the success probability, given by

$$R = \frac{c_{\text{fiber}}}{L} \text{Pr}(\text{repeater chain}) = \frac{c_{\text{fiber}}}{L} \left(\frac{1}{2} \right)^N \left[1 - \left(1 - \frac{1}{2} e^{-L/L_{\text{att}}} \right)^M \right]^{N+1}. \quad (6.50)$$

6.5 Proof of Equivalence

In this section, we prove the equivalence between the link-based formulation and path-based formulation. In order to make this material self-contained, in Table 6.1 we reintroduce some of the notations. Next, in Section 6.5.1, we briefly re-describe both of the formulations. After that, in Sections 6.5.2 and 6.5.3, we show how to construct a feasible

solution to the link-based formulation from the optimal solution to the path-based formulation and vice versa. By combining this result with the proof that the optimal objective values are equal, we conclude that the two formulations are equivalent. Here, we consider two ILP formulations to be equivalent if an optimal solution to one formulation can be used to obtain an optimal solution to the other and vice versa.

\mathcal{Q}	Set of all ordered pairs (s, t) of end-nodes.
\mathcal{P}_q	Set of all possible paths for a pair $q \in \mathcal{Q}$.
\mathcal{P}	Set of all possible paths between all of the pairs $q \in \mathcal{Q}$.
\mathcal{E}_q	Set of all elementary links that can be used by a pair $q \in \mathcal{Q}$.
\mathcal{R}	Set of potential repeater locations in the network.
L_{\max}	Maximum length of an elementary link.
N_{\max}	Maximum number of repeaters in a path.
K	The robustness parameter, which denotes the minimum number of quantum-repeater nodes or elementary links (it can be any combination) that need to break down before one of the other requirements can no longer be met.
\mathcal{K}	Set of all integers from 1 to K (inclusive).
D	The capacity parameter, which denotes the number of quantum-communication sessions that one quantum repeater can facilitate simultaneously.

Table 6.1: Overview of the sets and parameters that are relevant for the proof.

6.5.1 Formulations

Here we will restate both the path-based and link-based formulation for completeness. In the path-based formulation, we define the binary decision variables x_p corresponding to a path $p \in \mathcal{P} = \cup_{(s,t) \in \mathcal{Q}} \mathcal{P}_{(s,t)}$, where $\mathcal{P}_{(s,t)}$ is the set of all possible paths from end node s to end node t . A path itself is a sequence of elementary links reaching from s to t that does not contain any loops. They have value 1 when p is considered part of the set of chosen paths, and 0 otherwise. Furthermore, we use the binary decision variables y_u^p for all $u \in \mathcal{R}$. Note that we introduce the superscript p here to more clearly distinguish between the two formulations, which differs from the main text. The variable y_u^p is 1 if a quantum repeater is placed at potential repeater location u , and 0 otherwise. The exact formulation is given in Box 6.5.

Box 6.5: Restated path-based formulation.

$$\min \sum_{u \in \mathcal{R}} y_u^p \quad (6.51)$$

$$\text{s.t.} \quad L((u, v))x_p \leq L_{\max} \quad \forall (u, v) \in p, p \in \mathcal{P} \quad (6.52)$$

$$|p|x_p \leq N_{\max} + 1 \quad \forall p \in \mathcal{P} \quad (6.53)$$

$$\sum_{p \in \mathcal{P}_q} x_p = K \quad \forall q \in \mathcal{Q} \quad (6.54)$$

$$\sum_{p \in \mathcal{P}_q} r_{up}x_p \leq 1 \quad \forall u \in \mathcal{R}, q \in \mathcal{Q} \quad (6.55)$$

$$\sum_{p \in \mathcal{P}} r_{up}x_p \leq Dy_u^p \quad \forall u \in \mathcal{R} \quad (6.56)$$

$$x_p \in \{0, 1\} \quad \forall p \in \mathcal{P} \quad (6.57)$$

$$y_u^p \in \{0, 1\} \quad \forall u \in \mathcal{R} \quad (6.58)$$

$$\text{where} \quad r_{up} = \begin{cases} 1 & \text{if } p \text{ uses } u \text{ as a repeater} \\ 0 & \text{otherwise} \end{cases} \quad \forall u \in \mathcal{R}, p \in \mathcal{P} \quad (6.59)$$

On the other hand, in the link-based formulation we define the binary decision variable $x_{uv}^{q,k}$ for each pair of end nodes $q = (s, t) \in \mathcal{Q}$, every elementary link $(u, v) \in \mathcal{E}_q$ and $k \in \mathcal{K} = \{1, 2, \dots, K\}$. These variables can be interpreted as indicating whether an elementary link (u, v) is used in the k^{th} path connecting the end nodes s and t . Furthermore, in the link-based formulation we use the variables y_u^l to indicate whether node $u \in \mathcal{R}$ is used as a quantum-repeater node. The exact formulation is given in Box 6.6.

Box 6.6: Restated link-based formulation.

$$\min \sum_{u \in \mathcal{R}} y_u^l \quad (6.60)$$

$$\text{such that} \quad (6.61)$$

$$\sum_{\substack{v \\ (u,v) \in \mathcal{E}_q}} x_{uv}^{q,k} - \sum_{\substack{v \\ (v,u) \in \mathcal{E}_q}} x_{vu}^{q,k} \quad (6.62)$$

$$= \begin{cases} 1, & \text{if } u = s \\ -1, & \text{if } u = t \\ 0, & \text{if } u \in \mathcal{R} \end{cases} \quad \forall u \in \mathcal{R} \cup \{s, t\}, q = (s, t) \in \mathcal{Q}, k \in \mathcal{K} \quad (6.63)$$

$$L((u, v)) x_{uv}^{q,k} \leq L_{\max} \quad \forall (u, v) \in \mathcal{E}_q, q \in \mathcal{Q}, k \in \mathcal{K} \quad (6.64)$$

$$\sum_{(u,v) \in \mathcal{E}_q} x_{uv}^{q,k} \leq N_{\max} + 1 \quad \forall q \in \mathcal{Q}, k \in \mathcal{K} \quad (6.65)$$

$$\sum_{\substack{v \\ (u,v) \in \mathcal{E}_q}} \sum_{k \in \mathcal{K}} x_{uv}^{q,k} \leq 1 \quad \forall u \in \mathcal{R}, q \in \mathcal{Q} \quad (6.66)$$

$$\sum_{k \in \mathcal{K}} x_{st}^{q,k} \leq 1 \quad \forall q \in \mathcal{Q} \quad (6.67)$$

$$\sum_{q \in \mathcal{Q}} \sum_{\substack{v \\ (u,v) \in \mathcal{E}_q}} \sum_{k \in \mathcal{K}} x_{uv}^{q,k} \leq D y_u^l \quad \forall u \in \mathcal{R} \quad (6.68)$$

$$x_{uv}^{q,k} \in \{0, 1\} \quad \forall (u, v) \in \mathcal{E}_q, q \in \mathcal{Q}, k \in \mathcal{K} \quad (6.69)$$

$$y_u^l \in \{0, 1\} \quad \forall u \in \mathcal{R} \quad (6.70)$$

6.5.2 From the Path-Based Formulation to the Link-Based Formulation

In this section we will construct a solution to the link-based formulation from the optimal solution to the path-based formulation. We then proceed by proving that this newly constructed solution is indeed a feasible solution to the link-based formulation, i.e. that it satisfies all constraints.

From the optimal solution to the path-based formulation we can use the values of the variables x_p and y_u^p to assign values to our new binary decision variables $\tilde{x}_{uv}^{q,k}$ and \tilde{y}_u^l , which presumably give a solution to the link-based formulation, using Algorithm 2.

Algorithm 2 Methodology for assigning the values of $\tilde{x}_{uv}^{q,k}$ and \tilde{y}_u^l .

```

For all  $q \in \mathcal{Q}$ ,  $k \in \mathcal{K}$  and  $(u, v) \in \mathcal{E}_q$ , set  $\tilde{x}_{uv}^{q,k} = 0$  and for all  $u \in \mathcal{R}$ , set  $\tilde{y}_u^l = y_u^p$ 
for  $q \in \mathcal{Q}$  do  $k = 1$ 
  for  $p \in \mathcal{P}_q$  do
    if  $x_p = 1$  then
      for  $(u, v) \in p$  do
         $\tilde{x}_{uv}^{q,k} = 1$ 
      end for
       $k = k + 1$ 
    end if
  end for
end for
  
```

From Algorithm 2, we can see that for each pair $q \in \mathcal{Q}$ and value of $k \in \mathcal{K}$, we select a single, unique path p for which $x_p = 1$ (because there are exactly K paths with $x_p = 1$ in \mathcal{P}_q , due to Constraints (6.54)) and use its elementary links to assign the corresponding $\tilde{x}_{uv}^{q,k}$ variables to have value 1. Let us denote this path by $p^{q,k}$ for ease of notation in the remainder of this section.

Next, we will prove that the newly constructed solution is indeed feasible, by showing that all of the $\tilde{x}_{uv}^{q,k}$ and \tilde{y}_u^l variables satisfy all constraints of the link-based formulation.

Proposition 1 *The variables $\tilde{x}_{uv}^{q,k}$ that we obtain with Algorithm 2 satisfy Constraints (6.63) of the link-based formulation, i.e.*

$$\sum_{\substack{v \\ (u,v) \in \mathcal{E}_q}} \tilde{x}_{uv}^{q,k} - \sum_{\substack{v \\ (v,u) \in \mathcal{E}_q}} \tilde{x}_{vu}^{q,k} = \begin{cases} 1, & \text{if } u = s \\ -1, & \text{if } u = t \\ 0, & \text{if } u \in \mathcal{R} \end{cases} \quad \forall u \in \mathcal{R} \cup \{s, t\}, q = (s, t) \in \mathcal{Q}, k \in \mathcal{K}. \quad (6.71)$$

Proof: Consider the path $p^{q,k}$ for specific values of $q = (s, t) \in \mathcal{Q}$ and $k \in \mathcal{K}$, for which $x_{p^{q,k}} = 1$. This path starts at s and ends at t by construction, so there is exactly one node $v \in \mathcal{R} \cup \{t\}$ for which $\tilde{x}_{sv}^{q,k} = 1$ and hence $\sum_{v: (s,v) \in \mathcal{E}_q} \tilde{x}_{sv}^{q,k} = 1$. Additionally, since the set \mathcal{E}_q only contains outgoing edges from s , $\sum_{v: (v,s) \in \mathcal{E}_q} \tilde{x}_{vs}^{q,k}$ is an empty sum and thus, trivially, $\sum_{v: (v,s) \in \mathcal{E}_q} \tilde{x}_{vs}^{q,k} = 0$. This implies that

$$\sum_{\substack{v \\ (s,v) \in \mathcal{E}_q}} \tilde{x}_{sv}^{q,k} - \sum_{\substack{v \\ (v,s) \in \mathcal{E}_q}} \tilde{x}_{vs}^{q,k} = 1. \quad (6.72)$$

In a similar fashion, it must hold that there exists exactly one node $v \in \mathcal{R} \cup \{s\}$ such that $\tilde{x}_{vt}^{q,k} = 1$ and hence $\sum_{v: (v,t) \in \mathcal{E}_q} \tilde{x}_{vt}^{q,k} = 1$. Furthermore, since the set \mathcal{E}_q also only contains

the incoming edges to t , it follows trivially that $\sum_{v:(t,v) \in \mathcal{E}_q} \tilde{x}_{tv}^{q,k} = 0$, which implies that

$$\sum_{\substack{v \\ (t,v) \in \mathcal{E}_q}} \tilde{x}_{tv}^{q,k} - \sum_{\substack{v \\ (v,t) \in \mathcal{E}_q}} \tilde{x}_{vt}^{q,k} = -1. \quad (6.73)$$

If $p^{q,k}$ visits any other node $u \in \mathcal{R}$, it holds that there is exactly one incoming edge and one outgoing edge from this node, since a path cannot start nor end here and neither can a path contain loops by definition. In other words, there must be exactly one node $v \in \mathcal{R} \cup \{s\}$ for which $\tilde{x}_{vu}^{q,k} = 1$ and one node $v' \in \mathcal{R} \cup \{t\}$ (where $v \neq v'$) for which $\tilde{x}_{uv'}^{q,k} = 1$. This results in

$$\sum_{\substack{v \\ (u,v) \in \mathcal{E}_q}} \tilde{x}_{uv}^{q,k} - \sum_{\substack{v \\ (v,u) \in \mathcal{E}_q}} \tilde{x}_{vu}^{q,k} = 0 \quad \forall u \in \mathcal{R}. \quad (6.74)$$

Finally, if a node $u \in \mathcal{R}$ is not visited by $p^{q,k}$, there are no incoming and no outgoing edges. Thus, $\tilde{x}_{vu}^{q,k} = 0$ for all $v \in \mathcal{R} \cup \{s\}$, and $\tilde{x}_{uv'}^{q,k} = 0$ for all $v' \in \mathcal{R} \cup \{t\}$. As a result, Equation (6.74) is also satisfied in this case. The combination of (6.72), (6.73) and (6.74) for all $q \in \mathcal{Q}$ and $k \in \mathcal{K}$ concludes the proof. \square

Proposition 2 *The variables $\tilde{x}_{uv}^{q,k}$ that we obtain with Algorithm 2 satisfy Constraints (6.64) of the link-based formulation, i.e.*

$$L((u,v))\tilde{x}_{uv}^{q,k} \leq L_{\max} \quad \forall (u,v) \in \mathcal{E}_q, q \in \mathcal{Q}, k \in \mathcal{K}. \quad (6.75)$$

Proof: Consider the path $p^{q,k}$ for specific values of $q = (s,t) \in \mathcal{Q}$ and $k \in \mathcal{K}$. Because $x_{p^{q,k}} = 1$ by definition, it follows from Constraints (6.52) that any elementary link $(u,v) \in p^{q,k}$ has length $L((u,v)) \leq L_{\max}$. Since $\tilde{x}_{uv}^{q,k} = 1$ only if (u,v) is in $p^{q,k}$, it follows that every elementary link for which $\tilde{x}_{uv}^{q,k} = 1$ must have a length smaller than or equal to L_{\max} . Because this argument can be made for any $q \in \mathcal{Q}$ and any $k \in \mathcal{K}$, Constraints (6.64) are satisfied whenever $\tilde{x}_{uv}^{q,k} = 1$. Furthermore, they are trivially satisfied when $\tilde{x}_{uv}^{q,k} = 0$. \square

Proposition 3 *The variables $\tilde{x}_{uv}^{q,k}$ that we obtain with Algorithm 2 satisfy Constraints (6.65) of the link-based formulation, i.e.*

$$\sum_{(u,v) \in \mathcal{E}_q} \tilde{x}_{uv}^{q,k} \leq N_{\max} + 1 \quad \forall q \in \mathcal{Q}, k \in \mathcal{K}. \quad (6.76)$$

Proof: Consider the path $p^{q,k}$ for specific values of $q = (s,t) \in \mathcal{Q}$ and $k \in \mathcal{K}$, for which $x_{p^{q,k}} = 1$. According to Algorithm 2, $\tilde{x}_{uv}^{q,k} = 1$ only if $(u,v) \in p^{q,k}$. Hence, the number of $(u,v) \in \mathcal{E}_q$ for which $\tilde{x}_{uv}^{q,k} = 1$ is the same as the number of elementary links in $p^{q,k}$, which is $|p^{q,k}|$. Thus,

$$|p^{q,k}| = |p^{q,k}|x_{p^{q,k}} = \sum_{(u,v) \in \mathcal{E}_q} \tilde{x}_{uv}^{q,k}, \quad (6.77)$$

where the first equality holds because $x_{p^{q,k}} = 1$ by definition of $p^{q,k}$. According to Constraints (6.53),

$$|p|x_p \leq N_{\max} + 1 \quad \forall p \in \mathcal{P}. \quad (6.78)$$

which implies

$$|p^{q,k}|x_{p^{q,k}} \leq N_{\max} + 1 \quad \forall q \in \mathcal{Q}, k \in \mathcal{K}. \quad (6.79)$$

If we substitute (6.77) into (6.79) we directly get that

$$\sum_{(u,v) \in \mathcal{E}_q} \tilde{x}_{uv}^{q,k} \leq N_{\max} + 1 \quad \forall q \in \mathcal{Q}, k \in \mathcal{K}. \quad (6.80)$$

□

Proposition 4 *The variables $\tilde{x}_{uv}^{q,k}$ that we obtain with Algorithm 2 satisfy Constraints (6.66) and (6.67) of the link-based formulation, i.e.*

$$\sum_{\substack{v \\ (u,v) \in \mathcal{E}_q}} \sum_{k \in \mathcal{K}} \tilde{x}_{uv}^{q,k} \leq 1 \quad \forall u \in \mathcal{R}, q \in \mathcal{Q} \quad (6.81)$$

and

$$\sum_{k \in \mathcal{K}} \tilde{x}_{st}^{q,k} \leq 1 \quad \forall q \in \mathcal{Q}. \quad (6.82)$$

Proof: Consider the path $p^{q,k}$ for specific values of $q = (s, t) \in \mathcal{Q}$ and $k \in \mathcal{K}$, for which $x_{p^{q,k}} = 1$. According to Equation (6.59), the parameter $r_{up^{q,k}} = 1$ if the potential repeater location $u \in \mathcal{R}$ is in $p^{q,k}$. If this is the case, the path $p^{q,k}$ contains exactly one outgoing elementary link at u , and thus $\sum_{v: (u,v) \in \mathcal{E}_q} \tilde{x}_{uv}^{q,k} = 1$. Otherwise, there are no outgoing elementary links, and $\sum_{v: (u,v) \in \mathcal{E}_q} \tilde{x}_{uv}^{q,k} = 0$. Therefore,

$$r_{up^{q,k}} = \sum_{\substack{v \\ (u,v) \in \mathcal{E}_q}} \tilde{x}_{uv}^{q,k}. \quad (6.83)$$

Furthermore, we note that

$$\sum_{p \in \mathcal{P}_q} r_{up} x_p = \sum_{k \in \mathcal{K}} r_{up^{q,k}}, \quad (6.84)$$

since the paths $p \in \mathcal{P}_q$ for which $x_p = 1$ are exactly the paths that were labeled $p^{q,k}$ for some $k \in \mathcal{K}$. Combining Equations (6.83) and (6.84), and repeating this argument for every $u \in \mathcal{R}$ and $q \in \mathcal{Q}$ then gives

$$\sum_{p \in \mathcal{P}_q} r_{up} x_p = \sum_{\substack{v \\ (u,v) \in \mathcal{E}_q}} \sum_{k \in \mathcal{K}} \tilde{x}_{uv}^{q,k} \quad \forall u \in \mathcal{R}, q \in \mathcal{Q}. \quad (6.85)$$

We can then substitute (6.85) directly into (6.55), in order to get

$$\sum_{\substack{v \\ (u,v) \in \mathcal{E}_q}} \sum_{k \in \mathcal{K}} \tilde{x}_{uv}^{q,k} \leq 1 \quad \forall u \in \mathcal{R}, q \in \mathcal{Q}, \quad (6.86)$$

which are exactly Constraints (6.66).

Additionally, the set \mathcal{P}_q for $q = (s, t) \in \mathcal{Q}$ contains the path consisting of the direct elementary link (s, t) exactly once. Furthermore, no other paths containing (s, t) can exist because there exist no incoming edges to s nor outgoing edges from t in \mathcal{E}_q . If the path $p^{q,k'}$ is this direct path, then $\tilde{x}_{st}^{q,k'} = 1$. But because $p^{q,k}$ cannot contain (s, t) for $k \neq k'$, it holds that $\tilde{x}_{st}^{q,k} = 0$ for $k \neq k'$. Therefore,

$$\sum_{k \in \mathcal{K}} \tilde{x}_{st}^{q,k} = \tilde{x}_{st}^{q,k'} + \sum_{\substack{k \in \mathcal{K} \\ k \neq k'}} \tilde{x}_{st}^{q,k} = 1. \quad (6.87)$$

On the other hand, if there is no k' such that $p^{q,k'}$ is the direct path,

$$\sum_{k \in \mathcal{K}} \tilde{x}_{st}^{q,k} = 0. \quad (6.88)$$

In any case, the sum evaluates to smaller than or equal to 1. Since this argument holds for any $q \in \mathcal{Q}$, we can conclude that

$$\sum_{k \in \mathcal{K}} \tilde{x}_{st}^{q,k} \leq 1 \quad \forall q \in \mathcal{Q}. \quad (6.89)$$

□

Proposition 5 *The variables $\tilde{x}_{uv}^{q,k}$ and \tilde{y}_u^l that we obtain with Algorithm 2 satisfy Constraints (6.68) of the link-based formulation, i.e.*

$$\sum_{q \in \mathcal{Q}} \sum_{\substack{v \\ (u,v) \in \mathcal{E}_q}} \sum_{k \in \mathcal{K}} \tilde{x}_{uv}^{q,k} \leq D \tilde{y}_u^l \quad \forall u \in \mathcal{R}. \quad (6.90)$$

Proof: If we sum over all $q \in \mathcal{Q}$ on both sides of (6.85), we get

$$\sum_{q \in \mathcal{Q}} \sum_{p \in \mathcal{P}_q} r_{up} x_p = \sum_{p \in \mathcal{P}} r_{up} x_p = \sum_{q \in \mathcal{Q}} \sum_{\substack{v \\ (u,v) \in \mathcal{E}_q}} \sum_{k \in \mathcal{K}} \tilde{x}_{uv}^{q,k} \quad \forall u \in \mathcal{R}. \quad (6.91)$$

Substituting (6.91) into (6.56) then results in

$$\sum_{q \in \mathcal{Q}} \sum_{\substack{v \\ (u,v) \in \mathcal{E}_q}} \sum_{k \in \mathcal{K}} \tilde{x}_{uv}^{q,k} \leq D \tilde{y}_u^l \quad \forall u \in \mathcal{R}. \quad (6.92)$$

Finally, since we assign all the values of \tilde{y}_u^l to have the same values as y_u^p for all $u \in \mathcal{R}$ in Algorithm 2, we conclude that

$$\sum_{q \in \mathcal{Q}} \sum_{\substack{v \\ (u,v) \in \mathcal{E}_q}} \sum_{k \in \mathcal{K}} \tilde{x}_{uv}^{q,k} \leq D \tilde{y}_u^l \quad \forall u \in \mathcal{R}. \quad (6.93)$$

□

This concludes the proof that the variables we obtain from the optimal solution to the path-based formulation using Algorithm 2 provide a feasible solution to the link-based formulation. One important statement we make about the objective value of this newly constructed feasible solution is that

$$\sum_{u \in \mathcal{R}} y_u^p = \sum_{u \in \mathcal{R}} \tilde{y}_u^l \geq \sum_{u \in \mathcal{R}} y_u^l, \quad (6.94)$$

where $\sum_{u \in \mathcal{R}} y_u^l$ represents the optimal objective value of the link-based formulation. In other words, the objective value of the newly constructed feasible solution will always be greater than or equal to the objective value of the optimal solution, since we are solving a minimization problem.

6.5.3 From the Link-Based Formulation to the Path-Based Formulation

6

In this section we will go the other way around and construct a solution to the path-based formulation from the optimal solution to the link-based formulation using the path extraction algorithm, outlined in Algorithm 1. First, we show that the application of this algorithm indeed leads to valid paths, after which we proceed by proving that this newly constructed solution is a feasible solution to the path-based formulation.

From the optimal solution to the link-based formulation, we can use the values of the variables $x_{uv}^{q,k}$ and y_u^l to assign the values to our new binary decision variables \tilde{x}_p and \tilde{y}_u^p , which presumably give a solution to the path-based formulation. We do this by setting $\tilde{y}_u^p = y_u^l$ for all $u \in \mathcal{R}$, $\tilde{x}_p = 1$ for all $p \in \mathcal{P}^*$ and $\tilde{x}_p = 0$ for all $p \in \mathcal{P} \setminus \mathcal{P}^*$, where the set \mathcal{P}^* is obtained from the path extraction algorithm. It follows from Proposition 6 that this can always be done. Note that in the path extraction algorithm, to every $q \in \mathcal{Q}$ and $k \in \mathcal{K}$ there is a single path associated. We label this path $p^{q,k}$ for the remainder of this section. It follows that $x_{p^{q,k}} = 1$ for all $q \in \mathcal{Q}$ and $k \in \mathcal{K}$.

Proposition 6 *Algorithm 1 is always successful. That is, it is always able to construct the set \mathcal{P}^* such that $\mathcal{P}^* \subseteq \mathcal{P}$.*

Proof: We will prove this proposition by proving that Algorithm 3 can always successfully construct a sequence $\bar{p}^{q,k}$ and moreover that this sequence forms a valid path (i.e. $\bar{p}^{q,k} \in \mathcal{P}$). Because Algorithm 1 is nothing but the repeated application of Algorithm 3 (with $\mathcal{P}^* = \cup_{q,k} p^{q,k}$), it then follows that this proposition holds.

Algorithm 3 Path extraction sub-algorithm.

```

 $u_0 = s$ 
 $n = 0$ 
while  $u_n \neq t$  do
    Find the unique node  $v \in \mathcal{R} \cup \{t\}$  for which  $x_{u_n v}^{q,k} = 1$ 
     $n = n + 1$ 
     $u_n = v$ 
end while
 $\bar{p}^{q,k} = ((u_0, u_1), (u_1, u_2), \dots, (u_n, u_n))$ 

```

The first time when the algorithm enters the while loop, it has to find the single node v for which $x_{s v}^{q,k} = 1$. To prove that there exists exactly one such node, we consider Constraints (6.63) for $u = s$. Because there is no incoming elementary link at s , i.e. there is no v' such that $(v', s) \in \mathcal{E}_q$, the second summation is empty and the equation reduces to

$$\sum_{\substack{v \\ (s,v) \in \mathcal{E}_q}} x_{s v}^{q,k} = 1. \quad (6.95)$$

Since the variables $x_{u v}^{q,k}$ are binary, this implies that there is exactly one v such that $x_{s v}^{q,k} = 1$.

Now, we assume that $u = u_i$ such that $u_i \neq s$ and $u_i \neq t$ and show there is a unique v such that $x_{u_i v}^{q,k} = 1$. First, we combine Constraints (6.66) with the fact that

$$\sum_{\substack{v \\ (u_i, v) \in \mathcal{E}_q}} x_{u_i v}^{q,k} \leq \sum_{\substack{v \\ (u_i, v) \in \mathcal{E}_q}} \sum_{k \in \mathcal{K}} x_{u_i v}^{q,k}, \quad (6.96)$$

to find that

$$\sum_{\substack{v \\ (u_i, v) \in \mathcal{E}_q}} x_{u_i v}^{q,k} \leq 1. \quad (6.97)$$

From Constraints (6.63) with $u_i \in \mathcal{R}$ we find that

$$\sum_{\substack{v \\ (u_i, v) \in \mathcal{E}_q}} x_{u_i v}^{q,k} = \sum_{\substack{v \\ (v, u_i) \in \mathcal{E}_q}} x_{v u_i}^{q,k} \quad \forall q \in \mathcal{Q}, k \in \mathcal{K}. \quad (6.98)$$

We know that the left-hand side of this equation is upper bounded by 1 because of Equation (6.97). Furthermore, because node u_i was selected by Algorithm 3 (when entering the while loop for $u = u_{i-1}$), we know that $x_{u_{i-1} u_i}^{q,k} = 1$. This implies that the right-hand side is at least one. Therefore, both sides must be equal to one. Because the variables are binary, the equality of the right-hand side to 1 implies there is exactly one v such that $x_{u_i v}^{q,k} = 1$.

This procedure only concludes if there is an n such that $u_n = t$. This must be the case, as there is only a finite number of nodes in \mathcal{N} , and two nodes u_k, u_l cannot be the same unless $k = l$. To see that this last property holds, assume for the moment that there are a

k and $l > k$ such that $u_k = u_l$. In that case, by virtue of how Algorithm 3 works, it must be the case that $x_{u_{k-1}u_k}^{q,k} = x_{u_{l-1}u_l}^{q,k} = 1$. Since we concluded earlier that there can only be one v such that $x_{vu}^{q,k} = 1$, this implies that $u_{l-1} = u_{k-1}$. Then, the above argument can be repeated to find $u_{l-2} = u_{k-2}$. This can be continued until we find that $u_{l-k} = u_{k-k} = u_0 = s$. Because $l - k > 0$, u_{l-k} can only be in $\bar{p}^{q,k}$ if $x_{u_{l-k-1}u_{l-k}}^{q,k} = x_{u_{l-k-1}s}^{q,k} = 1$. However, this variable is not defined, because there is no elementary link $(v, s) \in \mathcal{E}_q$ for any $v \in \mathcal{N}$. We have thus reached a contradiction, and we can conclude that $u_k \neq u_l$ as long as $k \neq l$ and thus Algorithm 3 must eventually terminate.

At this point we can conclude that Algorithm 3 creates the sequence

$$\bar{p}^{q,k} = ((u_0, u_1), (u_1, u_2), (u_2, u_3), \dots, (u_{n-1}, u_n)) \quad (6.99)$$

for some integer n , where $u_0 = s$ and $u_n = t$. Clearly, this is a sequence of adjacent elementary links which connect the end node s to the end node t . Furthermore, since we concluded that $u_k \neq u_l$ for $k \neq l$, there are no loops, and thus $\bar{p}^{q,k}$ is in fact a path $\bar{p}^{q,k} = p^{q,k} \in \mathcal{P}$. Since $p^{q,k} \in \mathcal{P}$, the variable $\tilde{x}_{p^{q,k}}$ is well-defined and can be set to 1.

□

Next, we address the fact that optimal solutions to the link-based formulation can contain chosen elementary links that form loops, which do not contribute to satisfying constraints, but also do not violate them. To avoid the construction of ineffective elementary links, we define the variables $\tilde{x}_{uv}^{q,k}$ for all $q \in \mathcal{Q}$, $k \in \mathcal{K}$ and $(u, v) \in \mathcal{E}_q$. We set $\tilde{x}_{uv}^{q,k} = 1$ if $(u, v) \in p$ for some $p \in \mathcal{P}^*$ and $\tilde{x}_{uv}^{q,k} = 0$ otherwise for all $q \in \mathcal{Q}$ and $k \in \mathcal{K}$, where \mathcal{P}^* is the output of Algorithm 1 when applied to the variables $x_{uv}^{q,k}$ (which are part of an optimal solution to the link-based formulation). In other words, $\tilde{x}_{uv}^{q,k}$ represent a choice of elementary links that corresponds to the optimal solution, but with all links that are not in any of the paths $p \in \mathcal{P}^*$ removed.

Proposition 7 *The variables $\tilde{x}_{uv}^{q,k}$ and y_u^l form an optimal solution to the link-based formulation.*

Proof: If the variables form a feasible solution, they also form an optimal solution, since the variables y_u^l are defined to be part of an optimal solution and the objective function is independent of the values of $\tilde{x}_{uv}^{q,k}$.

The variables form a feasible solution if they satisfy all constraints in Box 6.6 (but with $x_{uv}^{q,k}$ substituted by $\tilde{x}_{uv}^{q,k}$ everywhere). It is easily verified that Constraints (6.64 - 6.68) are satisfied. Each of these set an upper bound on sums over (linear functions of) $\tilde{x}_{uv}^{q,k}$ variables. Since $\tilde{x}_{uv}^{q,k}$ is either equal to $x_{uv}^{q,k}$ or set to 0, it always holds that $\tilde{x}_{uv}^{q,k} \leq x_{uv}^{q,k}$. Thus, replacing $x_{uv}^{q,k}$ variables by $\tilde{x}_{uv}^{q,k}$ variables can only decrease the summations. Since the $x_{uv}^{q,k}$ variables satisfy all constraints by assumption (and the bounds are unaltered), we can conclude that all of these constraints are also satisfied by the $\tilde{x}_{uv}^{q,k}$ variables.

To show that Constraints (6.63) are satisfied as well, consider the path $p^{q,k}$ for some specific $q = (s, t) \in \mathcal{Q}$ and $k \in \mathcal{K}$. By definition, $\tilde{x}_{uv}^{q,k} = 1$ if and only if $(u, v) \in p^{q,k}$. By virtue of Proposition 6, we know that $p^{q,k}$ is a valid path between s and t , i.e.

$$p^{q,k} = ((u_0, u_1), (u_1, u_2), \dots, (u_{n_1}, u_n)) \quad (6.100)$$

for some integer n , where $u_0 = s$, $u_n = t$, $u_i \in \mathcal{R}$ for $0 < i < n$, and $u_i \neq u_j$ for $i \neq j$.

Consider Constraints (6.63) for $u = s$. $\bar{x}_{sv}^{q,k} = 1$ holds if and only if $v = u_1$, and thus $\sum_{v:(s,v) \in \mathcal{E}_q} \bar{x}_{sv}^{q,k} = \bar{x}_{su_1}^{q,k} = 1$. Furthermore, since there are no incoming elementary links at s , i.e. $(v, s) \notin \mathcal{E}_q$ for all $v \in \mathcal{R} \cup \{s, t\}$, $\sum_{v:(v,s) \in \mathcal{E}_q} \bar{x}_{vs}^{q,k} = 0$ trivially. Therefore,

$$\sum_{(s,v) \in \mathcal{E}_q} \bar{x}_{sv}^{q,k} - \sum_{(v,s) \in \mathcal{E}_q} \bar{x}_{vs}^{q,k} = 1 \quad (6.101)$$

and therefore, Constraints (6.63) hold for $u = s$.

When $u = t$, we can make a similar argument: $\bar{x}_{vt}^{q,k} = 1$ holds if and only if $v = u_{n-1}$, and thus $\sum_{v:(v,t) \in \mathcal{E}_q} \bar{x}_{vt}^{q,k} = 1$. Furthermore, there are no elementary links leaving t , i.e. there is no $v \in \mathcal{R} \cup \{s, t\}$ such that $(t, v) \in \mathcal{E}_q$. Therefore, $\sum_{v:(t,v) \in \mathcal{E}_q} \bar{x}_{tv}^{q,k} = 0$ trivially. Thus we can conclude Constraints (6.63) hold for $u = t$, i.e.

$$\sum_{(t,v) \in \mathcal{E}_q} \bar{x}_{tv}^{q,k} - \sum_{(v,t) \in \mathcal{E}_q} \bar{x}_{vt}^{q,k} = -1. \quad (6.102)$$

When $u \in \mathcal{R}$, it can be the case that there is an i such that $u = u_i$ for $1 < i < n$. Then, $\bar{x}_{u_i v}^{q,k} = 1$ holds if and only if $v = u_{i+1}$, and therefore $\sum_{v:(u_i, v) \in \mathcal{E}_q} \bar{x}_{u_i v}^{q,k} = \bar{x}_{u_i u_{i+1}}^{q,k} = 1$. Furthermore, $\bar{x}_{v u_i}^{q,k} = 1$ holds if and only if $v = u_{i-1}$, and therefore $\sum_{v:(v, u_i) \in \mathcal{E}_q} \bar{x}_{v u_i}^{q,k} = \bar{x}_{u_{i-1} u_i}^{q,k} = 1$. On the other hand, if there is no i such that $u = u_i$, u is not on the path. It then holds by definition that $\bar{x}_{uv}^{q,k} = \bar{x}_{vu}^{q,k} = 0$ for all $v \in \mathcal{R} \cup \{s, t\}$. In both cases, it follows directly that

$$\sum_{(u,v) \in \mathcal{E}_q} \bar{x}_{uv}^{q,k} - \sum_{(v,u) \in \mathcal{E}_q} \bar{x}_{vu}^{q,k} = 0. \quad (6.103)$$

Therefore, Constraints (6.63) also holds for $u \in \mathcal{R}$. We conclude that all constraints hold, and thus $\bar{x}_{uv}^{q,k}$ and y_u^l together form an optimal solution to the link-based formulation. \square

Note that, by definition, for all $q \in \mathcal{Q}$ and $k \in \mathcal{K}$, there are no elementary links $(u, v) \in \mathcal{E}_q$ such that $\bar{x}_{uv}^{q,k} = 1$ which are not in the path $p^{q,k}$. This property, together with Proposition 7, makes it easier to show that all constraints of the path-based formulation are satisfied for the variables \tilde{x}_p .

Proposition 8 *The variables \tilde{x}_p that we obtain satisfy Constraints (6.52) of the path-based formulation, i.e.*

$$L((u, v))\tilde{x}_p \leq L_{\max} \quad \forall (u, v) \in p, p \in \mathcal{P}. \quad (6.104)$$

Proof: Every path p for which $\tilde{x}_p = 1$ is equal to $p^{q,k}$ for some $q \in \mathcal{Q}$ and $k \in \mathcal{K}$. For every elementary link (u, v) that makes up $p^{q,k}$ it holds that $\bar{x}_{uv}^{q,k} = 1$. Therefore, due to Constraints (6.64), each elementary link $(u, v) \in p^{q,k}$ must have length $L((u, v)) = L((u, v))\tilde{x}_{p^{q,k}} \leq L_{\max}$. For all paths p which are not equal to $p^{q,k}$ for some $q \in \mathcal{Q}$ and $k \in \mathcal{K}$, $\tilde{x}_p = 0$ and $L((u, v))\tilde{x}_p = 0 \leq L_{\max}$. Therefore, $L((u, v))\tilde{x}_p \leq L_{\max}$ holds for any $(u, v) \in p$ for any path $p \in \mathcal{P}$. \square

Proposition 9 *The variables \tilde{x}_p that we obtain satisfy Constraints (6.53) of the path-based formulation, i.e.*

$$|p|\tilde{x}_p \leq N_{\max} + 1 \quad \forall p \in \mathcal{P}. \quad (6.105)$$

Proof: Consider the path $p^{q,k}$ for specific values of $q = (s, t) \in \mathcal{Q}$ and $k \in \mathcal{K}$. By definition, the number of elementary links in $p^{q,k}$ is the same as the number of elementary links for which $\tilde{x}_{uv}^{q,k} = 1$. Thus,

$$\sum_{(u,v) \in \mathcal{E}_q} \tilde{x}_{uv}^{q,k} = |p^{q,k}| = |p^{q,k}| \tilde{x}_{p^{q,k}}. \quad (6.106)$$

Substituting (6.106) into (6.65) then gives

$$|p^{q,k}| \tilde{x}_{p^{q,k}} \leq N_{\max} + 1. \quad (6.107)$$

Furthermore, for any path $p \in \mathcal{P}$ which is not equal to $p^{q,k}$ for some $q \in \mathcal{Q}$ and $k \in \mathcal{K}$, it holds that $\tilde{x}_p = 0$ and thus $|p|\tilde{x}_p = 0 \leq N_{\max} + 1$. Therefore, we can conclude that $|p|\tilde{x}_p \leq N_{\max} + 1$ for any $p \in \mathcal{P}$. \square

Proposition 10 *The variables \tilde{x}_p that we obtain satisfy Constraints (6.54) of the path-based formulation, i.e.*

$$\sum_{p \in \mathcal{P}_q} \tilde{x}_p = K \quad \forall q \in \mathcal{Q}. \quad (6.108)$$

Proof: Consider the set \mathcal{P}_q for a specific value of $q \in \mathcal{Q}$. Every path $p \in \mathcal{P}_q$ has $\tilde{x}_p = 1$ if it is equal to $p^{q,k}$ for some $k \in \mathcal{K}$ and $\tilde{x}_p = 0$ otherwise. Therefore,

$$\sum_{p \in \mathcal{P}_q} \tilde{x}_p = \sum_{k \in \mathcal{K}} \tilde{x}_{p^{q,k}} = \sum_{k \in \mathcal{K}} 1 = K \quad \forall q \in \mathcal{Q}. \quad (6.109)$$

\square

Proposition 11 *The variables \tilde{x}_p that we obtain satisfy Constraints (6.55) of the path-based formulation, i.e.*

$$\sum_{p \in \mathcal{P}_q} r_{up} \tilde{x}_p \leq 1 \quad \forall u \in \mathcal{R}, q \in \mathcal{Q}. \quad (6.110)$$

Proof: Consider the path $p^{q,k}$ for specific values of $q = (s, t) \in \mathcal{Q}$ and $k \in \mathcal{K}$. The parameter $r_{up^{q,k}}$ is defined in Equation (6.59), and takes the value 1 if the path $p^{q,k}$ passes the potential repeater location $u \in \mathcal{R}$ and 0 otherwise. Since $p^{q,k}$ can only pass u if there is an outgoing elementary link from u in $p^{q,k}$, and since the elementary links in $p^{q,k}$ are exactly those elementary links (u, v) for which $\tilde{x}_{uv}^{q,k} = 1$, $r_{up^{q,k}} = 1$ if and only if $\tilde{x}_{uv}^{q,k} = 1$ for some v such that $(u, v) \in \mathcal{E}_q$. Therefore,

$$r_{up^{q,k}} = \sum_{(u,v) \in \mathcal{E}_q} \tilde{x}_{uv}^{q,k}. \quad (6.111)$$

Since $x_{p^{q,k}} = 1$, this directly implies that

$$r_{up^{q,k}} \tilde{x}_{p^{q,k}} = \sum_{(u,v) \in \mathcal{E}_q} \tilde{x}_{uv}^{q,k}. \quad (6.112)$$

Furthermore, since for every path $p \in \mathcal{P}_q$, $\tilde{x}_p = 1$ if p is equal to $p^{q,k}$ for some $k \in \mathcal{K}$ and $\tilde{x}_p = 0$ otherwise,

$$\sum_{p \in \mathcal{P}_q} r_{up} \tilde{x}_p = \sum_{k \in \mathcal{K}} r_{up^{q,k}} \tilde{x}_{p^{q,k}}. \quad (6.113)$$

Combining Equation (6.112) and Equation (6.113) then gives

$$\sum_{p \in \mathcal{P}_q} r_{up} \tilde{x}_p = \sum_{(u,v) \in \mathcal{E}_q} \sum_{k \in \mathcal{K}} \tilde{x}_{uv}^{q,k}. \quad (6.114)$$

Substituting (6.114) into (6.66) gives

$$\sum_{p \in \mathcal{P}_q} r_{up} \tilde{x}_p \leq 1. \quad (6.115)$$

Repeating this argument for every every $u \in \mathcal{R}$ and $q \in \mathcal{Q}$ results in Constraints (6.55).

□

Proposition 12 *The variables \tilde{x}_p and \tilde{y}_u^p that we obtain satisfy Constraints (6.56) of the path-based formulation, i.e.*

$$\sum_{p \in \mathcal{P}} r_{up} \tilde{x}_p \leq D \tilde{y}_u^p \quad \forall u \in \mathcal{R}. \quad (6.116)$$

Proof: If we substitute (6.114) into (6.68) (with every $x_{uv}^{q,k}$ replaced by $\tilde{x}_{uv}^{q,k}$), we get that

$$\sum_{q \in \mathcal{Q}} \sum_{p \in \mathcal{P}_q} r_{up} \tilde{x}_p = \sum_{p \in \mathcal{P}} r_{up} \tilde{x}_p \leq D y_u^l \quad \forall u \in \mathcal{R}. \quad (6.117)$$

Additionally, we assign all the values of \tilde{y}_u^p to have the same value as y_u^l for all $u \in \mathcal{R}$, such that we can replace y_u^l with \tilde{y}_u^p in (6.117) to get

$$\sum_{p \in \mathcal{P}} r_{up} \tilde{x}_p \leq D \tilde{y}_u^p \quad \forall u \in \mathcal{R}. \quad (6.118)$$

□

This concludes the proof that the variables we obtain from the optimal solution to the link-based formulation provide a feasible solution to the path-based formulation. Another important observation we can make about the objective value of this newly constructed feasible solution is that

$$\sum_{u \in \mathcal{R}} y_u^l = \sum_{u \in \mathcal{R}} \tilde{y}_u^p \geq \sum_{u \in \mathcal{R}} y_u^p. \quad (6.119)$$

If we now combine (6.94) and (6.119), we reach the conclusion that

$$\sum_{u \in \mathcal{R}} y_u^l = \sum_{u \in \mathcal{R}} y_u^p, \quad (6.120)$$

i.e. the optimal objective values of the path-based formulation and link-based formulation are equal. This implies that the feasible solution to the link-based formulation we obtain from the path-based formulation and vice versa are actually optimal solutions. We thus conclude that the two formulations are equivalent.

References

- [1] J. Forrest, L. Hafer, J. Hall, and M. Saltzman, *Coin-or linear programming*, <http://dx.doi.org/10.5281/zenodo.3634628> (2020).
- [2] L. Gurobi Optimization, *Gurobi optimizer reference manual*, <https://www.gurobi.com> (2020).
- [3] IBM, *IBM ILOG CPLEX 12.9 User's Manual*, <http://www.cplex.com> (2019).
- [4] M. S. Daskin, *Network and discrete location: models, algorithms, and applications* (John Wiley & Sons, 2011).
- [5] J. Rabbie and G. Avis, *RepAlloc*, <https://github.com/jtrabbie/RepAlloc> (2020).
- [6] N. Sinclair, E. Saglamyurek, H. Mallahzadeh, J. A. Slater, M. George, R. Ricken, M. P. Hedges, D. Oblak, C. Simon, W. Sohler, and W. Tittel, *Spectral Multiplexing for Scalable Quantum Photonics using an Atomic Frequency Comb Quantum Memory and Feed-Forward Control*, *Physical Review Letters* **113**, 053603 (2014).
- [7] D. Jones, M. Tamiz, *et al.*, *Practical goal programming*, Vol. 141 (Springer, 2010).
- [8] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, *Inside Quantum Repeaters*, *IEEE Journal of Selected Topics in Quantum Electronics* **21**, 78 (2015).
- [9] M. Penrose *et al.*, *Random geometric graphs*, Vol. 5 (Oxford university press, 2003).
- [10] A. A. Hagberg, D. A. Schult, and P. J. Swart, *Exploring network structure, dynamics, and function using networkx*, in *Proceedings of the 7th Python in Science Conference*, edited by G. Varoquaux, T. Vaught, and J. Millman (Pasadena, CA USA, 2008) pp. 11 – 15.
- [11] C. B. Barber, D. P. Dobkin, and H. Huhdanpaa, *The quickhull algorithm for convex hulls*, *ACM Trans. Math. Softw.* **22**, 469–483 (1996).
- [12] P. Virtanen, R. Gommers, T. E. Oliphant, M. Haberland, T. Reddy, D. Cournapeau, E. Burovski, P. Peterson, W. Weckesser, J. Bright, S. J. van der Walt, M. Brett, J. Wilson, K. J. Millman, N. Mayorov, A. R. J. Nelson, E. Jones, R. Kern, E. Larson, C. J. Carey, Í. Polat, Y. Feng, E. W. Moore, J. VanderPlas, D. Laxalde, J. Perktold, R. Cimrman, I. Henriksen, E. A. Quintero, C. R. Harris, A. M. Archibald, A. H. Ribeiro, F. Pedregosa, and P. van Mulbregt, *SciPy 1.0: Fundamental algorithms for scientific computing in Python*, *Nature Methods* **17**, 261 (2020).

- [13] S. Wagon, *Round formulas for exponential polynomials and the incomplete gamma function*, <http://math.colgate.edu/~integers/q79> (2016).

7

Analysis of multipartite entanglement distribution using a central quantum-network node

Guus Avis, Filip Rozpędek and Stephanie Wehner.

We study the performance (rate and fidelity) of distributing multipartite entangled states in a quantum network through the use of a central node. Specifically, we consider the scenario where the multipartite entangled state is first prepared locally at a central node, and then transmitted to the end nodes of the network through quantum teleportation. As our first result, we present leading-order analytical expressions and lower bounds for both the rate and fidelity at which a specific class of multipartite entangled states, namely Greenberger-Horne-Zeilinger (GHZ) states, are distributed. Our analytical expressions for the fidelity accurately account for time-dependent depolarizing noise encountered by individual quantum bits while stored in quantum memory, as verified using Monte Carlo simulations. As our second result, we compare the performance to the case where the central node is an entanglement switch and the GHZ state is created by the end nodes in a distributed fashion. Apart from these two results, we outline how the teleportation-based scheme could be physically implemented using trapped ions or nitrogen-vacancy centers in diamond.

7

7.1 Introduction

While the previous chapters all focus on the distribution of bipartite entangled states, in this chapter we instead focus on the distribution of multipartite entanglement. Various investigations have been performed into how specific multipartite entangled states can best be distributed in a quantum network [1–22]. A recurring theme that can be discerned in prior work is the use of a central node that establishes bipartite entanglement with a number of end nodes, and then executes local operations to transform the bipartite states

This chapter is based on the publication Phys. Rev. A 107, 012609 (2023).

into a single multipartite entangled state between those end nodes [3, 8, 12, 15, 16, 20–22]. Notably, such a scheme is a key ingredient for different efficient protocols and network architectures for distributing multipartite entanglement [3, 16, 20–22].

In this chapter, we consider the case where a multipartite entangled state is distributed in a quantum network by first creating the target state locally at the central node, and then transmitting the qubits of the state to the end nodes through quantum teleportation using preshared Bell states [23]. Teleportation is realized by executing a Bell-state measurement (BSM) on the to-be teleported qubit and a qubit in a Bell state. Here, we refer to a node capable of creating and teleporting multipartite entangled states as a *factory node*. The function of a factory node is illustrated in Figure 7.1.

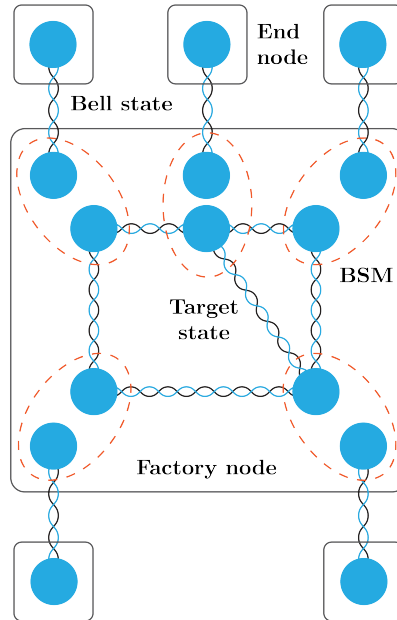


Figure 7.1: A factory node can be used to distribute some multipartite entangled target state (for example, a graph state) between a set of end nodes. This is done by preparing the target state locally at the factory node and teleporting it. Quantum teleportation of the target state is realized using Bell states shared between the factory node and the end nodes and Bell-state measurements (BSMs).

Understanding the performance of factory nodes in the presence of hardware imperfections allows for the assessment of the different proposed protocols and network architectures that incorporate such central nodes. Metrics that quantify the performance of multipartite entanglement distribution are the rate at which states can be distributed, and the fidelity of distributed states to the target state. Developing a good understanding of the rate and fidelity is of special relevance to the work done in [21]. Here, the authors present a protocol to decide which node in a larger network to select as the central node for the distribution of GHZ states. This protocol relies on an analytical model of the rate and fidelity with which the states can be distributed for different possible placements of the central node. We contribute to understanding the rate and fidelity in Section 7.3. Fur-

thermore, we remark that it is not only of interest to quantify the performance of factory nodes in an absolute sense. It is also of interest to understand how the performance of factory nodes compares to other schemes that also allow for distributing multipartite entangled states, such that statements about their relative performance can be made. We contribute to this by considering different types of central nodes in Sections 7.1.3 and 7.4.

In this chapter, we specifically study the use of factory nodes to distribute GHZ states in a symmetric star-shaped network. In such a network, depicted in Figure 7.2, a central node is connected to N end nodes through, in total, N identical quantum connections. These quantum connections can be used to distribute Bell states. We will model the distribution of Bell states using quantum connections as a series of attempts of constant duration and success probability. When such an attempt is successful, the series terminates and a Bell state is created. When a quantum connection creates a Bell state, it is shared between the central node and the corresponding end node, and can be stored in quantum memory. These Bell states can be used as a resource to create multipartite entangled states shared by the end nodes.

7.1.1 Summary of results

In this chapter, we present two main results. As our first result, in Section 7.3, we provide analytical leading-order expressions and lower bounds for both the rate and fidelity of GHZ-state distribution in a symmetric star-shaped network using a factory node, and additionally an exact expression for the rate. The leading-order expressions become exact in the limit when the success probability of a single attempt at Bell-state distribution using a quantum connection is small, and the probability of losing a qubit due to memory decoherence during the time span of a single such attempt is small. As our second result, in Section 7.4, we provide a comparison between the performance of GHZ-state distribution on a symmetric star-shaped network when the central node is a factory node, and when the central node is instead a “2-switch” capable of performing BSMs to create Bell states shared between end nodes [14]. A key advantage to the use of factory nodes is an increased resilience to noise in Bell-state distribution. However, a disadvantage is reduced resilience to noise in BSMs. Additionally, the factory node is typically outperformed by the 2-switch in terms of rate.

7.1.2 Comparison of analytical results to prior work

Here, we compare the analytical results for the rate and fidelity that we present in Section 7.3 to existing results. First, we note that we are aware of only one prior analytical result for the fidelity of distributed GHZ states in a similar scheme, which is found in [21]. However, the authors make the simplifying assumption that Bell states cannot be stored in quantum memory between attempts at Bell-state distribution. Therefore, all connections need to be successful simultaneously. When the success probability for distributing Bell states is small, this is a very inefficient scheme. In contrast, we assume entangled qubits are stored within the factory node until all Bell states are in place and the GHZ state can be teleported. Here, we are able to accurately account for the time-dependent noise due to qubits being stored in noisy quantum memory for random periods of time. Additionally, it is assumed in [21] that local operations are always noiseless, which is not an assumption made in this chapter.

Second, we compare our results with the study of the “entanglement switch”. An en-

tanglement switch, first defined in [14], is a quantum-network node capable of generating and storing Bell states with k end nodes, and executing GHZ-state measurements on n local qubits, thereby creating GHZ states shared by n out of k end nodes. From this perspective, a factory node that distributes GHZ states, as studied in this chapter, can be described as an $n = k$ entanglement switch. An entanglement switch for which $n = 2$ is referred to as “2-switch” throughout this chapter.

In [12–15, 24], the entanglement switch is studied analytically using Markov-chain techniques. In [15], it is discussed that a minimum fidelity can be guaranteed by incorporating a cutoff time after which qubits are discarded from memory in the protocol, and the effects of the cutoff time on the rate are studied for $n = 2$. However, there are no expressions for the actual fidelity (with or without cutoff time), and in case there is no cutoff time there is also no lower bound. Additionally, none but [12] consider the case $n > 3$, where the only result that is presented for $n = k$ is that no steady-state solution exists in case the switch is able to store an infinite number of entangled qubits. This is in contrast to this chapter, where we present analytical results for the fidelity in the absence of a cutoff time, the parameter n can take any value, and we assume there is only one qubit of buffer memory available per end node. Our results are limited to $n = k$, but we discuss in Section 7.6 how the results can be extended to $n < k$.

A paper that does derive results for an entanglement switch of general $n = k$ with only a single qubit of buffer memory is [10]. The authors provide analytical tools for understanding and bounding the rate, but do not consider the fidelity. Finally, numerical results for the fidelity obtained from Monte Carlo simulations can be found in [11]. While Monte Carlo simulations can be used to study a larger range of setups than our analytical results (e.g., they can be used to study asymmetric star-shaped networks), they may need to be evaluated many times in order to obtain results with small error bars. Doing so can be computationally expensive. This is especially the case when there is a large number of end nodes, as quantum states in the system will be large and therefore hard to simulate. On the other hand, our analytical results are computationally cheap to evaluate and have no error bars. Furthermore, analytical results are often more suited to understand how a quantity scales and gain intuition.

7

7.1.3 Different central nodes

In order to understand how well factory nodes perform relative to other schemes that allow for the distribution of multipartite entangled states, a comparison needs to be performed. This allows us to put the rate and fidelity that factory nodes can achieve into context, and can help determine under what circumstances it is best to use a factory node, and under what circumstances it may be better to consider a different scheme. Here, we provide a non-exhaustive comparison by discussing two alternative strategies for distributing multipartite entangled states on the symmetric star-shaped network depicted in Figure 7.2. The first of these utilizes a central node without quantum memory, while the second uses a 2-switch as central node.

The first alternative method to factory nodes for the distribution of multipartite entanglement in a star-shaped network is to utilize a central node that does not have any quantum memory. This memoryless scheme requires connections through which photons can be directly transmitted, e.g. they can be optical fibers. To distribute a multipartite entangled state, the end nodes emit entangled photons that are sent through the connections

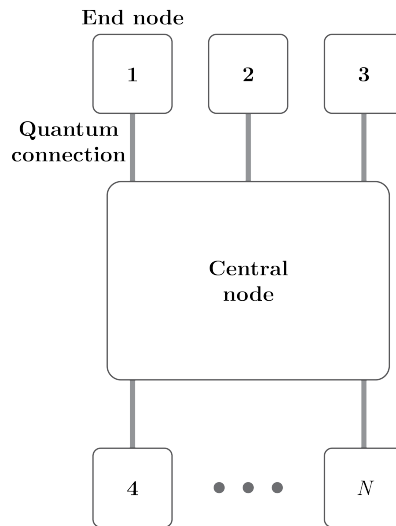


Figure 7.2: Symmetric star-shaped network studied in this chapter. N identical end nodes are each connected to a central node through one of, in total, N identical quantum connections. These quantum connections can be used to distribute Bell states, which can be stored in quantum memory and provide a resource to create a multipartite entangled states shared by the end nodes. An example of a possible central node is a factory node.

to the central node. Here, the photons are interfered and measured, resulting in the creation of the target state on the end nodes. Such schemes exist for the distribution of GHZ states [4, 25] and W states [26, 27], and they are illustrated in Figure 7.3.

An advantage of these schemes is that the central node can be very simple, requiring only linear-optics components and single-photon detectors. A downside however, when distributing GHZ states, is that all photons need to arrive at the central station simultaneously, making it very sensitive to photon losses; if each of the N connections transmits photons successfully with probability η (the transmittance of the connection), the distribution rate will scale as η^N . On the other hand, a factory node could be used to distribute states with a rate that falls only logarithmically with N , and linearly with the success probability of Bell-state distribution (see Section 7.3.1). How this success probability scales with η depends on the nature of the connection and the specific method used to distribute Bell states. When using direct transmission of entangled photons, the scaling will be linear in η , but schemes with better scaling exist. For example, single-click heralded entanglement generation [28] can be used for $\sqrt{\eta}$ scaling, and the scaling could be further improved using quantum repeaters, with the exact scaling depending on how they are implemented [29]. No further comparison between memoryless schemes and the use of a factory node is performed in this chapter.

The second alternative method to using factory nodes for the distribution of multipartite entanglement in a star-shaped network, is to use a 2-switch as a central node. The 2-switch functions as an intermediary, allowing the end nodes to share Bell states with one another even though they are not directly connected. By executing the appropriate local operations at the end nodes, these Bell states can be transformed into the target mul-

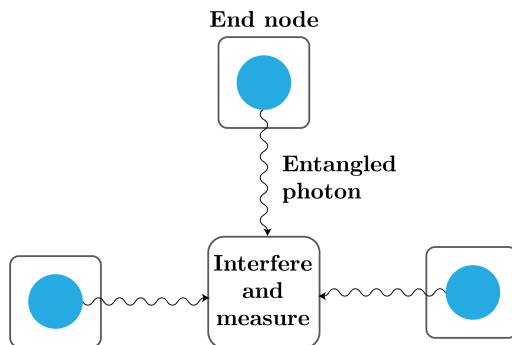


Figure 7.3: Some multipartite entangled states, such as GHZ states and W states, can be distributed between end nodes through the interference and measurement of entangled photons. Each of the end nodes needs to emit a photon that is entangled to a qubit held in local quantum memory, and transmit it to a central node. At this node, the photons originating from all the different nodes are interfered.

tipartite entangled state. One downside to this option is that it imposes the requirement that end nodes must be able to store multiple qubits within their quantum memory, and that they must be able to execute multipartite entangling operations. An additional downside is that, even if each end node is able to store and exert full control over two qubits, there still exist multipartite entangled states that the nodes would be able to store but cannot create in their limited quantum memory using only bipartite entangled states shared between them [19]. On the other hand, when utilizing a factory node, any multipartite entangled state that the end nodes have enough quantum memory to store can be distributed among them. Generally, when using a factory node, advanced quantum capabilities are required only of the dedicated network device, not of the end nodes.

In section 7.4, we present our second main result. This result is a comparison, based on Monte Carlo simulations, of the rate and fidelity of GHZ-state distribution on the symmetric star-shaped network using a factory node and using a 2-switch. Here, we assume the 2-switch follows a specific protocol under which BSMs are not executed whenever possible, but only when they result in a Bell state that directly contributes to the creation of a GHZ state.

7.1.4 Outline

The remainder of this chapter is set up as follows. First, in Section 7.2, we introduce the exact factory-node setup and noise model we study. Next, in Section 7.3, we provide analytical results for the rate and fidelity with which GHZ states can be distributed on this setup. In Section 7.4, we use Monte Carlo simulations to compare the performance of GHZ-state distribution using a factory node and using a 2-switch. We provide examples of how a factory node could be physically implemented using trapped ions or nitrogen-vacancy centers in diamond in Section 7.5. Finally, we conclude in Section 7.6, where we discuss how the results presented in this chapter could be generalized and used for further study.

7.2 Setup, Protocol and Model

In this section, we discuss in detail the factory-node setup that we study in this chapter. Additionally, we introduce the exact protocol used to distribute GHZ states on this setup, and the model that we use to account for noise and losses.

We consider a symmetric star-shaped quantum network. Such a network, depicted in Figure 7.2, consists of N end nodes, and one central node that shares a single quantum connection with each of the end nodes. For the factory-node setup discussed in this section, this central node is a factory node. The quantum connections can be used to distribute Bell states of the form

$$|\phi_{00}\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle). \quad (7.1)$$

Each end node contains a single qubit. On the other hand, the factory node contains $2N$ qubits. N of these can be used to store the local halves of Bell states that are distributed using the quantum connections. The other N can be used to prepare and store a target quantum state to be distributed among the end nodes. Furthermore, for each of the first N qubits, the node is able to execute a BSM with exactly one of the second N qubits. In our modeling, we allow for probabilistic BSMs. A BSM is probabilistic e.g. when it is implemented using linear optics [30, 31]. When a BSM has success probability q_{BSM} , we model this as raising a “fail” flag with probability $1 - q_{\text{BSM}}$, and executing a perfect BSM otherwise. On this setup, any N -partite target state can be distributed between the end nodes by creating the target state locally, and then teleporting it to the end nodes using Bell states. Specifically, we consider the distribution of an N -partite GHZ state using Protocol 7.1, which is illustrated in Figure 7.4. Such a state is defined by

$$|\text{GHZ}\rangle = \frac{1}{\sqrt{2}} (|0\rangle^{\otimes N} + |1\rangle^{\otimes N}). \quad (7.2)$$

7

Protocol 7.1 GHZ-State Distribution Using Factory Node

1. *Repeatedly attempt Bell-state distribution over each of the N quantum connections shared between the factory node and the N different end nodes, until the factory node shares a Bell state with each end node.*
2. *Create an N -partite GHZ state on the N remaining free memory qubits in the factory node.*
3. *Perform N BSMs at the factory node, each between one qubit that holds part of the GHZ state, and one qubit that holds part of a Bell state.*
4. *Send a classical message from the factory node to each of the end nodes containing the results of the BSMs.*
5. *If any of the BSMs was unsuccessful, all end nodes reset their memory qubits. Return to Step 1. Otherwise, the end nodes perform Pauli corrections based on the outcomes of the BSMs, such that, in the absence of noise, the end nodes now share a GHZ state.*

Each step in the protocol is performed after the previous step has been concluded. In case the BSMs are all successful, the last three steps of Protocol 7.1 implement quantum

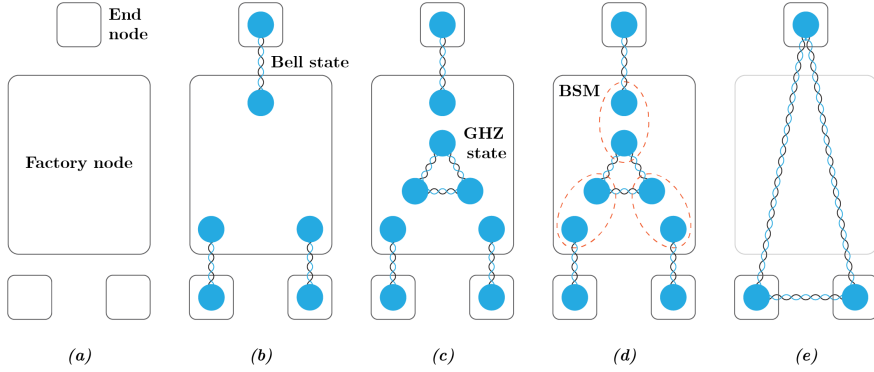


Figure 7.4: Illustration of GHZ-state distribution through a factory node, using Protocol 7.1. **(a)** There is one factory node, and there are $N = 3$ end nodes. **(b)** Bell states are distributed between the factory node and each of the end nodes (Step 1 of Protocol 7.1). **(c)** After all Bell states are in place, a GHZ state is created locally (Step 2 of Protocol 7.1). **(d)** BSMs are executed between qubits in Bell states and qubits in the GHZ state (Step 3 of Protocol 7.1). **(e)** If all BSMs were successful and the corresponding Pauli corrections have been applied, the end nodes share a GHZ state (Steps 4 and 5 of Protocol 7.1).

teleportation of the N qubits sharing a GHZ state from the factory node to the end nodes. Therefore, in the absence of noise, this results in the N end nodes sharing an N -partite GHZ state.

7

In this study, we assume the time it takes to distribute a Bell state over a quantum connection follows a geometric distribution. That is, Bell-state distribution is a series of attempts, where each attempt is of constant duration Δt , and where the probability that an attempt is successful is described by the constant q_{link} . To be more precise, Δt is the time it takes after starting an attempt until both the end node and factory node know whether it was successful or not. Only after they have obtained this knowledge, they can decide whether they want to reset their local qubits and start again, or whether they should instead keep the created quantum state stored in memory. We use this time, i.e. Δt after the start of the attempt, as the start of the storage time of the Bell state that is generated if the attempt is successful. Describing Bell-state distribution as a sequence of independent attempts is accurate when the quantum connection consists of, for example, heralded entanglement generation through either direct transmission [32, 33] or photon interference [28, 34–44], or a quantum-repeater chain with fixed-time quantum memory [45, 46].

Another assumption made here is that all quantum connections are identical, i.e. Δt and q_{link} are the same for each of the N connections between the factory node and the end nodes. Therefore, Δt is used as the standard time unit throughout the rest of this chapter, and one time step of duration Δt during which attempts at Bell-state distribution take place is sometimes referred to as a “round”.

The time that it takes to send a classical message between the factory node and any of the end nodes is denoted t_{cl} . Since Step 4 of Protocol 7.1 consists of sending classical messages, it will take t_{cl} to finish that step. How large t_{cl} is compared to Δt depends on

how the quantum connections are implemented. For example, in the case of heralded entanglement generation through photon interference, Δt includes the time required to send photons to a midpoint station, and the time required to send back the measurement outcome to the nodes. Assuming classical signals travel at the same speed of light (in fiber) as the photons used to generate entanglement, this time is exactly equal to t_{cl} . Δt may be further limited by, among others, the rate at which entangled photons can be emitted and by classical overhead due to e.g. synchronizing emission times [38, 47, 48]. In that case, $t_{\text{cl}} < \Delta t$. In this chapter, we focus on the case $q_{\text{link}} \ll 1$. In that regime, the number of attempts required to successfully distribute a Bell state is typically very large. Then, as long as t_{cl} is not much larger than Δt , classical communication will only take up a negligibly small part of both the time required to distribute one GHZ state and qubit storage times. Therefore, we use $t_{\text{cl}} = 0$ throughout the rest of this chapter. Additionally, we assume that all local operations executed at the factory node and the end nodes are instantaneous. These operations do not suffer from any speed-of-light delay, and their execution time will always become comparatively small for small enough q_{link} . Because both classical communication and local operations are modeled as instantaneous, Step 1 is the only step of Protocol 7.1 with nonzero duration.

All noise in the network is modeled by depolarizing channels, described by the action [49]

$$\mathcal{D}_{\mathcal{H}_A, p}(\rho) = p\rho + (1-p)\text{Tr}_{\mathcal{H}_A}(\rho) \otimes \frac{\mathbb{1}_{\mathcal{H}_A}}{\text{Tr} \mathbb{1}_{\mathcal{H}_A}}. \quad (7.3)$$

Here, ρ is a density matrix in the Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, \mathcal{H}_A is the subspace of \mathcal{H} that describes the system that the depolarizing channel acts on, $\mathbb{1}_{\mathcal{H}_A}$ is the identity operator of \mathcal{H}_A , $\text{Tr}_{\mathcal{H}_A}$ is the partial trace over \mathcal{H}_A , and p is the so-called depolarizing parameter. It can be interpreted as losing all information about the system described by \mathcal{H}_A with probability $1 - p$. Specifically, we consider the following sources of noise:

- Noisy connections. Whenever a Bell state is created, a depolarizing channel with parameter p_{link} acts on the two qubits that hold the Bell state (i.e. \mathcal{H}_A has dimension 4). We note that, because of the symmetry of the Bell state, this is equivalent to a single-qubit depolarizing channel acting with parameter p_{link} on either of the individual qubits.
- Noisy memory. For every time unit Δt that a quantum state is stored in a memory qubit, a depolarizing channel with parameter p_{mem} acts on that qubit (i.e. \mathcal{H}_A has dimension 2).
- Noisy BSMs. Whenever a BSM is executed, it is preceded by two depolarizing channels with parameter p_{BSM} , one on each of the participating qubits (i.e. \mathcal{H}_A has dimension 2). This measurement itself, following the depolarizing channels, is then modeled as being noiseless.
- Noisy GHZ states. Whenever a GHZ state is created, a depolarizing channel with parameter p_{GHZ} acts on the N qubits that hold the GHZ state (i.e. \mathcal{H}_A has dimension 2^N).

Local Pauli corrections are modeled as noiseless.

7.3 Analytical Results

Here, we present analytical results for the rate and fidelity of GHZ-state distribution using Protocol 7.1. For the rate, we provide three analytical results: an exact expression, a lower bound, and a leading-order expression. For the fidelity, we present two analytical results: a lower bound and a leading-order expression. The accuracy of the leading-order expression for the rate, and of both the leading-order expression and the lower bound for the fidelity, is verified against a numerical model built using the quantum-network simulator NetSquid [11] in Section 7.9.

7.3.1 Rate

We denote the time required to distribute a single GHZ state using Protocol 7.1 by T , which is a random variable. The (average) rate at which GHZ states are distributed is then defined by

$$R = 1/\langle T \rangle. \quad (7.4)$$

Thus, to calculate the rate, we need to know the expected value of the distribution time. To this end, we decompose the distribution time as

$$T = n_{\text{teleport}} T_{\text{teleport}}. \quad (7.5)$$

Here, n_{teleport} is the number of attempts at teleporting a GHZ state until such an attempt is successful. That is, it is the number of times Steps 1 through 4 of Protocol 7.1 need to be executed for the protocol to finish. Such an attempt at teleportation may fail in case the BSMs are probabilistic, i.e. $q_{\text{BSM}} < 1$. On the other hand, T_{teleport} is the time required to perform Steps 1 through 4 once. Both these quantities are random variables. Because under the present assumptions only Step 1 of Protocol 7.1 has a nonzero duration, T_{teleport} can be further dissected into

$$T_{\text{teleport}} = n_{\text{all}} \Delta t, \quad (7.6)$$

where n_{all} is again a random variable, corresponding to the number of rounds of Bell-state distribution required to share Bell states between the factory node and all of the end nodes. That is, it is the number of rounds required to finish Step 1 of Protocol 7.1. Combining the two expressions yields

$$T = n_{\text{teleport}} n_{\text{all}} \Delta t. \quad (7.7)$$

Because the expected value of a product of two independent random variables is the product of their expected values, we find

$$\langle T \rangle = \langle n_{\text{teleport}} \rangle \langle n_{\text{all}} \rangle \Delta t. \quad (7.8)$$

Since each teleportation attempt succeeds with a fixed success probability of q_{BSM}^N (teleportation succeeds if and only if all N BSMs are successful), n_{teleport} is geometrically distributed with $\langle n_{\text{teleport}} \rangle = 1/q_{\text{BSM}}^N$. Thus,

$$R = \frac{q_{\text{BSM}}^N}{\langle n_{\text{all}} \rangle \Delta t}. \quad (7.9)$$

The probability distribution of n_{all} is more complicated: the number of rounds required to distribute Bell states with all N end nodes is the number of rounds required to distribute

the Bell state that takes the longest. Writing n_i for the number of attempts required to distribute a Bell state with end node i , we have

$$n_{\text{all}} = \max\{n_1, n_2, \dots, n_N\}. \quad (7.10)$$

Each of the n_i is geometrically distributed with $\langle n_i \rangle = 1/q_{\text{link}}$. It can be evaluated exactly using [50]

$$\langle n_{\text{all}} \rangle = \sum_{j=1}^N (-1)^{j+1} \binom{N}{j} \frac{1}{1 - (1 - q_{\text{link}})^j}. \quad (7.11)$$

This can be substituted into Eq. (7.9) to obtain an exact expression for the rate. However, we also report here a known leading-order expression [10, 51, 52],

$$\langle n_{\text{all}} \rangle \approx \frac{H_N}{q_{\text{link}}}, \quad (7.12)$$

where H_N is the N^{th} harmonic number,

$$H_N \equiv \sum_{i=1}^N \frac{1}{i} = \gamma + \ln N + \mathcal{O}\left(\frac{1}{N}\right). \quad (7.13)$$

Here, $\gamma \approx 0.5772$ is the Euler-Mascheroni constant. Substituting this into Equation (7.9) yields

$$R \approx \frac{q_{\text{BSM}}^N q_{\text{link}}}{H_N \Delta t}, \quad (7.14)$$

which is valid up to leading order in q_{link} .

There are two reasons why we report the leading-order approximation (7.14) even though an exact expression is available. First, in the regime $q_{\text{link}} \ll 1$, Eq. (7.14) is accurate and easier to evaluate. Second, Eq. (7.14) more clearly shows how the rate scales with q_{link} , N and q_{BSM} , thereby providing more intuition. We additionally note that there exists an upper bound [10, 53],

$$\langle n_{\text{all}} \rangle < 1 + \frac{H_N}{-\ln(1 - q_{\text{link}})}. \quad (7.15)$$

Therefore, Eq. (7.14) is a lower bound on the actual rate if

$$\frac{H_N}{q_{\text{link}}} > 1 + \frac{H_N}{-\ln(1 - q_{\text{link}})}. \quad (7.16)$$

This is the case for any $N > 3$. Additionally, it is true for $N = 3$ if $q_{\text{link}} \gtrsim 0.42$. Therefore, using the simpler leading-order expression usually does not lead to overestimating the performance of Protocol 7.1. In Section 7.9, for $N = 5$, we find that Eq. (7.14) is indeed a tight lower bound for small values of q_{link} , while underestimating the rate up to a factor of two for $q_{\text{link}} \sim 1$.

7.3.2 Fidelity

In this section, we calculate the fidelity of the state shared by the end nodes after a successful execution of Protocol 7.1. This fidelity is defined with respect to the perfect GHZ state. The first step is to determine the density matrix of that state, which we denote ρ . In the absence of noise, ρ would simply be a perfect GHZ state. However, due to the depolarizing noise in the creation of the local GHZ state within the factory node, the performance of BSMs, the distribution of Bell states and the storage of qubits, ρ is generally not a GHZ state and is a function of the noise parameters p_{GHZ} , p_{BSM} , p_{link} and p_{mem} . Additionally, we note that each individual execution of the protocol is characterized by the values that the random variables n_1, n_2, \dots, n_N take. Just like above, the random variable n_i represents the number of rounds it takes to distribute a Bell state between the factory node and end node i . How much decoherence due to the storage of qubits in quantum memories is suffered, will depend on the value that each n_i takes. Therefore, ρ is additionally a function of the random variables n_1, n_2, \dots, n_N .

We derive ρ as a function of the noise parameters and random variables in Section 7.10. Here, we briefly summarize how this derivation is performed. First, we note that there are single-qubit depolarizing channels acting on three groups of qubits. First, there are the qubits that are part of the locally created GHZ state in the factory node. Second, there are the qubits stored at the GHZ factory that are entangled to those at the end nodes and partake in BSMs together with the GHZ-state qubits. Finally, there are the qubits stored at the end nodes. Because of the symmetry of Bell states, and by extension of BSMs, it is possible to “move” all these single-qubit depolarizing channels to only the qubits stored at the end nodes. That is, the state ρ can be derived correctly by pretending that as the protocol is executed, there is no single-qubit depolarizing noise within the factory node, but instead there are only single-qubit depolarizing channels acting at the end nodes. Because the composition of depolarizing channels is itself a depolarizing channel, each end node i only undergoes a single depolarizing channel with parameter

$$p_i = p_{\text{link}} p_{\text{BSM}}^2 p_{\text{mem}}^{2\Delta n_i}, \quad (7.17)$$

where

$$\Delta n_i \equiv n_{\text{all}} - n_i \quad (7.18)$$

is the number of rounds the Bell state shared with end node i is stored until it partakes in a BSM. Describing the protocol in this way is very convenient, because it then amounts to performing perfect quantum teleportation of a noisy GHZ state to the end nodes, followed by depolarizing channels on each of the N individual qubits of the state. Resolving all these depolarizing channels gives the result

$$\begin{aligned} \rho = & \frac{1 - p_{\text{GHZ}}}{2^N} \mathbb{1}_{\mathcal{N}} \\ & + p_{\text{GHZ}} \left[\prod_{i \in \mathcal{N}} p_i (|\text{GHZ}\rangle\langle\text{GHZ}|)_{\mathcal{N}} + \prod_{i \in \mathcal{N}} \frac{1 - p_i}{2} \mathbb{1}_{\mathcal{N}} \right. \\ & \left. + \frac{1}{2} \sum_{\substack{U \subset \mathcal{N} \\ 1 \leq |U| \leq N}} \left(\prod_{i \in U} \frac{1 - p_i}{2} \prod_{j \in \mathcal{N} \setminus U} p_j \right) \mathbb{1}_U \otimes \mathcal{P}_{\mathcal{N} \setminus U} \right]. \end{aligned} \quad (7.19)$$

Here, we have defined $\mathcal{N} = \{1, 2, \dots, N\}$, and \mathcal{P} is the classically correlated, unnormalized state

$$\mathcal{P}_{1,2,\dots,k} \equiv (|0\rangle\langle 0|)^{\otimes k} + (|1\rangle\langle 1|)^{\otimes k}. \quad (7.20)$$

The different terms in the density matrix correspond to all different combinations of some of the qubits being lost due to single-qubit depolarizing noise, and some being unscathed.

Using Eq. (7.19), the fidelity can be efficiently written as

$$\begin{aligned} F_{\text{rand}} &\equiv \langle \text{GHZ} | \rho | \text{GHZ} \rangle \\ &= \frac{1 - p_{\text{GHZ}}}{2^N} \\ &\quad + p_{\text{GHZ}} \sum_{U \subseteq \mathcal{N}} 2^{\delta_{|U|,0} + \delta_{|U|,N} - 1} \prod_{i \in U} \left(\frac{1 - p_i}{2} \right) \prod_{j \in \mathcal{N} \setminus U} p_j, \end{aligned} \quad (7.21)$$

where $|U|$ is the cardinality of set U and $\delta_{i,j}$ denotes the Kronecker delta function. As the fidelity is a function of the random variables Δn_i , it is itself a random variable: it depends on how quickly one after another the different Bell states are distributed. This is the reason why the fidelity above is denoted with the subscript “rand”. The delta functions are there to account for the fact that there is “one less” factor of $\frac{1}{2}$ in the fidelity when no qubits are lost, and when all qubits are lost. The reason for this is that losing a single qubit (i.e. tracing that qubit out and then replacing it by a maximally mixed state) in a GHZ state does not only destroy the information held by that qubit, but also reduces the correlation between the remaining qubits to classical correlation instead of quantum correlation. Therefore, the first qubit that is lost accounts for a larger drop in fidelity than subsequent qubits. Additionally, the last qubit that is lost does not account for any drop in fidelity, as losing $N - 1$ qubits of the GHZ state will already result in an N -qubit maximally mixed state, the fidelity of which cannot be further decreased by depolarizing noise.

Here, we are assuming no post-selection on distributed GHZ states takes place. Therefore, we can describe the state produced by execution of Protocol 7.1 as a mixture between all ρ 's corresponding to different values of Δn_i . This state is then independent of the random variables, and the same for each execution of the protocol. The mixed state is the expected value of the density matrix ρ , and its fidelity is the expected value of F_{rand} , which can be written as

$$\begin{aligned} F &= \langle F_{\text{rand}} \rangle = \frac{1 - p_{\text{GHZ}}}{2^N} \\ &\quad + p_{\text{GHZ}} \sum_{U \subseteq \mathcal{N}} 2^{\delta_{|U|,0} + \delta_{|U|,N} - 1} \left\langle \prod_{i \in U} \frac{1 - p_i}{2} \prod_{j \in \mathcal{N} \setminus U} p_j \right\rangle. \end{aligned} \quad (7.22)$$

In Section 7.11 we work out the combinatorics to rewrite the fidelity as

$$F = \frac{1 - p_{\text{GHZ}}}{2^N} + p_{\text{GHZ}} \sum_{U \subseteq \mathcal{N}} A_{|U|} \left\langle \prod_{i \in U} (p_{\text{mem}}^2)^{\Delta n_i} \right\rangle, \quad (7.23)$$

where

$$A_{|U|} = \begin{cases} (p_{\text{link}} p_{\text{BSM}}^2)^{|U|} \left(\frac{1}{2^N} + \frac{1}{2} \delta_{|U|,N} \right) & \text{if } |U| \text{ is even,} \\ \frac{1}{2} (p_{\text{link}} p_{\text{BSM}}^2)^{|U|} \delta_{|U|,N} & \text{if } |U| \text{ is odd.} \end{cases} \quad (7.24)$$

Now, we note that after Bell states have been distributed between the factory node and all end nodes, it is possible to order the end nodes based on the order in which they were connected to the factory node. That is, to each end node $i \in \mathcal{N}$ we assign $d_i \in \mathcal{N}$ such that if $d_i > d_j$, then end node i shared a Bell state with the factory node at the same time as or later than end node j . For example, if end node 4 shared a Bell state first, we assign $d_4 = 1$. If such an ordering is given, it is possible to use the results from Section 7.12 to evaluate expressions like Eq. (7.23). However, in general, such an ordering cannot be imposed a priori; it is only well-defined after executing the protocol. Because the order in which Bell states are shared is random, each d_i is a random variable. Therefore, to apply the results from Section 7.12, an average should be taken over all possible orders in which Bell states can be distributed. Because of the symmetry of the setup under consideration, however, we need not worry about that. The success probability is q_{link} for all quantum connections, so all orderings are equally likely. Furthermore, since the effective depolarizing probability per round is p_{mem}^2 for all end nodes, the fidelity is invariant under changes in the ordering (it does not matter if end node 4 shares a Bell state first and end node 6 last, or the other way around). Therefore, we can safely pretend the order in which Bell states are distributed is fixed. Furthermore, we set our labeling to coincide with this order. That is, we set it such that $d_i = i$.

It follows from Eq. (7.114) in Section 7.12 that, to leading order in q_{link} and $(1 - p_{\text{mem}}^2)$,

$$\left\langle \prod_{i \in U} (p_{\text{mem}}^2)^{\Delta n_i} \right\rangle \approx \prod_{k=1}^N \frac{(N+1-k)q_{\text{link}}}{|U_k|(1-p_{\text{mem}}^2) + (N+1-k)q_{\text{link}}}, \quad (7.25)$$

where

$$U_k \equiv \{u \in U \mid u < k\}. \quad (7.26)$$

For example, if $U = \{1, 3\}$, then $U_1 = \emptyset$, $U_2 = U_3 = \{1\}$ and $U_4 = U$. Since the expression is to leading order in $1 - p_{\text{mem}}^2$ and $1 - p_{\text{mem}}^2 \geq 1 - p_{\text{mem}}$, we consider the approximation to be valid up to leading order in $1 - p_{\text{mem}}$. A leading-order expression for the fidelity is then obtained by combining Eq. (7.23) with Eq. (7.25).

The main reason why working to leading order in q_{link} and $1 - p_{\text{mem}}^2$ allows us to derive Eq. (7.25), is that in this approximation we can neglect the possibility of multiple Bell states being generated at the same time. For $q_{\text{link}} \ll 1$, the probability of more than one Bell state being generated during a single round is very small; most likely, there are many rounds between one success and the next. Additionally, when $1 - p_{\text{mem}}^2 \ll 1$, the drop in fidelity per extra round that qubits have to wait in memory is small. If that were not the case, the fidelity can be still high in case all Bell states succeed in quick succession, including some at the same time, while the fidelity would already be small in case there is some waiting time between different successes. Therefore, the contribution to the average fidelity of cases with multiple simultaneous successes would be relatively large despite them occurring with small probability, and neglecting their contribution would be inaccurate.

We see in Section 7.9 that the real fidelity of Protocol 7.1 is typically larger than the leading-order expression given by Eq. (7.25). This is explained by the fact that we ignore cases where multiple Bell states are generated simultaneously: we are effectively calculating the average of F_{rand} over a sub-normalized probability distribution. However, this does not prove Eq. (7.25) is a lower bound on the fidelity. The reason for this is that, in Section 7.12, in order to work consistently at leading order in q_{link} and $1 - p_{\text{mem}}$ we have

also neglected terms that would lower the calculated fidelity if they were included, and we do not know if these neglected terms generally outweigh the terms corresponding to multiple simultaneously distributed Bell states. When not throwing these higher-order terms out, a strict lower bound is obtained. However, it typically approximates the real fidelity (far) worse than the leading-order expression, as discussed below. The bound is calculated in Section 7.12 (Eq. (7.121)) and yields

$$\left\langle \prod_{i \in U} (p_{\text{mem}}^2)^{\Delta n_i} \right\rangle \geq \prod_{k=1}^N \frac{(N+1-k)q_{\text{link}}(1-q_{\text{link}})^{N-k}(1-p_{\text{mem}}^2)^{|U_k|}}{1-(1-q_{\text{link}})^{N+1-k}(1-p_{\text{mem}}^2)^{|U_k|}}. \quad (7.27)$$

The lower bound on the fidelity is obtained by using Eq. (7.27) to evaluate Eq. (7.23).

In Section 7.9, we compare the analytical results to a Monte Carlo simulation of Protocol 7.1. One such comparison figure is also included here, see Figure 7.5. In Section 7.9, we find that both the leading-order expression and lower bound closely approximate simulation results for small values of q_{link} and $1-p_{\text{mem}}$. Remarkably, the leading-order expression remains reasonably accurate all the way up to $q_{\text{link}} \sim 1$, where deviations are on the percent level. This can be explained by the fact that as q_{link} grows, the effect of memory decoherence slowly becomes negligible in case $1-p_{\text{mem}} \ll 1$, and the leading-order expression happens to be accurate up to the point where the fidelity becomes approximately constant. The lower bound however becomes very loose for larger values of q_{link} . When instead $1-p_{\text{mem}}$ is increased, we find that the leading-order expression stays accurate and the lower bound remains tight until the fidelity becomes close to that of a maximally mixed state.

To calculate both the approximate and bounded values of F , we use a Python script that evaluates Eq. (7.23) using either Eq. (7.25) (for an approximation) or Eq. (7.27) (for a lower bound). This script has been made public and can be found in our repository [54].

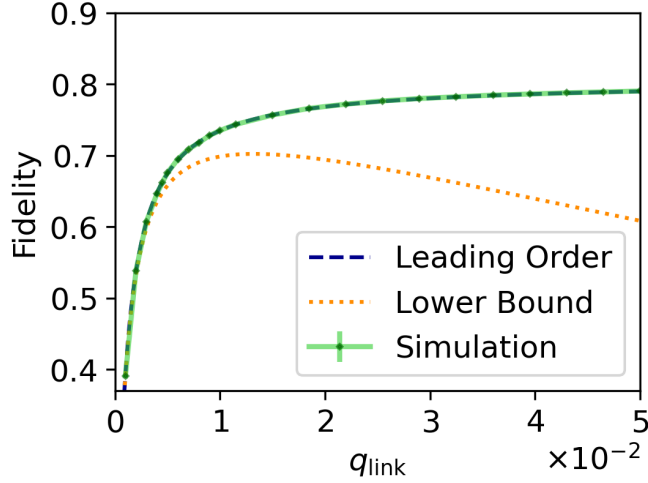


Figure 7.5: Comparison between simulation result and analytical expressions for the fidelity of Protocol 7.1. The parameters are $N = 5$, $q_{\text{BSM}} = 0.95$, $p_{\text{BSM}} = p_{\text{link}} = 1 - 10^{-2}$ and $p_{\text{mem}} = 1 - 10^{-4}$. GHZ states are locally prepared with a fidelity of 0.9, which corresponds to $p_{\text{GHZ}} \approx 0.872$. The lower bound is tight for small values of q_{link} , but not for larger values. The leading-order expression on the other hand stays accurate also for larger values of q_{link} . Each data point represents the average over 10,000 simulated executions of Protocol 7.1. Error bars represent the standard deviation of the mean and are smaller than the markers. Note that the lines showing the leading-order result and the simulation result can be hard to distinguish because of their overlap.

7

7.4 Comparison

In this section, we compare the performance of GHZ-state distribution on a symmetric star-shaped network (depicted in Figure 7.2) in case the central node is a factory node to the performance in case the central node is not a factory node. Specifically, we will compare the performance of Protocol 7.1 as described in Section 7.2 to the performance of Protocol 7.2, which requires the central node to be a 2-switch. The 2-switch serves as an intermediary in the creation of Bell states between end nodes by performing BSMs on pairs of entangled qubits. Protocol 7.2 is illustrated in Figure 7.6.

There are two differences between the factory-node setup discussed in Section 7.2, and the 2-switch setup considered here. The first difference is in the central node. The central node is the 2-switch, and it is able to store a maximum of N qubits in quantum memory (one per end node). The only way this node can manipulate qubits, is through the execution of BSMs on any pair of the qubits in its memory. When the node executes a BSM between a qubit that is entangled to one end node and a qubit that is entangled to another end node, this results in a Bell state shared between the two end nodes. The second difference is in the end nodes. As discussed in Section 7.1, end nodes that only have access to bipartite entangled resource states among themselves cannot create multipartite entangled states if they can only store a single qubit. Therefore, in order to enable the distribution of GHZ states through the use of a 2-switch, end nodes in the 2-switch setup have a quantum memory of two qubits each. Additionally, they are able to execute CNOT gates and Z-basis measurements.

We model the 2-switch setup largely the same as the factory-node setup. Each attempt

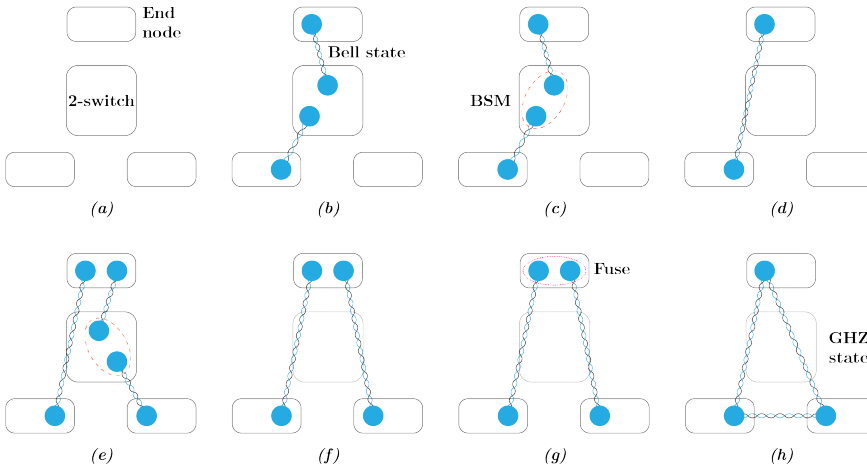


Figure 7.6: Illustration of GHZ-state distribution through a 2-switch, using Protocol 7.2. **(a)** There is one 2-switch, and there are $N = 3$ end nodes. **(b)** Bell states are distributed between the 2-switch and end nodes (Step 1 of Protocol 7.2). **(c)** When there are two Bell states, a BSM is executed (Step 2 of Protocol 7.2). **(d)** If the BSM was successful and the corresponding Pauli corrections have been applied, the two end nodes now share a Bell state (Steps 3 and 4 of Protocol 7.2). **(e)** Bell states are distributed until the 2-switch is entangled to two end nodes that are not themselves already entangled. A BSM is executed on the corresponding entangled qubits (Steps 1 - 3 of Protocol 7.2). **(f)** If the BSM was successful and the corresponding Pauli corrections have been applied, one end node is now entangled to the two other end nodes, but those other end nodes are not themselves entangled to each other (Step 4 of Protocol 7.2). **(g)** A fusion operation (which involves a CNOT gate and Z-basis measurement) is executed in the end node holding two qubits (Steps 5 and 6 of Protocol 7.2). **(h)** As a consequence of the fusion operation, the three end nodes now share a GHZ state together.

at Bell-state distribution takes a time Δt . Exchanging a classical message between the central node and an end node takes time t_{cl} , which we assume to be zero. An attempt at Bell-state distribution succeeds with probability q_{link} , a BSM succeeds with probability q_{BSM} . Whenever a Bell state is distributed by a quantum connection, the qubits are depolarized with parameter p_{link} . Qubits stored in memory undergo depolarization with parameter p_{mem} once during each time unit Δt . Finally, whenever a BSM is executed, both qubits first undergo depolarization with parameter p_{BSM} . We model CNOT gates and Z-basis measurements as noiseless.

Protocol 7.2 *Bipartite GHZ-state distribution.*

1. *Repeatedly attempt Bell-state distribution over all quantum connections for which there is a free qubit at the 2-switch until the first success occurs.*
2. *At the 2-switch, execute BSMs randomly between pairs of entangled qubits, on the condition that the end nodes that are entangled to those qubits are not yet part of the same (noisy) GHZ state. If no BSMs are executed, go back to Step 1.*
3. *Send a classical message from the 2-switch to each of the end nodes, informing them about which BSMs have been executed, and what the results of the measurements are.*
4. *Each end node that was entangled to a qubit that has partaken in a BSM, checks the result of that BSM. If the BSM failed, the qubit is reset. If it succeeded, a Pauli correction (chosen based on the outcome of the BSM) is applied to the qubit to ensure this qubit and the qubit it is entangled with are in the $|\phi_{00}\rangle$ Bell state (in the absence of noise).*
5. *Each end node that now holds two qubits in its quantum memory executes a CNOT gate between those qubits followed by a Z-basis measurement on the target qubit.*
6. *Each end node that has executed a Z-basis measurement sends a classical message with the result to all other end nodes. These end nodes then perform single-qubit Pauli corrections, chosen based on the measurement outcomes, to transform each entangled state that is shared between end nodes into a GHZ state (in the absence of noise).*
7. *If there is a GHZ state shared between all end nodes, the protocol has finished. Otherwise, go back to Step 1.*

We now make some remarks about Protocol 7.2.

- In Step 1 of Protocol 7.1, Bell-state distribution is attempted until there has been one success for each of the N quantum connections. In contrast, in Step 1 of Protocol 7.2, Bell-state distribution is only attempted until there is a round during which at least one success occurs.
- Steps 5 and 6 together implement a fusion operation [9]. Such an operation combines two GHZ states into one, at the cost of measuring out a single qubit. Here, the $|\phi_{00}\rangle$ Bell state is considered a two-qubit GHZ state. Each time a fusion operation is executed, a larger GHZ state is created, until eventually all N end nodes share in the GHZ state.

- For each time Step 1 is executed, classical communication takes up a time $3t_{\text{cl}}$ (one t_{cl} to send BSM results from the 2-switch to the end nodes, one t_{cl} to send Z-basis-measurement results from the end nodes to the 2-switch, and one t_{cl} to forward those measurement results from the 2-switch to the end nodes). When $q_{\text{link}} \ll 1$, Step 1 requires many rounds and therefore both the completion time and the qubit storage times are dominated by entanglement distribution, assuming t_{cl} is not much larger than Δt . The classical communication time can then be safely neglected, just as for Protocol 7.1. This motivates the choice to consistently set $t_{\text{cl}} = 0$ throughout this chapter.
- Protocol 7.2 is inefficient in terms of the amount of classical communication it requires. Specifically, the protocol could be altered such that all Pauli corrections are only performed after creating a GHZ-like state shared between all end nodes. Additionally, in the case of deterministic BSMs, the 2-switch does not need to inform the end nodes about the success of the measurements. In this chapter, however, we make the assumption that the exchange of classical messages is instantaneous ($t_{\text{cl}} = 0$). Therefore, any inefficiency with respect to classical communication does not affect the results presented here.

We have studied the performance of Protocol 7.2 numerically using quantum-network simulator NetSquid [11]. NetSquid is able to track time-dependent noise accurately by jumping through a timeline consisting of discrete events, at which quantum states are acted upon to account for errors. On top of NetSquid, our simulations utilize user-contributed NetSquid snippets [55, 56]. Apart from using NetSquid to study Protocol 7.2, we also set up a NetSquid simulation to study Protocol 7.1. This simulation model serves two purposes. First, it is used to verify the accuracy of the analytical results presented in Section 7.3. This verification is described in Section 7.9. Second, simulations of Protocol 7.1 are used in this section to compare the performance of Protocols 7.1 and 7.2. Note that it would also have been possible to compare simulations of Protocol 7.2 to our leading-order expressions for Protocol 7.1. Instead, we are comparing simulations to simulations. This makes the results of this section independent of the importance of subleading terms that are not included in the leading-order expressions.

Every numerical value that is reported in this chapter, either for Protocol 7.1 or for Protocol 7.2, is based on the simulation of 10,000 protocol executions. Error bars on the rate and fidelity represent the standard deviation of the mean, and are sometimes smaller than the marker size. Additionally, we remark that when simulating Protocol 7.2, the network state is not reset between executions of the protocol. It can happen that there are Bell states in the network, generated during Step 1, that never feed into a BSM during Step 2 and are thus not used to create a GHZ state. Then, there are already Bell states present in the network at the start of the next protocol execution. This entanglement is used as a resource to create the next GHZ state.

While comparing Protocols 7.1 and 7.2, we observe the relative sensitivity of their performance to the various parameters describing their setups. This comparison can help us understand in what parameter regimes the use of a factory node can be beneficial. Throughout the comparison, we use $\Delta t = 1$ to make the results independent of specific time scales. As a result, the rate is a dimensionless quantity, and can be interpreted as “average number of GHZ states distributed per round”. Our comparison will focus on the

regime $q_{\text{link}} \ll 1$. Only at the end of this Section will we briefly study what happens for $q_{\text{link}} \sim 1$.

First, we compare the rates of the two protocols. Since noise parameters of the setups cannot affect the rate at which GHZ states are distributed (only the fidelity), we limit our attention to the effects of the success probability of Bell-state distribution q_{link} , the BSM success probability q_{BSM} , and the number of end nodes N . Their effects are shown in Figure 7.7. From this figure, we must conclude that for small q_{link} Protocol 7.2 typically has a higher rate than Protocol 7.1. It is notable that the difference in rate becomes large especially for probabilistic BSMs, as the rate of Protocol 7.1 drops exponentially as q_{BSM} is decreased. However, also for deterministic BSMs Protocol 7.1 tends to be slower than Protocol 7.2, especially for larger values of N . This can be surprising, considering that Protocol 7.2 requires a larger total number of Bell states to be distributed than Protocol 7.1 ($2(N-1)$, as opposed to N for Protocol 7.1). The reason for this is that, as discussed above, Bell states that are generated but not used during one execution of Protocol 7.2 can still be used during the next execution. In Protocol 7.2, BSMs are executed continuously at the central node, thereby freeing up qubits. This allows quantum connections to generate multiple Bell states during a single execution of Protocol 7.2, which is not the case for Protocol 7.1. Combining this with the possibility to distribute Bell states ahead of time for the next GHZ state allows Protocol 7.2 to use its quantum connections more efficiently than Protocol 7.1, to such a degree that the larger number of Bell states can be distributed in a smaller amount of time.

Now, we compare the fidelities of the two protocols. From Figure 7.8, we see that Protocol 7.2 is more sensitive to the noise parameter p_{link} . This is explained by the fact that it requires more Bell states between the central node and end nodes to distribute a single GHZ state ($2(N-1)$ instead of N). Additionally, we see that Protocol 7.1 is more sensitive to p_{BSM} . The reason for this, is that the protocol executes more successful BSMs per GHZ state than Protocol 7.2 (N vs $N-1$). We note though that Protocol 7.2 also requires the execution of fusion operations at the end nodes, consisting of a CNOT gate and one Z-basis measurement. As a deterministic BSM can be implemented using a CNOT gate, a Hadamard gate, and two Z-basis measurements, it could very well be the case that the noise in the fusion operations is of similar magnitude as the noise in the BSMs. If we would have modeled the fusion operation as also inflicting depolarizing channels with parameter p_{BSM} on the involved qubits, we would likely instead have found that Protocol 7.2 is more sensitive to p_{BSM} , as it requires $N-1$ successful BSMs and $N-2$ fusions, giving a total of $2N-3$ instances at which the noise is suffered.

The final source of noise that the two setups have in common is the memory decoherence, p_{mem} . How much decoherence enters into the final GHZ state depends on the amount of time qubits are stored while executing the protocol. Therefore, it is reasonable to expect that the amount of memory decoherence behaves similar to the rate. Comparing Figures 7.7 and 7.9 reveals that indeed for both the rate and the memory decoherence, both setups perform comparably well for small q_{link} , $N = 5$ and $q_{\text{BSM}} = 1$ (and small $1 - p_{\text{mem}}$). For the rate, increasing N is in favor of Protocol 7.2. Similarly, the amount of memory decoherence seems to scale more favourably with N for Protocol 7.2 than for Protocol 7.1, although the difference is not as pronounced as for the rate. The effect of q_{BSM} , however, is reversed between the rate and memory decoherence. While the amount of memory decoherence suffered in Protocol 7.1 is unaffected by decreasing q_{BSM} , it does affect the

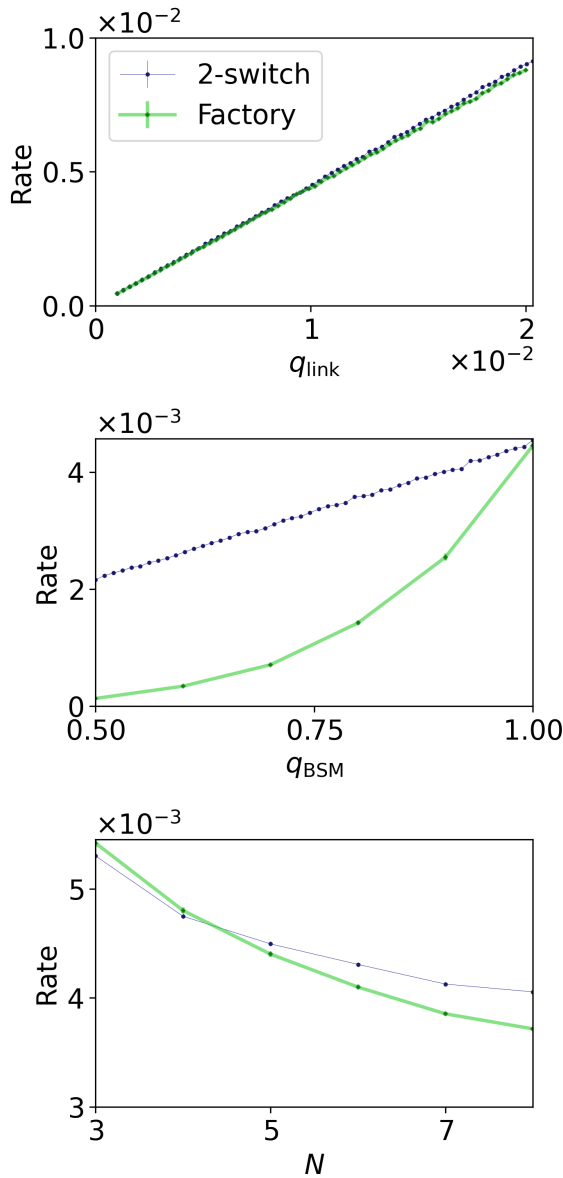


Figure 7.7: Sensitivity of the rate of Protocols 7.1 (“Factory”) and 7.2 (“2-switch”) to the success probability of Bell-state distribution q_{link} , the number of end nodes N , and the BSM success probability q_{BSM} . When the parameters are not varied over, their values are $q_{\text{link}} = 0.01$, $N = 5$ and $q_{\text{BSM}} = 1$. We see that for small values of q_{link} , the rates are of similar magnitude for $q_{\text{BSM}} = 1$ and $N = 5$, with Protocol 7.2 slightly outperforming Protocol 7.1. If either q_{BSM} is decreased or N is increased, this difference becomes more pronounced. Note that the lines in the top figure can be hard to distinguish because of their overlap. The rate is dimensionless as the round time Δt has been set to 1.

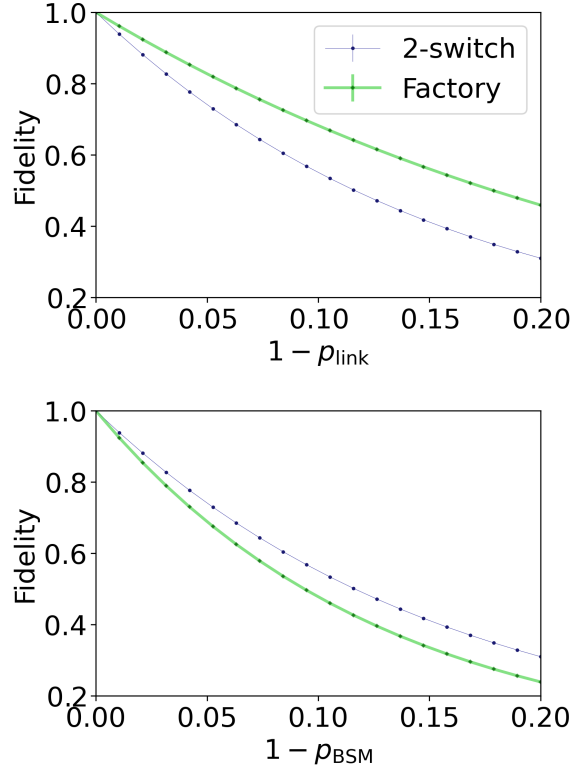


Figure 7.8: Sensitivity of the fidelity of Protocols 7.1 (“Factory”) and 7.2 (“2-switch”) to the noise in Bell states shared between the central node and the end nodes (p_{link}) and the noise in BSMs (p_{BSM}). Apart from the parameter varied over, there are no sources of noise ($p_{\text{link}} = p_{\text{BSM}} = p_{\text{mem}} = p_{\text{GHZ}} = 1$). The other parameters have the values $q_{\text{link}} = 0.01$, $N = 5$ and $q_{\text{BSM}} = 1$. While Protocol 7.1 is more resilient against noise in Bell states, Protocol 7.2 is more resilient against noise in BSMs.

performance of Protocol 7.2. The reason for this, is that while Protocol 7.1 is reset upon a failed BSM, the same is not true for Protocol 7.2. This makes Protocol 7.2 more resilient to failing BSMs in terms of rate, but less so in terms of fidelity.

Finally, we observe what happens to both the rate and the memory decoherence if q_{link} is increased beyond the $q_{\text{link}} \ll 1$ regime we have studied so far. It is seen in Figure 7.10 that the similarity in performance for $N = 5$ and $q_{\text{BSM}} = 1$ observed for small values of q_{link} disappears for larger values; here, Protocol 7.1 outperforms Protocol 7.2 with respect to both metrics. We note that for $q_{\text{link}} = 1$, the rate of Protocol 7.1 becomes one, as it takes exactly one round to distribute all N Bell states. On the other hand, the rate of Protocol 7.2 becomes approximately one half, as it takes one round to distribute N Bell states, and then another round to distribute the remaining $N - 2$ Bell states. This also explains the difference in fidelity for large values of q_{link} . Note that Protocol 7.2 had the advantage of using quantum connections more efficiently for small q_{link} because an excess number of Bell states can be distributed during one protocol execution to be used during the next. However, this advantage largely disappears for large values of q_{link} . When all Bell states

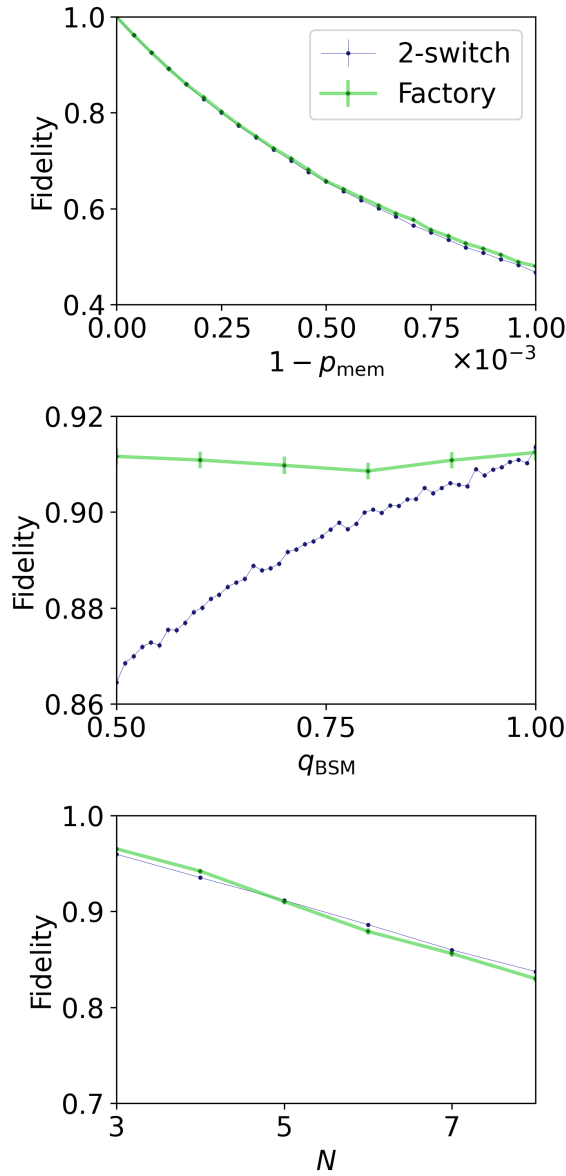


Figure 7.9: Sensitivity of the fidelity of Protocols 7.1 (“Factory”) and 7.2 (“2-switch”) to the memory depolarizing parameter p_{mem} , the number of end nodes N , and the BSM success probability q_{BSM} , when the only source of noise is memory decoherence ($p_{\text{link}} = p_{\text{BSM}} = p_{\text{GHZ}} = 1$). When the parameters are not varied over, their values are $p_{\text{mem}} = 1 - 10^{-4}$, $q_{\text{link}} = 0.01$, $N = 5$ and $q_{\text{BSM}} = 1$. We see that when both q_{link} and $1 - p_{\text{mem}}$ are small, the fidelities are approximately equal for $q_{\text{BSM}} = 1$ and $N = 5$. When q_{BSM} is decreased, this is in favor of Protocol 7.1. However, if N is increased, this is slightly in favor of Protocol 7.2. Note that the lines in the top (and to lesser degree, the bottom) figure can be hard to distinguish because of their overlap.

required to create a GHZ state are generated in quick succession, there is not much “spare time” during which these excess Bell states can be generated. We remark that for $q_{\text{link}} \sim 1$, the classical-communication time t_{cl} could have a large effect on both the rate and the amount of memory decoherence. We have assumed it to be zero because for $q_{\text{link}} \ll 1$, the classical communication time becomes negligible compared to the time required to distribute a Bell state successfully. This might or might not be true for larger values of q_{link} . Therefore, we cannot draw definitive conclusions about the relative performance between the two protocols for large values of q_{link} from Figure 7.10.

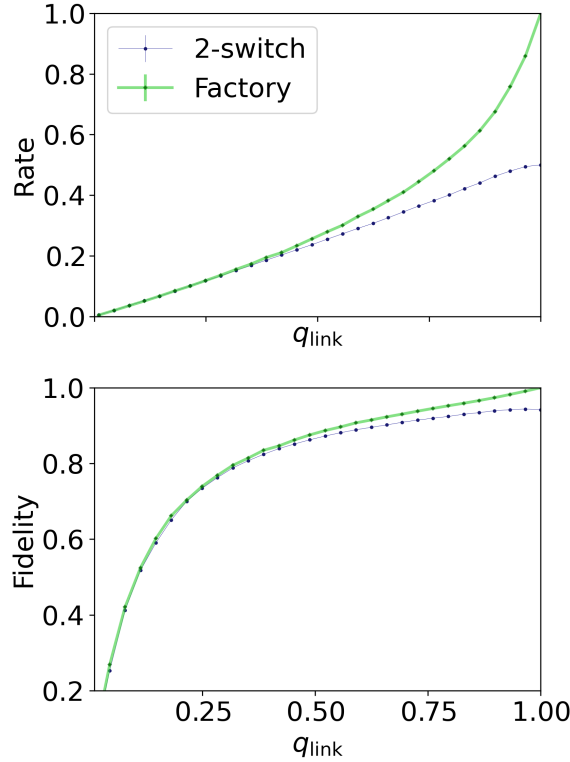


Figure 7.10: Sensitivity of both the rate and fidelity of Protocols 7.1 (“Factory”) and 7.2 (“2-switch”) to the success probability of Bell-state distribution q_{link} , when the only source of noise is memory decoherence ($p_{\text{link}} = p_{\text{BSM}} = p_{\text{GHZ}} = 1$). The other parameters are set to $p_{\text{mem}} = 1 - 10^{-2}$, $N = 5$ and $q_{\text{BSM}} = 1$. We see that while both protocols have similar performance for $q_{\text{link}} \ll 1$, Protocol 7.1 wins out both in terms of rate and fidelity for $q_{\text{link}} \sim 1$. The rate is dimensionless as the round time Δt has been set to 1.

7.5 Physical Implementation

In this section, we discuss different ways factory nodes capable of creating GHZ states could be physically realized. First, we discuss how they could be implemented using trapped ions in Section 7.5.1, and then we discuss in Section 7.5.2 how they could be implemented using nitrogen-vacancy centers in diamond.

7.5.1 Trapped Ions

The first physical implementation we discuss is based on trapped ions [57]. In an ion trap, charged atoms are suspended in an electromagnetic field. The energy levels of the ions can be used to define qubits, and these qubits can be manipulated by driving them with laser pulses. Trapped ions have properties that would make them suitable to implement a factory node, such as long coherence times [58–60], high-fidelity state preparation and readout [61–63], and a good optical interface [64–70] that has allowed for the generation of entanglement with remote nodes [39, 40, 71].

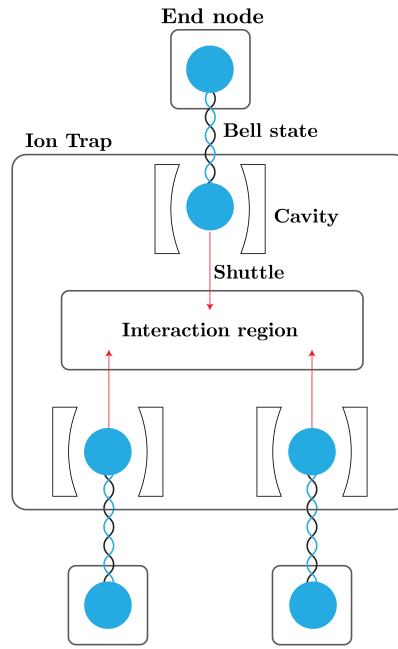
One quantum gate that can be executed on trapped ions is the Mølmer-Sørensen (MS) gate [72, 73]. This gate affects all qubits in the trap, and can be used to map maximally entangled GHZ-like states to computational-basis states. In combination with single-qubit Z-basis measurements, the MS gate can therefore be used to execute a GHZ-basis measurement on all qubits. We note that throughout this chapter we have assumed the factory node creates a GHZ state locally, and then executes BSMs between qubits of the GHZ state and qubits that are entangled to qubits at the end nodes. However, the same result is acquired (i.e., the creation of a GHZ state shared between the end nodes) when executing a GHZ-basis measurement on the qubits that are entangled to the end nodes, given that appropriate Pauli corrections are performed at the end nodes based on the outcome of the measurement.

We note that an additional challenge when using trapped ions to realize a factory node is that N different ionic qubits in the same device need to participate in simultaneous Bell-state distribution with end nodes. One potential method to allow for a good photonic interface with individual ions is to use shuttling techniques [74–80]. This way, ions could be physically moved to separate cavities, where they can be made to emit entangled photons suitable for Bell-state distribution. After ions have been successfully entangled, they can be shuttled to an interaction region where the GHZ-basis measurement is executed. This setup is illustrated in Figure 7.11. Potentially, different ion species could be used for generating and storing entanglement, such that for each task the species can be selected with the most favourable properties [81, 82].

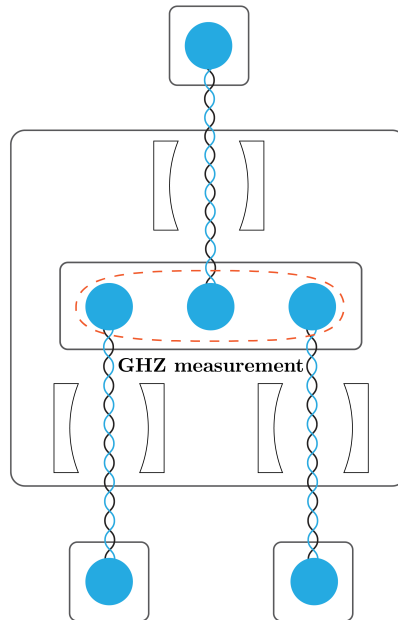
7.5.2 Nitrogen-Vacancy Centers

The second physical implementation of factory nodes we discuss is based on nitrogen-vacancy (NV) centers in diamond [35–38, 83–85]. An NV center provides an electronic communication qubit that can be used as optical interface, and is surrounded by Carbon-13 nuclear spins that can be used as memory qubits. NV centers were used to perform the first loophole-free Bell test [84], have been used to demonstrate entanglement distillation between remote nodes [37], and have recently been used to construct the first three-node quantum network [38].

A downside to NV centers is that they only provide a single communication qubit. Although entanglement can in principle be stored in N memory qubits, N Bell states cannot be distributed simultaneously, which is a prerequisite for Protocol 7.1. If the time required to perform a single attempt at Bell-state distribution with a remote node, Δt , is much larger than the time it takes to emit an entangled photon and transfer a state to a carbon atom, temporal multiplexing could potentially be used to perform N entangling attempts during a single round [86]. After Bell states have been established with all N end nodes, a GHZ-basis measurement can be executed within the NV center [87].



(a)



(b)

Figure 7.11: Implementation example of a factory node capable of distributing GHZ states based on trapped ions. **(a)** Single ions in cavities provide optical interfaces, allowing for Bell-state distribution with all $N = 3$ end nodes. After all ions are entangled, they are shuttled to an interaction region. **(b)** At the interaction region, a GHZ measurement is executed using an MS gate and single-qubit measurements, which has the effect of creating a GHZ state shared by the end nodes.

If temporal multiplexing is not feasible, however, a factory node could be realized from N separate NV centers. Each NV center can then be dedicated to creating and storing Bell states with a single end node. When all Bell states are in place, a GHZ state needs to be distributed between the N NV centers, after which deterministic BSMs can be executed. We here discern two methods of generating this GHZ state. The first is to interfere and measure entangled photons emitted by all N NV centers [4, 25]. This is illustrated in Figure 7.12 (a). However, the success probability of such schemes drops exponentially with N , and thus many attempts may be needed to generate a single GHZ state. Apart from having a negative influence on the rate of GHZ-state distribution for large N , this can also be expected to severely degrade the fidelity of the final GHZ state, as the memory qubits undergo decoherence each time the communication qubit is interfaced with [88]. An alternative method that circumvents this exponential scaling, is to add one more NV center to the factory node. After all Bell states are in place, each of the N outward facing NV centers can generate a Bell state with the extra NV center. Then, the extra NV center can execute a GHZ-basis measurement on the entangled qubits it has stored, thereby creating a GHZ state between the N outward-facing NV centers. Because Bell states can be generated with each outward-facing NV center sequentially, the number of required attempts will scale linearly with N . This can be thought of as a “factory within a factory” approach, and is illustrated in Figure 7.12 (b). Using a single NV center as a factory within a factory could be feasible even when using a single NV center as the entire factory node is not. The reason for this is that Bell-state distribution between NV centers located within the same node can happen at smaller time scales than with remote end nodes.

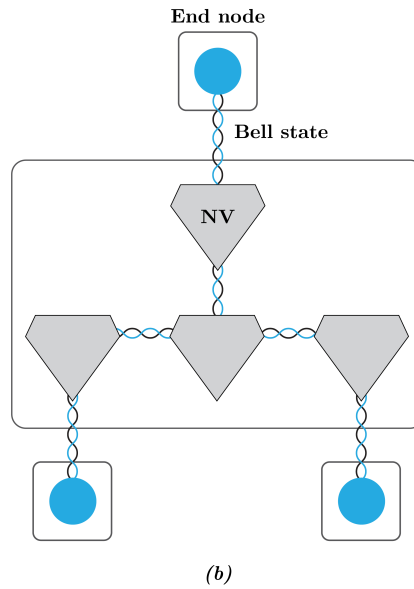
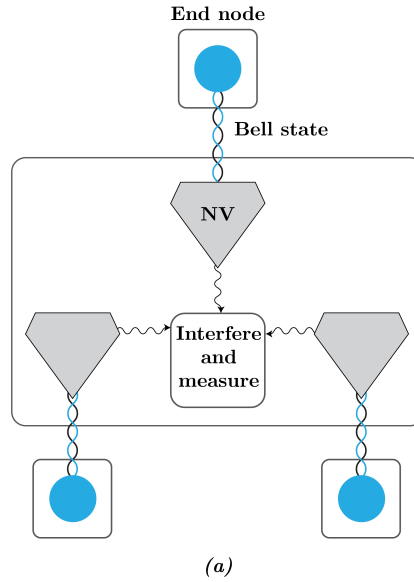


Figure 7.12: Implementation examples of factory nodes capable of distributing GHZ states based on NV centers in diamond. Within the factory node, $N = 3$ NV centers distribute and store entanglement with the end nodes. When all these NV centers are entangled, a GHZ state is distributed between them, after which each executes a BSM to teleport the GHZ state to the end nodes. **(a)** The GHZ state can be distributed between the NV centers by emitting entangled photons, interfering these photons, and measuring them. **(b)** The GHZ state can be distributed between the NV centers by first creating Bell states between all N NV centers and one additional NV center. Then, a GHZ measurement is executed at this NV center.

7.6 Conclusion

In this chapter, we have studied the distribution of multipartite entangled states in networks through local preparation of the target state at a factory node, and subsequent quantum teleportation of the state to a set of end nodes. We have presented two main results. First, we have derived analytical results for the rate and fidelity of GHZ-state distribution on a symmetrical star-shaped network, with a factory node at the center. Second, we have compared the rate and fidelity to what is achievable on the same setup without a factory node, using a 2-switch that is only capable of executing BSMs instead.

From the comparison, we found that the use of a factory node provides more resilience to noise in Bell states that are distributed between the central node and end nodes. Furthermore, when BSMs at the central node are not deterministic, using a factory node provides better protection against memory decoherence. We note that two additional advantages of using a factory node are that it only requires the end nodes to store a single qubit, while using a 2-switch requires more quantum capabilities of the end nodes, and that it can be used to distribute any multipartite target state using the same method, while the 2-switch protocol is specific to GHZ states. However, the results are not all in favor of the factory node. The 2-switch attains exponentially higher rates when BSMs are probabilistic, is less sensitive to noise in BSMs, and both the rate and (to lesser extent) the sensitivity to memory decoherence scale more favourably with the number of end nodes. We note that no thorough search for an optimal protocol utilizing a 2-switch has been performed, and doing so could boost performance even further. For example, it might be possible to increase performance by incorporating cutoff times in the protocol, that is, by discarding Bell states when they have undergone too much memory decoherence [89–92]. Cutoff times are expected to increase the fidelity, but at the cost of having a smaller rate. However, it must be noted that we have also not optimized the factory-node protocol. Also for this protocol e.g. cutoff times could be introduced. As discussed in Section 7.1, various protocols and network architectures that have been proposed in earlier work make use of factory nodes. We conclude that when hardware limitations are present, depending on the nature and severity of those limitations, it could be worthwhile to consider other types of central nodes instead.

One of our motivations for studying the factory node is to allow for assessment of proposed schemes involving factory nodes in the presence of hardware limitations. We consider the analytical results presented in this chapter a first step towards better assessment. However, we have made various assumptions that limit the scope of applicability. Here, we discuss how some of these assumptions could be removed. First, all the results in this chapter assume the star-shaped network is symmetric, meaning that noise parameters are the same for each end node (same coherence time, same Bell-state fidelity, and same quality of BSMs), and that attempts at Bell-state distribution take the same amount of time and have the same success probability for each end node. With respect to the calculation of fidelity, the assumption of same noise parameters can straightforwardly be removed within the framework of the analysis presented in this chapter. In Section 7.3.2, when evaluating Eq. (7.23), an average should be taken over all possible orderings in which end nodes generate a Bell state with the factory node. Because of the assumption of symmetry, we were able to avoid performing such an average explicitly, but in principle there is nothing preventing us from doing so. Then, each of the terms in this average can be evaluated using the Eqs. (7.114) and (7.121) (or Eqs. (7.25) and (7.27) in case p_{mem} is the same for

each qubit in the network). On the other hand, it is a key assumption in the results of Section 7.12 that the success probability of Bell-state distribution is the same for each connection. Removing this assumption, therefore, would be less straightforward and could provide an interesting subject for future research. The same holds for the assumption that the attempt durations are the same for each connection.

Second, all the results in this chapter are specific to the distribution of GHZ states. However, Protocol 7.1 could also be used to distribute other states, as long as they can be prepared locally and consist of exactly one qubit per end node. The analytical results for the rate that are presented in Section 7.3.1 are applicable for the distribution of any such state, as the time that each step takes in Protocol 7.1 does not depend on the specific quantum state, nor does the success probability of the teleportation procedure. For the analytical fidelity results that are presented in Section 7.3.2, we note that the final distributed state will be equal to the target state but with the individual qubits depolarized with the parameters p_i given by Eq. (7.17), and the full state depolarized with a parameter that was called p_{GHZ} in the GHZ case (analogously to Eq. (7.19)). The fidelity of this state as a random variable is a weighted sum over products of depolarizing parameters (analogously to Eqs. (7.22) and (7.24)). Here, the weights depend on the fidelity of the state after specific sets of qubits undergo depolarizing errors. The expected values of these products of depolarizing parameters can be evaluated using Eqs. (7.25) and (7.27). Therefore, the only ingredient missing to determine the lower bound or leading-order expression for the fidelity in case of a different target state, are the weights that appear in the fidelity. We note that in case the target state is not invariant under qubit permutations, the symmetry of the setup is broken. In that case, an explicit average should be taken over the different orders in which Bell states can be distributed, as discussed above.

7

The leading-order expressions and lower bounds presented in this chapter are accurate when the success probability per attempt at Bell-state distribution (q_{link}) is small, and when the probability of losing a qubit to the environment when storing it in memory during a single attempt ($1 - p_{\text{mem}}$) is small. When the first assumption holds, the second typically also holds; otherwise, qubits need to be stored in memory during many attempts as new states are generated, and if the probability of losing the qubit is large already for a single attempt, then the final distributed state will not be entangled. The parameter regime of small q_{link} but large $1 - p_{\text{mem}}$ is therefore not very interesting to study. E.g. for heralded entanglement generation, the success probability per attempt is expected to be small because of photon (attenuation) losses. However, there are also physical setups for which the assumption does not hold, such as quantum-repeater chains making use of error correction [29, 93–99] or massive multiplexing [45, 46, 100], for which the success probability is close to one. For such setups, the approximations presented in this chapter are not applicable, although we have found that our leading-order expression for the fidelity is remarkably accurate for large values of q_{link} . Additionally, we note that setups for which the quantum connections are near deterministic can be approximated by assuming they are fully deterministic. In this case, the protocol becomes easy to analyze, as no probabilities need to be accounted for.

Now, we discuss how the techniques presented in this chapter can be used to study the performance of quantum-network protocols different from the one we have studied. An entanglement switch is a central node that is able to generate Bell states shared with k end nodes, and executes local GHZ-state measurements on groups of n entangled qubits.

As remarked in Section 7.1, the factory-node setup studied in this chapter is equivalent to an entanglement switch with $n = k$. A possible extension of the calculations in this chapter is to apply them also to entanglement switches for which $n < k$. In Section 7.13, we present a leading-order expression for the maximum switching rate for any value of n when there is a single qubit of buffer memory per end node. However, it would be especially interesting to study the fidelity of states produced by the entanglement switch, as there are almost no known results about this. Such an extension of the fidelity calculation, assuming a symmetric star-shaped network and one qubit of buffer memory per end node, could be realized by repeating the calculation in Section 7.3.2 and replacing the parameter N (the number of end nodes, equal to k) by $n < N$ in Eq. (7.23), but not replacing it in Eq. (7.25) (which is needed to evaluate Eq. (7.23)). Evaluating this expression and verifying it (against a Monte Carlo simulation) is beyond the scope of this chapter.

Another possible extension of the work done in this chapter, is the approximation of the rate and fidelity of Bell states distributed by specific types of quantum-repeater chains. In the factory-node setup, there are N Bell states that are distributed according to geometric distributions. Entangled states that are established need to be stored in memory until all states are distributed, after which they are transformed into some target state through BSMs. If any of the BSMs fails, the protocol is restarted. The target state is a GHZ state. Now consider a quantum-repeater chain consisting of N elementary links, where entanglement swapping (i.e. BSMs) is only executed after entangled states have been distributed on all links. If any of the BSMs fail, all entanglement is discarded and Bell-state distribution starts anew. This is then exactly the same scenario as for the factory node, only the target state is not a GHZ state but a bipartite state. For the rate of such a repeater chain, analytical results similar to ours already exist [10, 51, 52].

The fidelity of Bell states distributed by such a repeater protocol can however also be analyzed using the techniques presented in this chapter. The expression for the state's fidelity in terms of different depolarizing parameters (Eq. (7.23) for the factory node) will look different (simpler, as all depolarizing noise can be “moved” to a single qubit), but the same type of expected values will need to be evaluated, allowing for the direct use of Eqs. (7.25) and (7.27) to obtain a leading-order expression and a lower bound respectively. Examples of repeater protocols where swapping is only performed after all links are present are schemes that use error correction to protect against operational errors in the repeater nodes [101], such as the ones studied for NV centers in [102]. In [102], it is remarked that accounting for depolarizing noise in individual memories is no easy task, and the authors instead assume each qubit decoheres an amount of time equal to the average waiting time. In contrast, our techniques, although approximate, do account for the depolarizing noise in each individual qubit. A similar approach to [102] is taken in [52], where the case of all swaps occurring only in the end is considered to calculate analytical bounds on the decoherence suffered when swaps are performed earlier. This approximation provides a lower bound on the fidelity by Jensen's inequality. An interesting direction for further study is to compare the tightness of Jensen's inequality to the lower bound presented in this chapter.

7.7 Data Availability

The data presented in this chapter has been made available at <https://doi.org/10.4121/19235937> [103]. Scripts that generate all the plots presented in this chapter can also be

found here.

7.8 Code Availability

All the code used to evaluate the analytical results presented in this chapter, and to perform NetSquid simulations of Protocol 7.1 and Protocol 7.2, has been made available at <https://gitlab.com/softwarequtech/netsquid-snippets/netsquid-factory> [54].

7.9 Verification of Analytical Expressions for Rate and Fidelity

In this section we verify the analytical results for the rate and fidelity of Protocol 7.1, as presented in Section 7.3, against Monte Carlo simulations of the protocol. These simulations have been performed using the quantum-network simulator NetSquid [11] and user-contributed NetSquid snippets [55, 56]. The simulation code can be found in the public repository [54]. Just like in Section 7.4, we use $\Delta t = 1$ to make the results independent of specific time scales, each data point is the result of 10,000 simulated executions of the protocol, and error bars represent the standard deviation of the mean. Often, the error bars are smaller than the marker size, making them hard to see.

There are three parameters that can influence the rate of GHZ-state distribution. These are the success probability of Bell-state distribution q_{link} , the number of end nodes N and the BSM success probability q_{BSM} . First, we examine the influence of q_{link} on the accuracy of the leading-order expression for the rate (Eq. (7.14)). On the left in Figure 7.13 we verify that the difference between the leading-order expression and its simulated value becomes negligible for $q_{\text{link}} \ll 1$. For larger values of q_{link} it is much larger, with a maximum deviation of a factor ~ 2 for $q_{\text{link}} = 1$. While not shown here, we have checked that the leading-order expression is accurate for small values of q_{link} for the number of end nodes $3 \leq N \leq 8$ (larger values become computationally demanding to simulate). The corresponding data can be found in our data repository [103]. Finally, we note that our treatment of the effect of q_{BSM} on the rate in Section 7.3 is exact. Therefore, we do not explicitly investigate the influence of this parameter on the accuracy of the leading-order result here. However, we do note that the leading-order result is accurate for at least one nontrivial value of q_{BSM} , as the parameter was set to 0.95 for Figure 7.13.

On the right in Figure 7.13, we do the same but for the fidelity, but apart from the leading-order expression (obtained from combining Eq. (7.23) with Eq. (7.25)) we also include the lower bound (obtained from combining Eq. (7.23) with Eq. (7.27)). Again we see close agreement for the leading-order expression for small values of q_{link} . Remarkably, it remains highly accurate even for $q_{\text{link}} \sim 1$. The lower bound does not attain the same level of agreement. While it is tight for very small values of q_{link} , the lower bound on the fidelity starts decreasing at $q_{\text{link}} \approx 0.015$, even though the fidelity itself is a monotonically increasing function. Consequently, the bound is very loose already for $q_{\text{link}} \gtrsim 0.015$.

On the left in Figure 7.14, the fidelity is considered as a function of p_{mem} , for a small value of q_{link} (0.01). Both the leading-order expression and lower bound remain remarkably close as $1 - p_{\text{mem}}$ grows, up to the point where the fidelity becomes close to that of a maximally-mixed state. This seems to suggest that as long as q_{link} is small, the analytical expressions are accurate for all values of p_{mem} that allow for the generation of useful entanglement. We note that the other noise parameters, p_{GHZ} , p_{BSM} and p_{link} , have a

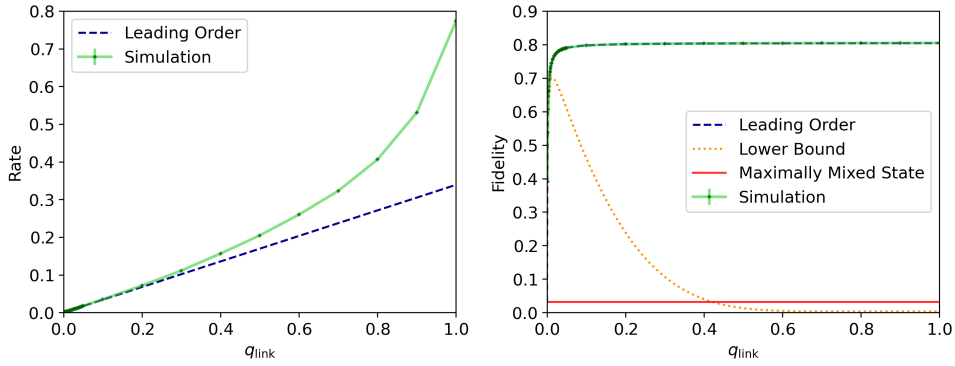


Figure 7.13: Comparison between simulation results and analytical expressions for the performance of Protocol 7.1 for different values of q_{link} . On the left, the simulated rate is compared to the leading-order expression in Eq. (7.14). On the right, the simulated fidelity is compared to the leading-order expression and lower bound from Section 7.3.2. The parameters are $N = 5$, $q_{\text{BSM}} = 0.95$, $p_{\text{BSM}} = p_{\text{link}} = 1 - 10^{-2}$ and $p_{\text{mem}} = 1 - 10^{-4}$. GHZ states are locally prepared with a fidelity of 0.9, which corresponds to $p_{\text{GHZ}} \approx 0.872$. We see that there is close agreement between analytical results for small values of q_{link} . As q_{link} is increased up to a value of one, deviations in the rate grow up to a factor of ~ 2 while the leading-order estimate for the fidelity remains accurate. The lower bound for the fidelity is tight for approximately $q_{\text{link}} \leq 0.05$ (which is hard to see in this figure) but not for larger values, eventually even dropping below the fidelity of the maximally mixed state. The rate is dimensionless as the round time Δt has been set to 1. Note that the lines showing analytical results and simulation results can sometimes be hard to distinguish because of their overlap.

much simpler effect on the fidelity as their effect does not depend on the times at which entanglement is distributed between the factory node and the different end nodes. This has allowed our treatment of these parameters to be exact and therefore verification plots where these parameters are varied are not required. We note though that in Figure 7.13 the accuracy of the analytical expressions is verified for nontrivial values of these parameters.

Finally, on the right in Figure 7.14, we consider the fidelity as a function of the number of end nodes N . We observe that the leading-order expression is accurate in the range $3 \leq N \leq 8$, while the lower bound deviates already for small values of N . The lower bound becomes increasingly loose as N increases. As it is computationally demanding to simulate large quantum states, we have not investigated the accuracy of the leading-order expression or lower bound beyond $N = 8$.

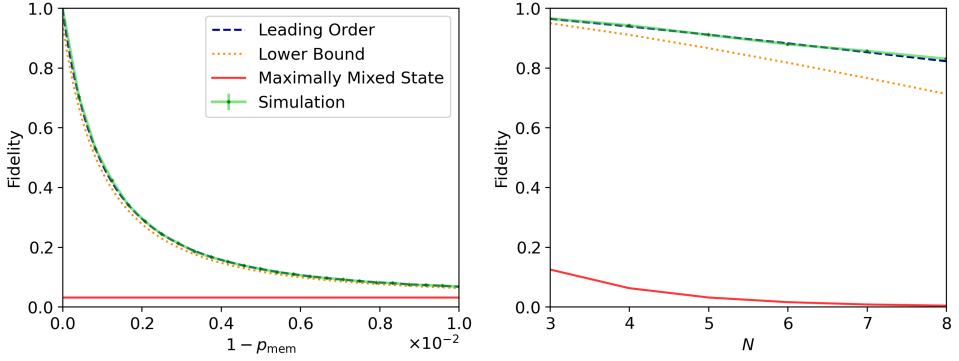


Figure 7.14: Comparison between simulation result and the analytical leading-order expression and lower bound from Section 7.3.2 for the fidelity of Protocol 7.1. The parameters, when they are not varied over, are $q_{\text{link}} = 0.01$, $N = 5$, $q_{\text{BSM}} = 1$, $p_{\text{mem}} = 1 - 10^{-4}$ and $p_{\text{BSM}} = p_{\text{link}} = p_{\text{GHZ}} = 1$. On the left, we see that when q_{link} is sufficiently small, the lower bound is tight and the leading-order expression remains accurate as $1 - p_{\text{mem}}$ becomes large, even as the fidelity becomes close to that of a maximally mixed state. On the right, we see that while the lower bound is never very tight, the leading-order expression remains accurate up to at least $N = 8$. Note that the lines showing the leading-order result, lower bound and the simulation result can be hard to distinguish because of their overlap.

7.10 Deriving the Density Matrix Created by Protocol 7.1

In this section, we formally derive the density matrix ρ that is shared after executing Protocol 7.1. To this end, we first define three relevant Hilbert spaces. Let \mathcal{H}_A be the space spanned by the N qubits used by the factory node to create GHZ states locally. Let \mathcal{H}_B be the space spanned by the N qubits used by the factory node to store Bell states shared with end nodes. Finally, let \mathcal{H}_C be the space spanned by the N qubits at the N different end nodes. Then, Protocol 7.1 does the following. First, a state $\sigma_A \otimes \tau_{BC}$ is prepared, where σ is a noisy N -qubit GHZ state, and where τ is a noisy entangled state between $2N$ qubits. Specifically, it contains depolarizing noise due to noise in the distribution of Bell states and storage of those Bell states in noisy memory. Secondly, noisy BSMs are executed between the qubits of \mathcal{H}_A and \mathcal{H}_B . The measurement outcomes are sent to the end nodes, where Pauli corrections are performed in accordance with the measurement outcomes. The final state on \mathcal{H}_C shared between the end nodes is ρ_C .

The four Bell states are defined by

$$|\phi_{ij}\rangle = (\mathbb{1} \otimes X^i Z^j) |\phi_{00}\rangle = \pm (X^i Z^j \otimes \mathbb{1}) |\phi_{00}\rangle. \quad (7.28)$$

for $i, j = 0, 1$. As is apparent from this equation, the Bell states have the special property that it does not matter (up to a global sign) on which of the two qubits the Pauli operator $X^i Z^j$ acts. This means that Pauli operators in the system can be “moved” through Bell states: $(P \otimes \mathbb{1}) |\phi_{ij}\rangle = \pm (\mathbb{1} \otimes P) |\phi_{ij}\rangle$ for any Pauli operator P . We combine this with the fact that the single-qubit depolarizing channel is a Pauli channel. That is, its Kraus operators are Pauli operators. The consequence is that also single-qubit depolarizing noise can be moved through Bell states. We can make use of this in the following way:

1. When a BSM is executed between a pair of qubits (one in \mathcal{H}_A , one in \mathcal{H}_B), we use the measurement operators (which are projectors onto the Bell states) to move all

the single-qubit depolarizing noise from \mathcal{H}_A to \mathcal{H}_B .

2. Now, because before the measurement every qubit in \mathcal{H}_B is (up to single-qubit depolarizing noise) in the state $|\phi_{00}\rangle$ with a qubit in \mathcal{H}_C , we move all single-qubit depolarizing noise and the operator $X^i Z^j$ in the definition of each measurement operator from \mathcal{H}_B to \mathcal{H}_C .

At \mathcal{H}_C the operators $X^i Z^j$ from the measurement operators cancel exactly against the Pauli corrections that are applied at Step 5 of Protocol 7.1, which are chosen to match the measurement outcome. Therefore, all measurement operators effectively become the same projector on $|\phi_{00}\rangle$, and each BSM can therefore be modelled as a projection of two qubits on the state $|\phi_{00}\rangle$. Additionally, as the probability of a measurement outcome occurring is determined by the corresponding measurement operator and all outcomes effectively have the same measurement operator, each of the four outcomes must occur with equal probability $\frac{1}{4}$. This means that the normalization factor in the post-measurement state is given by 4. We define the maximally entangled state $|\omega\rangle$ as the tensor product of N copies of $|\phi_{00}\rangle$, i.e.,

$$|\omega\rangle \equiv |\phi_{00}\rangle^{\otimes N} = \frac{1}{2^{N/2}} \sum_{i \in \{0,1\}^{\otimes 2N}} |i\rangle \otimes |i\rangle. \quad (7.29)$$

Then, we can write the post-measurement state on \mathcal{H}_C (and thus the final state produced by the protocol) as

$$\rho_C = 2^{2N} \langle \omega |_{AB} \sigma_A \otimes \tau_{BC} | \omega \rangle_{AB}. \quad (7.30)$$

Furthermore, the effect of moving all the single-qubit depolarizing channels to the system \mathcal{H}_C results in the pre-measurement states σ and τ to effectively become

$$\sigma = p_{\text{GHZ}} |\text{GHZ}\rangle\langle\text{GHZ}| + \frac{1}{2^N} (1 - p_{\text{GHZ}}) \mathbb{1}, \quad (7.31)$$

$$\tau_{BC} = \mathcal{E}_{\mathcal{E}} \left(|\omega\rangle\langle\omega|_{BC} \right), \quad (7.32)$$

where \mathcal{E} is a quantum channel applying single-qubit depolarizing noise to N different qubits. This quantum channel accounts for the noisy BSMs, the noisy distributed Bell states, and noise due to the storage of Bell states in memory. As can be seen, the noise in the GHZ state prepared within the factory is the only source of noise that is not contained in the channel \mathcal{E} . Instead, this source of noise is contained by the expression for σ .

Now, we notice that the state τ is exactly the Choi state [104, 105] of the quantum channel \mathcal{E} . Additionally, Eq. (7.30) is exactly the expression for the effect of a quantum channel in terms of its Choi state [106]. Therefore, we can immediately conclude that

$$\rho = \mathcal{E}(\sigma). \quad (7.33)$$

Using the fact that the maximally-mixed component of σ will remain maximally mixed by the effect of \mathcal{E} , we can write

$$\rho = p_{\text{GHZ}} \mathcal{E} \left(|\text{GHZ}\rangle\langle\text{GHZ}| \right) + \frac{1 - p_{\text{GHZ}}}{2^N} \mathbb{1}. \quad (7.34)$$

The final remaining step towards determining ρ is thus evaluating the quantum channel \mathcal{E} .

Because depolarizing channels have the property

$$\mathcal{D}_{\mathcal{H}_A, p_1} \circ \mathcal{D}_{\mathcal{H}_A, p_2} = \mathcal{D}_{\mathcal{H}_A, p_1 p_2}, \quad (7.35)$$

all the depolarizing noise that has been moved to the qubits of \mathcal{H}_C can be combined into a single depolarizing channel per qubit, giving

$$\mathcal{E}(|\text{GHZ}\rangle\langle\text{GHZ}|) = \mathcal{D}_{\mathcal{H}_1, p_1} \circ \mathcal{D}_{\mathcal{H}_2, p_2} \circ \dots \circ \mathcal{D}_{\mathcal{H}_N, p_N}(|\text{GHZ}\rangle\langle\text{GHZ}|). \quad (7.36)$$

Here, \circ indicates the composition (i.e., subsequent application) of the channels and \mathcal{H}_i denotes the Hilbert space of the qubit at the i^{th} end node. The combined depolarizing parameter p_i accounts for noise due to one BSM, one noisy distributed Bell state and memory decoherence at both the factory node and the end node itself, and is given by Eq. (7.17). Each depolarizing channel $\mathcal{D}_{\mathcal{H}_i, p_i}$ gives one term proportional to p_i where nothing happens to the \mathcal{H}_i subspace, and one term proportional to $1 - p_i$ where \mathcal{H}_i is traced out of the GHZ state and then put into the state $\mathbb{1}_i/2$. Thus, evaluating Eq. (7.36) comes down to accounting for all different combinations of terms. Tracing out one qubit from a GHZ state results in

$$\text{Tr}_i(|\text{GHZ}\rangle\langle\text{GHZ}|)_{1,2,\dots,k} = \frac{1}{2} \mathcal{P}_{1,2,\dots,i-1,i+1,\dots,k}, \quad (7.37)$$

where \mathcal{P} is the classically correlated, unnormalized state defined in Eq. (7.20). Tracing out a qubit from \mathcal{P} yields

$$\text{Tr}_i \mathcal{P}_{1,2,\dots,k} = \mathcal{P}_{1,2,\dots,i-1,i+1,\dots,k}, \quad (7.38)$$

unless $k = 1$, in which case

$$\text{Tr}_1 \mathcal{P}_1 = \text{Tr}_1 \mathbb{1}_1 = 2. \quad (7.39)$$

Now, we define the set $\mathcal{N} = \{1, 2, \dots, N\}$ as the set of all qubit indices. Working out the combinatorics, we find

$$\begin{aligned} \rho = & \frac{1 - p_{\text{GHZ}}}{2^N} \mathbb{1}_{\mathcal{N}} + p_{\text{GHZ}} \left[\prod_{i \in \mathcal{N}} p_i (|\text{GHZ}\rangle\langle\text{GHZ}|)_{\mathcal{N}} + \prod_{i \in \mathcal{N}} \frac{1 - p_i}{2} \mathbb{1}_{\mathcal{N}} \right. \\ & \left. + \frac{1}{2} \sum_{\substack{U \subset \mathcal{N} \\ 1 < |U| < N}} \left(\prod_{i \in U} \frac{1 - p_i}{2} \prod_{j \in \mathcal{N} \setminus U} p_j \right) \mathbb{1}_U \otimes \mathcal{P}_{\mathcal{N} \setminus U} \right]. \end{aligned} \quad (7.40)$$

Note that due to the factors appearing when taking traces in Eqs. (7.37), (7.38), and (7.39), the terms where more than 0 but less than N of the qubits are traced out effectively have an “extra” factor of $\frac{1}{2}$.

7.11 Coefficients of Fidelity Function

In this section, we derive the coefficients in the expression for the fidelity of GHZ states distributed by Protocol 7.1. That is, we show that Eq. (7.22) can be rewritten into the form of Eq. (7.23), with the coefficients $A_{|U|}$ given by Eq. (7.24).

First, we collect products of p_i 's such that we may write

$$\sum_{U \subseteq \mathcal{N}} 2^{\delta_{U|,0} + \delta_{U|,N} - 1} \left\langle \prod_{i \in U} \frac{1 - p_i}{2} \prod_{j \in \mathcal{N} \setminus U} p_j \right\rangle = \sum_{U \subseteq \mathcal{N}} B_U \left\langle \prod_{i \in U} p_i \right\rangle \quad (7.41)$$

for some constants B_U . To find these constants, we start by expanding

$$\prod_{i \in W} \frac{1 - p_i}{2} = \left(\frac{1}{2}\right)^{|W|} \sum_{V \subseteq W} (-1)^{|V|} \prod_{i \in V} p_i, \quad (7.42)$$

giving

$$\sum_{W \subseteq \mathcal{N}} 2^{\delta_{W|,0} + \delta_{W|,N} - 1} \left\langle \prod_{i \in W} \frac{1 - p_i}{2} \prod_{j \in \mathcal{N} \setminus W} p_j \right\rangle = \sum_{W \subseteq \mathcal{N}} 2^{\delta_{W|,0} + \delta_{W|,N} - 1 - |W|} \sum_{V \subseteq W} (-1)^{|V|} \left\langle \prod_{i \in V \cup (\mathcal{N} \setminus W)} p_i \right\rangle. \quad (7.43)$$

We now equate Eqs. (7.41) and (7.43). Each is the expected value of a polynomial in the independent random variables p_i . They are equal if the coefficients of all terms in the polynomial are equal. Therefore, we determine B_U by collecting all parts of the sum in Eq. (7.43) that are proportional to $\langle \prod_{i \in U} p_i \rangle$ and thus contribute to the same term. Writing as a shorthand $\overline{W} = \mathcal{N} \setminus W$, this gives

$$B_U = \sum_{W \subseteq \mathcal{N}} 2^{\delta_{W|,0} + \delta_{W|,N} - 1 - |W|} \sum_{V \subseteq W} (-1)^{|V|} \delta_{V \cup \overline{W}, U}, \quad (7.44)$$

where we are slightly abusing notation by using the Kronecker delta for two sets. It is defined by

$$\delta_{U,V} = \begin{cases} 1 & \text{for } U = V, \\ 0 & \text{otherwise,} \end{cases} \quad (7.45)$$

where U and V are sets. The delta function ensures that we are adding together exactly those coefficients of (7.44) that contribute to the right term of the polynomial.

We note that the equation $V \cup \overline{W} = U$ implies that $\overline{W} \subseteq U$. Therefore, the Kronecker delta will always be zero when this condition does not hold, allowing us to refine the summation limit and write

$$B_U = \sum_{\substack{W \\ \overline{W} \subseteq U}} 2^{\delta_{W|,0} + \delta_{W|,N} - 1 - |W|} \sum_{V \subseteq W} (-1)^{|V|} \delta_{V \cup \overline{W}, U}. \quad (7.46)$$

The Kronecker delta now limits the sum to values of V and W where $V \cup \overline{W} = U$ holds. Because $V \subseteq W$ for all terms in the sum, it always holds that $V \cap \overline{W} = \emptyset$, i.e. there is no overlap between the two sets. Therefore, the equation $V \cup \overline{W} = U$ implies that $V = U \setminus \overline{W}$. Additionally, because $\overline{W} \subseteq U$ for all terms in the sum, the equation $V = U \setminus \overline{W}$ implies that $V \cup \overline{W} = U$. It follows that the two equations are equivalent given the conditions imposed on V and W by the summation limits, and we can safely rewrite the Kronecker delta function to obtain

$$B_U = \sum_{\substack{W \\ \overline{W} \subseteq U}} 2^{\delta_{W|,0} + \delta_{W|,N} - 1 - |W|} \sum_{V \subseteq W} (-1)^{|V|} \delta_{V, U \setminus \overline{W}}. \quad (7.47)$$

Since $U \setminus \overline{W}$ contains only elements not in \overline{W} , and since W contains all elements in \mathcal{N} that are not in \overline{W} , it follows that $U \setminus \overline{W} \subseteq W$. If this were not always the case, it could be the case for some W that the sum over $V \subseteq W$ contains no terms for which the delta function is nonzero. But since it is the case, for every W there is exactly one value of V , namely $V = U \setminus \overline{W}$, for which the delta function has a nonzero value. For this value, $|V| = |U| - |\overline{W}|$, and therefore the equation becomes

$$B_U = \sum_{\substack{W \\ \overline{W} \subseteq U}} 2^{\delta_{|W|,0} + \delta_{|W|,N-1-|W|}} (-1)^{|U|-|\overline{W}|}. \quad (7.48)$$

To further resolve the equation, we note that when the cardinality of \overline{W} is equal to $|\overline{W}| = i$, there are exactly $|U|$ choose i different ways \overline{W} can be chosen from U . Since only the cardinalities of \overline{W} and W (with $|W| = N - i$) appear in the sums, this allows us to write

$$B_U = \sum_{i=0}^{|U|} \binom{|U|}{i} 2^{\delta_{N-i,0} + \delta_{N-i,N-1-N+i}} (-1)^{|U|-i} = \sum_{i=0}^{|U|} \binom{|U|}{i} 2^{\delta_{i,N} + \delta_{i,0-1-N+i}} (-1)^{|U|-i}. \quad (7.49)$$

Now, we make a change of variable, $i \rightarrow |U| - i$. Conveniently, the binomial coefficient is invariant under this transformation, giving

$$B_U = \sum_{i=0}^{|U|} \binom{|U|}{i} 2^{\delta_{|U|-i,N} + \delta_{|U|-i,0-1-N+|U|-i}} (-1)^i = \left(\frac{1}{2}\right)^{N+1-|U|} \sum_{i=0}^{|U|} \binom{|U|}{i} 2^{\delta_{|U|,N} + \delta_{i,0}} \left(\frac{-1}{2}\right)^i. \quad (7.50)$$

By the binomial theorem,

$$\sum_{i=0}^{|U|} \binom{|U|}{i} \left(\frac{-1}{2}\right)^i = \left(1 - \frac{1}{2}\right)^{|U|} = \left(\frac{1}{2}\right)^{|U|}. \quad (7.51)$$

By adding the contributions from when the delta functions are nonzero separately on top of that, we find

$$B_U = \left(\frac{1}{2}\right)^{N+1-|U|} \left\{ \left(\frac{1}{2}\right)^{|U|} + \delta_{|U|,N} + \left(\frac{-1}{2}\right)^{|U|} \right\}, \quad (7.52)$$

which can be rewritten as (using the fact that $N - |U| = 0$ whenever the remaining delta function is nonzero)

$$B_U = \left(\frac{1}{2}\right)^{N+1} \left(1 + (-1)^{|U|}\right) + \frac{1}{2} \delta_{|U|,N}. \quad (7.53)$$

Noticing furthermore that the value of B_U only depends on the cardinality of the set U , we write

$$B_{|U|} = \begin{cases} \frac{1}{2^N} + \frac{1}{2} \delta_{|U|,N} & \text{if } |U| \text{ is even,} \\ \frac{1}{2} \delta_{|U|,N} & \text{if } |U| \text{ is odd.} \end{cases} \quad (7.54)$$

Now, we can derive the coefficients $A_{|U|}$ in Eq. (7.23). To this end, we substitute Eq. (7.17) into Eq. (7.41) to find

$$\begin{aligned} \sum_{U \subseteq \mathcal{N}} 2^{\delta_{|U|,0} + \delta_{|U|,N-1}} \left\langle \prod_{i \in U} \frac{1-p_i}{2} \prod_{j \in \mathcal{N} \setminus U} p_j \right\rangle &= \sum_{U \subseteq \mathcal{N}} B_{|U|} (p_{\text{link}} p_{\text{BSM}}^2)^{|U|} \left\langle \prod_{i \in U} (p_{\text{mem}}^2)^{\Delta n_i} \right\rangle \\ &= \sum_{U \subseteq \mathcal{N}} A_{|U|} \left\langle \prod_{i \in U} (p_{\text{mem}}^2)^{\Delta n_i} \right\rangle \end{aligned} \quad (7.55)$$

where $A_{|U|}$ is exactly as defined in Eq. (7.24). Therefore, Eq. (7.23) indeed follows from Eq. (7.22).

7.12 Expected Values for Memory Decoherence

In this section, we derive both a leading-order expression and a lower bound for the effect of memory decoherence on the fidelity of GHZ states produced using Protocol 7.1. These results allow us to write down a leading-order expression for the fidelity of states produced using this protocol (Eq. (7.25)), and a lower bound ((7.27)). To this end, we first derive more general results for the case where the decoherence rate is different for each quantum memory.

7.12.1 Indices

Trying to establish a Bell state happens according to discrete rounds, with the probability of succeeding during each round being q_{link} for all end nodes. When all Bell states are in place, a GHZ state is generated locally and then teleported by the factory node towards the end nodes after which, in case all BSMs are successful, the protocol terminates. While the BSM success probability influences the rate with which GHZ states can be distributed (see Section 7.3.1), it will not influence the fidelity, since all states are discarded whenever a BSM fails and the protocols starts again from the beginning. Therefore, without loss of generality, we will henceforth assume BSMs are deterministic. In that case, each execution of the protocol is uniquely defined by which end node established a Bell state during which attempt. This can be described by assigning indices $i \in \mathcal{N}$ to the different end nodes (where $\mathcal{N} = \{1, \dots, N\}$ as before), and denoting the round during which end node i established a Bell state by n_i .

For any given realization of the protocol, an ordering can be imposed on the indices in correspondence with the order in which the different Bell states were distributed. We denote the ordered index corresponding to end node i by d_i , and they have the property

$$n_i \geq n_j \quad \text{if} \quad d_i > d_j. \quad (7.56)$$

for $i, j = 1, 2, \dots, N$. That means that if $d_5 = 1$, end node with label 5 was the first end node to share a Bell state with the factory node, while if $d_1 = N$, end node with label 1 was the last to do so.

What we want to calculate, are expected values including only the waiting times of a specific subset of the end nodes. We denote this subset $V \subseteq \mathcal{N}$, with $|V| = M$, and define the indices v_1, v_2, \dots, v_M as the ordered elements of the subset V . That is, $V = \{v_1, v_2, \dots, v_M\}$ and

$$d_{v_{i+1}} > d_{v_i} \quad (7.57)$$

for $i = 1, 2, \dots, M - 1$. To simplify our notation, we now introduce the symbols

$$\begin{aligned} c_i &\equiv d_{v_i}, \\ m_i &\equiv n_{v_i}. \end{aligned} \quad (7.58)$$

We note that Eq. (7.56) and (7.57) together imply that

$$m_{i+1} \geq m_i \quad (7.59)$$

for $i = 1, 2, \dots, M - 1$.

An example of the values these different indices can take, let us consider the case $N = 4$. For a specific realization of the protocol, it might be that the end node with index 2 shared a Bell state with the factory node first during $n_2 = 3$, then 3 during $n_3 = 5$, then 1 at $n_1 = 10$ and finally 4 at $n_4 = 17$. In that case, $d_2 = 1$, $d_3 = 2$, $d_1 = 3$, and $d_4 = 4$. Now, if we take $V = \{1, 3\}$, then $v_1 = 3$ and $v_2 = 1$. This gives, $c_1 = d_3 = 2$ and $c_2 = d_1 = 3$, which correctly satisfies $c_2 > c_1$. Furthermore, $m_1 = n_3 = 5$ and $m_2 = n_1 = 10$.

7.12.2 Probability Building Blocks

At the start of Protocol 7.1, there are N quantum connections simultaneously distributing Bell states between the factory node and end nodes $1, 2, \dots, N$. Each of these will follow a geometric distribution. That is,

$$\Pr(\text{Bell state } i \text{ is successfully distributed during round } n) = q_{\text{link}}(1 - q_{\text{link}})^{n-1}, \quad (7.60)$$

for $i = 1, 2, \dots, N$, and $n = 1, 2, 3, \dots$.

Now, we introduce some probabilities based on this that will be useful later on:

$$\begin{aligned} P_{i/N}(n) &\equiv \Pr(\text{during round } n, \text{ the } i^{\text{th}} \text{ Bell state is distributed,} \\ &\quad \text{given that there were zero before round 1,} \\ &\quad \text{and distribution takes place on } N \text{ quantum connections}), \end{aligned} \quad (7.61)$$

$$\begin{aligned} P'_{i/N}(n) &\equiv \Pr(\text{after round } n, \text{ exactly } i \text{ Bell states are distributed,} \\ &\quad \text{given that there were zero before round 1,} \\ &\quad \text{and distribution takes place on } N \text{ quantum connections;} \\ &\quad \text{the } i^{\text{th}} \text{ Bell state was established during round } n). \end{aligned} \quad (7.62)$$

Note that the difference between $P_{i/N}(n)$ and $P'_{i/N}(n)$ is that the first also includes the probability for the case that, during round n , more Bell states are simultaneously established than was required to reach i . The first of these two is a properly normalized probability distribution, and has the random variable $n_{i/N}$ associated to it, representing the number of rounds needed to distribute i Bell states using N quantum connections. A special case is the variable $n_{1/N}$, as it is a geometrically distributed random variable. The reason for this is that the probability that the first Bell state is distributed during round n , is equal to the probability that all quantum connections failed up until round n , and that not all quantum connections fail during round n . That is,

$$P_{1/N}(n) = [1 - (1 - q_{\text{link}})^N](1 - q_{\text{link}})^{N(n-1)}, \quad (7.63)$$

which is geometric with $1/\langle n_{1/N} \rangle = 1 - (1 - q_{\text{link}})^N$.

Furthermore, we define

$$P_{i/N}^j(n) \equiv \Pr \left(\begin{array}{l} \text{after round } n, \text{ exactly } i \text{ Bell states are distributed,} \\ \text{given that there were zero before round 1,} \\ \text{and distribution takes place on } N \text{ quantum connections;} \\ j \text{ of those } i \text{ Bell states were distributed during round } n \end{array} \right). \quad (7.64)$$

Here, $j \leq i \leq N$, and $j \geq 1$. This allows us to be more specific about the number of success events during the last round. Since for $P_{i/N}^j(n)$ the number of success events at round n can be any number larger than zero (and, of course, smaller or equal to i), we can write down the relation

$$P'_{i/N}(n) = \sum_{l=1}^i P_{i/N}^l(n). \quad (7.65)$$

Similar, since $P_{i/N}(n)$ is the same as $P'_{i/N}(n)$ but also includes to possibility that “too many” successes occurred during round n , bringing the number of entangled states above i , we can write

$$P_{i/N}(n) = \sum_{k=0}^{N-i} \sum_{l=1}^i P_{(i+k)/N}^{k+l}(n) = P'_{i/N}(n) + \sum_{k=1}^{N-i} \sum_{l=1}^i P_{(i+k)/N}^{k+l}(n). \quad (7.66)$$

Note however that both equations only hold for $i > 0$.

It is possible to derive a recursive relation for $P_{i/N}^j(n)$. We can express the probability as

$$P_{i/N}^j(n) = \binom{N-(i-j)}{j} \Pr \left(\begin{array}{l} \text{during round } n, \text{ out of } N-(i-j) \text{ quantum connections} \\ \text{trying to establish a Bell state, exactly } j \text{ succeed} \end{array} \right) \quad (7.67) \\ \times \Pr \left(\text{after round } n-1, \text{ there were } i-j \text{ Bell states} \right).$$

The first probability is simply $q_{\text{link}}^j (1 - q_{\text{link}})^{N-i}$. The second probability depends on what $i-j$ is. If it is zero, it is simply the probability that there have been no success events up to and including round $n-1$, i.e. $(1 - q_{\text{link}})^{N(n-1)}$. If $i-j \neq 0$, we must distinguish between the different cases in which the final Bell state is established during different rounds. This gives

$$\begin{aligned} & \Pr \left(\text{after round } n-1, \text{ there were } i-j \text{ Bell states} \right) \\ &= \sum_{n'=1}^{n-1} P'_{(i-j)/N}(n') \times \Pr \left(\begin{array}{l} \text{none out of } N-(i-j) \text{ active quantum connections distribute a} \\ \text{Bell state after round } n' \text{ up to round } n-1 \end{array} \right) \\ &= \sum_{n'=1}^{n-1} P'_{(i-j)/N}(n') (1 - q_{\text{link}})^{[N-(i-j)][(n-1)-n']}. \end{aligned} \quad (7.68)$$

Now, we note that the definition of $P'_{i/N}(n)$ is somewhat ambiguous for $i = 0$ and $n = 0$. Therefore, we here define it explicitly for these values, in such a way that we can extend the above relation to the cases $j = i$ and $n = 1$. The definition is as follows:

$$P'_{0/N}(n) \equiv \delta_{n,0}. \quad (7.69)$$

This allows us to extend the above sum to include $n' = 0$, which gives exactly what we need for $j = i$ and vanishes anyway for $j < i$, i.e.

$$P_{i/N}^j(n) = \binom{N-i+j}{j} \sum_{n'=0}^{n-1} q_{\text{link}}^j (1 - q_{\text{link}})^{(n-n')(N-i+j)-j} P'_{(i-j)/N}(n'). \quad (7.70)$$

We can rewrite this equation into a form that makes it easier to deal with later on. Using Eq. (7.63) we can write

$$P_{i/N}^j(n) = \binom{N-i+j}{j} \frac{q_{\text{link}}^j (1 - q_{\text{link}})^{N-i}}{1 - (1 - q_{\text{link}})^{N-i+j}} \sum_{n'=0}^{n-1} P_{1/(N-i+j)}(n - n') P'_{(i-j)/N}(n'). \quad (7.71)$$

Furthermore, to turn this into a true recursion relation, we also fill in Eq. (7.65) to find

$$P_{i/N}^j(n) = \binom{N-i+j}{j} \frac{q_{\text{link}}^j (1 - q_{\text{link}})^{N-i}}{1 - (1 - q_{\text{link}})^{N-i+j}} \sum_{n'=0}^{n-1} P_{1/(N-i+j)}(n - n') \sum_{l=1}^i P_{i/N}^l(n). \quad (7.72)$$

However, we must be aware of the fact that this equation only covers the $i > 0$ cases. If $i = j = 0$, there are no Bell states distributed at all, and thus we can also not split up the success events as we did in our arguing above. Analogues to $P'_{0/N}(n) = \delta_{n,0}$, we define $P_{0/N}^0(n) = \delta_{n,0}$. Furthermore, while $P_{i/N}^j(n)$ is technically undefined for $j = 0$ and $i > 0$, we define it to be zero for later convenience. Note that therefore $P_{i/N}^0(n)$ for $i > 0$ is not equal to the probability that there are i Bell states after round n , of which there where 0 distributed during round n , since this would be a nonzero quantity.

Finally, we will abuse notation to write

$$\sum_{n=0}^{\infty} n P_{i/N}^j(n) = \langle n_{i/N}^j \rangle, \quad (7.73)$$

even though $P_{i/N}^j(n)$ is not a normalized probability distribution and thus $n_{i/N}^j$ is not a well-defined random variable.

7.12.3 Probability Distribution of Links

Now, we introduce the probability distribution

$$P(m_1 = m'_1, m_2 = m'_2, \dots, m_M = m'_M), \quad (7.74)$$

which is the probability that, if Protocol 7.1 is executed once, and labels are defined and ordered as described above, that m_i has the value m'_i for each $i = 1, 2, \dots, M$. Below, we will

use this probability distribution to write down expected values of the type we need to account for memory decoherence. First, we will investigate what the probability distribution looks like.

Then, what is the probability that Bell state c_i is distributed at round m_i ? Consider the fact that Bell state c_{i-1} was distributed at round m_{i-1} . During this round, many Bell states could have been distributed simultaneously, as multiple quantum connections are attempting to distribute them in parallel. However, assume for the moment that only Bell state c_{i-1} was distributed at round m_{i-1} . In that case, the probability that c_i succeeds during round m_i is equal to the probability that $c_i - c_{i-1}$ Bell states are distributed using $N - c_{i-1}$ parallel quantum connections in $m_i - m_{i-1}$ rounds, which is the probability $P_{(c_i - c_{i-1})/(N - c_{i-1})}(m_i - m_{i-1})$ defined above. Now assume that there were in fact multiple successes during round m_{i-1} . Specifically, let it be such that there were so many successes that after round m_{i-1} , the number of distributed Bell states is $c_{i-1} + k_{i-1}$. That is, k_{i-1} is the “overshoot” during round m_{i-1} . Then, we can distinguish two different cases. In the first case, $k_{i-1} < c_i - c_{i-1}$, and Bell state number c_i is not yet distributed after round m_{i-1} . We can then repeat the logic above: the probability of distributing Bell state c_i during round m_i is $P_{(c_i - c_{i-1} - k_{i-1})/(N - c_{i-1} - k_{i-1})}(m_i - m_{i-1})$. However, in the second case, $k_{i-1} \geq c_i - c_{i-1}$; the overshoot is so large that Bell state c_i was already distributed during round m_{i-1} , and the probability can be written as the Kronecker delta function $\delta_{m_i, m_{i-1}}$.

Using this logic, the probability distribution can be completely characterized using $P_{i/N}^j(n)$ -type probabilities that were defined above. For each c_i , we can put a Heaviside step function $\theta(c_i - c_{i-1} - k_{i-1} - 1)$ to account for the case where the overshoot was small enough to ensure $m_i \neq m_{i-1}$, and $\theta(c_{i-1} + k_{i-1} - 1 - c_i)$ when they are the same. The Heaviside step function is defined as

$$\theta(x) = \begin{cases} 0 & \text{if } x < 0, \\ 1 & \text{if } x \geq 0. \end{cases} \quad (7.75)$$

There are just two additional aspects we need to consider. First of all, the number of successes during round m_{i-1} is not necessarily equal to k_{i-1} ; k_{i-1} is just the overshoot. It could e.g. be the case that $c_{i-1} = 6$ and $k_{i-1} = 3$. That means that after m_{i-1} , the number of distributed Bell states is 9. But it says nothing about the number of Bell states before that round. It could e.g. be 4, in which case there were 5 successes during round m_{i-1} . We denote the number of “additional” successes that did not go into the overshoot by l_{i-1} . Thus, the number of successes during round m_{i-1} is $l_{i-1} + k_{i-1}$. In the example, $l_{i-1} = 2$. Secondly, we need to consider the fact that if k_{i-1} is large enough that $m_i = m_{i-1}$, then the overshoot k_i must be equal to $k_{i-1} - (c_i - c_{i-1})$, which can be accounted for using a

Kronecker delta. Combining all this into a single equation, we find

$$\begin{aligned}
& \Pr(m_1 = m'_1, m_2 = m'_2, \dots, m_M = m'_M) \\
&= \prod_{i=1}^M \sum_{k_i=0}^{N-c_i} \left[\theta(c_i - c_{i-1} - k_{i-1} - 1) \sum_{l_i=1}^{c_i - c_{i-1} - k_{i-1}} P_{(c_i + k_i - c_{i-1} - k_{i-1})/(N - c_{i-1} - k_{i-1})}^{k_i + l_i} (m'_i - m'_{i-1}) \right. \\
&\quad \left. + \theta(c_{i-1} + k_{i-1} - c_i) \delta_{k_i, c_{i-1} + k_{i-1} - c_i} \delta_{m'_i, m'_{i-1}} \right] \\
&= \prod_{i=1}^M \left[\sum_{k_i=0}^{N-c_i} \sum_{l_i=-k_i}^{c_i - c_{i-1} - k_{i-1}} \left(\theta(l_i - 1) + \delta_{k_i, c_{i-1} + k_{i-1} - c_i} \right) \right. \\
&\quad \left. \times P_{(c_i + k_i - c_{i-1} - k_{i-1})/(N - c_{i-1} - k_{i-1})}^{k_i + l_i} (m'_i - m'_{i-1}) \right],
\end{aligned} \tag{7.76}$$

where we set $m'_0 \equiv c_0 \equiv k_0 \equiv 0$ by definition to allow for the more compact form of the equation.

7.12.4 Expected Value

In order to calculate the expected values for the amount of decoherence in quantum memory, what we need is a probability distribution not for at what time each Bell state was distributed, but for how long each Bell state had to sit in memory before Protocol 7.1 terminated. Luckily, the second can be easily obtained from the first. First, we define n_f to be the round during which the final Bell state is distributed. Then, we define $\Delta m_i = n_f - m_i$ as the number of rounds Bell state v_i waits in memory until all Bell states are distributed. The probability distribution we are then interested in is

$$\Pr(\Delta m_1 = \Delta m'_1, \Delta m_2 = \Delta m'_2, \dots, \Delta m_M = \Delta m'_M), \tag{7.77}$$

which can be written as

$$\begin{aligned}
& \Pr(\Delta m_1 = \Delta m'_1, \Delta m_2 = \Delta m'_2, \dots, \Delta m_M = \Delta m'_M) \\
&= \sum_{n'_f=1}^{\infty} \prod_{i=1}^M \left(\sum_{m'_i=1}^{\infty} \delta_{n'_f - m'_i, \Delta m'_i} \right) \Pr(m_1 = m'_1, m_2 = m'_2, \dots, m_M = m'_M, n_f = n'_f).
\end{aligned} \tag{7.78}$$

The latter probability distribution is the one from Eq. 7.76, except for the additional condition $n_f = n'_f$. However, this condition can be easily incorporated by extending the set V of end nodes under consideration slightly, such that we include v_{M+1} which corresponds to the last Bell state that is distributed. That is,

$$c_{M+1} = N, \tag{7.79}$$

and $m_{N+1} = n_f$. In that case, we can directly use Eq. 7.76 to write down

$$\begin{aligned}
 & \Pr(\Delta m_1 = \Delta m'_1, \Delta m_2 = \Delta m'_2, \dots, \Delta m_M = \Delta m'_M) \\
 &= \sum_{m'_{M+1}=1}^{\infty} \prod_{i=1}^M \left(\sum_{m'_i=1}^{\infty} \delta_{n'_f - m'_i, \Delta m'_i} \right) \Pr(m_1 = m'_1, m_2 = m'_2, \dots, m_M = m'_M, m_{M+1} = m'_{M+1}) \\
 &= \sum_{m'_{M+1}=1}^{\infty} \prod_{i=1}^M \left(\sum_{m'_i=1}^{\infty} \delta_{m'_{M+1} - m'_i, \Delta m'_i} \right) \prod_{i=1}^{M+1} \left[\sum_{k_i=0}^{N-c_i} \sum_{l_i=-k_i}^{c_i - c_{i-1} - k_{i-1}} \left(\theta(l_i - 1) + \delta_{k_i, c_{i-1} + k_{i-1} - c_i} \right) \right. \\
 &\quad \left. \times P_{(c_i + k_i - c_{i-1} - k_{i-1}) / (N - c_{i-1} - k_{i-1})}^{k_i + l_i}(m'_i - m'_{i-1}) \right].
 \end{aligned} \tag{7.80}$$

First, we resolve the Kronecker delta functions. If $\Delta m'_i = m'_{M+1} - m'_i$, then $m'_i - m'_{i-1} = \Delta m_{i-1} - \Delta m_i$. Therefore, if we define $\Delta m'_{M+1} \equiv 0$ and write $\Delta m'_0 = m'_{M+1}$, we find

$$\begin{aligned}
 & \Pr(\Delta m_1 = \Delta m'_1, \Delta m_2 = \Delta m'_2, \dots, \Delta m_M = \Delta m'_M) \\
 &= \sum_{\Delta m'_0=0}^{\infty} \prod_{i=1}^{M+1} \left[\sum_{k_i=0}^{N-c_i} \sum_{l_i=-k_i}^{c_i - c_{i-1} - k_{i-1}} \left(\theta(l_i - 1) + \delta_{k_i, c_{i-1} + k_{i-1} - c_i} \right) \right. \\
 &\quad \left. \times P_{(c_i + k_i - c_{i-1} - k_{i-1}) / (N - c_{i-1} - k_{i-1})}^{k_i + l_i}(\Delta m'_{i-1} - \Delta m'_i) \right].
 \end{aligned} \tag{7.81}$$

Now, we will use these results to calculate the expected value

$$\begin{aligned}
 G(r_1, r_2, \dots, r_M) &\equiv \left\langle \prod_{i=1}^M (1 - r_i)^{\Delta m_i} \right\rangle \\
 &= \prod_{i=1}^M \left[\sum_{\Delta m'_i=0}^{\infty} (1 - r_i)^{\Delta m'_i} \right] \Pr(\Delta m_1 = \Delta m'_1, \Delta m_2 = \Delta m'_2, \dots, \Delta m_M = \Delta m'_M)
 \end{aligned} \tag{7.82}$$

Here, the r_i are some numbers between zero and one. The fidelity of GHZ states created by Protocol 7.1 is expressed as a sum over such expected values in Eq. (7.23). Therefore, if we are able to evaluate Eq. (7.82), we are able to evaluate the fidelity using the substitution $r_i = 1 - p_{\text{mem}}^2$ for all i (i.e. r_i becomes the probability that a quantum state is lost in memory per round of Bell-state distribution). We make two remarks about the expected value G . First, an evaluation of G is a more general result than what we need to calculate the fidelity, as here we allow each r_i to take a different value. As discussed in Section 7.6, this makes such a result suitable to study asymmetric quantum networks. Second, in the definition of G , a product over quantities of the form $1 - r_i$ appears. We could just as well make the redefinition $r_i \rightarrow 1 - r_i$. This would make the definition of G more compact, and would lead to the perhaps more natural mapping $r_i = p_{\text{mem}}^2$ in order to calculate the fidelity. However, we are ultimately interested in the regime $1 - p_{\text{mem}}^2 \ll 1$, where the probability of losing a quantum state when storing it in memory for a single round is small. This translates here to $r_i \ll 1$. Therefore, if we want to calculate the fidelity to leading order in $1 - p_{\text{mem}}^2$, we need to evaluate G to leading order in the variables r_i . This is easier to do than working to leading order in $1 - r_i$.

First of all, we substitute Eq. (7.81) into Eq. (7.82). By defining $r_0 \equiv 0$, we can conveniently write the result as

$$\begin{aligned}
 & G(r_1, r_2, \dots, r_M) \\
 &= \sum_{\Delta m'_0, \Delta m'_1, \dots, \Delta m'_M=0}^{\infty} \prod_{i=1}^{M+1} \left[\sum_{k_i=0}^{N-m_i} \sum_{l_i=-k_i}^{m_i-m_{i-1}-k_{i-1}} \left(\theta(l_i-1) + \delta_{k_i, m_{i-1}+k_{i-1}-m_i} \right) \right. \\
 & \quad \left. \times (1-r_{i-1})^{\Delta n_{i-1}} P_{(m_i+k_i-m_{i-1}-k_{i-1})/(N-m_{i-1}-k_{i-1})}^{k_i+l_i}(\Delta m'_{i-1} - \Delta m'_i) \right], \quad (7.83)
 \end{aligned}$$

To evaluate it, we can make use of the fact that probability $P_{i/N}^j(n)$ is only nonzero for $n \geq 0$, and that the sum only contains terms for which $\Delta m'_i \geq 0$. Thus, for some number $0 < a < 1$,

$$\begin{aligned}
 & \sum_{\Delta m'_{i-1}=0}^{\infty} a^{\Delta m'_{i-1}} P_{i/N}^j(\Delta m'_{i-1} - \Delta m'_i) \\
 &= \sum_{\Delta m'_{i-1}=\Delta m'_i}^{\infty} a^{\Delta m'_{i-1}} P_{i/N}^j(\Delta m'_{i-1} - \Delta m'_i) \\
 &= \sum_{n=0}^{\infty} a^{n+\Delta m'_i} P_{i/N}^j(n) \\
 &= \langle a^{n_{i/N}^j} \rangle a^{\Delta m'_i}. \quad (7.84)
 \end{aligned}$$

This shows that the summation over $\Delta m'_i$ cannot be resolved independently from the summation over $\Delta m'_{i-1}$. However, the summation over $\Delta m'_{i-1}$ can be safely performed before the summation over $\Delta m'_i$, as shown above. Thus, our strategy is to sum over the $\Delta m'_i$'s in the order of their index (i.e. $\Delta m'_0$ first, $\Delta m'_M$ last). For $\Delta m'_0$, we get

$$\left\langle (1-r_0)^{n_{m_1+k_1-m_0-k_0/(N-m_0-k_0)}^{k_1+l_1}} \right\rangle (1-r_0)^{\Delta m'_1}. \quad (7.85)$$

Before performing the sum over $\Delta m'_1$, we must remember to also include the $(1-r_0)^{\Delta m'_1}$ that came out of the sum over $\Delta m'_0$ and thus we get

$$\left\langle [(1-r_0)(1-r_1)]^{n_{m_2+k_2-m_1-k_1/(N-m_1-k_1)}^{k_2+l_2}} \right\rangle [(1-r_0)(1-r_1)]^{\Delta m'_2}. \quad (7.86)$$

Then, for the sum over $\Delta m'_3$, we should not forget to add the $[(1-r_0)(1-r_1)]^{\Delta m'_2}$ to the

$(1 - r_2)^{\Delta m'_2}$ already present. And so on. The result is

$$\begin{aligned}
 & G(r_1, r_2, \dots, r_M) \\
 &= \prod_{i=1}^{M+1} \left[\sum_{k_i=0}^{N-c_i} \sum_{l_i=-k_i}^{c_i-c_{i-1}-k_{i-1}} \left(\theta(l_i - 1) + \delta_{k_i, c_{i-1}+k_{i-1}-c_i} \right) \right. \\
 &\quad \times \left. \left\langle \left(\prod_{j=0}^{i-1} (1 - r_j) \right)^{n_{(c_i+k_i-c_{i-1}-k_{i-1})/(N-c_{i-1}-k_{i-1})}} \right\rangle \right] \\
 &= \prod_{i=1}^{M+1} \left[\sum_{k_i=0}^{N-c_i} \sum_{l_i=-k_i}^{c_i-c_{i-1}-k_{i-1}} \left(\theta(l_i - 1) + \delta_{k_i, c_{i-1}+k_{i-1}-c_i} \right) \right. \\
 &\quad \times \left. \left\langle (1 - \bar{r}_{i-1})^{n_{(c_i+k_i-c_{i-1}-k_{i-1})/(N-c_{i-1}-k_{i-1})}} \right\rangle \right],
 \end{aligned} \tag{7.87}$$

where we defined

$$\bar{r}_i = 1 - \prod_{j=0}^i (1 - r_j). \tag{7.88}$$

The next step is to calculate the expected values of the form encountered in the above equation. That is, we need to calculate

$$\langle (1 - r)^{n_{i/N}^j} \rangle = \sum_{n=0}^{\infty} P_{i/N}^j(n) (1 - r)^n. \tag{7.89}$$

We can use equation (7.72) to write down the recursive relation

$$\begin{aligned}
 & \langle (1 - r)^{n_{i/N}^j} \rangle \\
 &= \binom{N-i+j}{j} \frac{q_{\text{link}}^j (1 - q_{\text{link}})^{N-i}}{1 - (1 - q_{\text{link}})^{N-i+j}} \sum_{n=0}^{\infty} \sum_{n'=0}^{n-1} (1 - r)^n P_{1/(N-i+j)}(n - n') \sum_{l=0}^{i-j} P_{(i-j)/N}^l(n') \\
 &= \binom{N-i+j}{j} \frac{q_{\text{link}}^j (1 - q_{\text{link}})^{N-i}}{1 - (1 - q_{\text{link}})^{N-i+j}} \sum_{l=0}^{i-j} \sum_{\Delta n=1}^{\infty} \sum_{n'=0}^{\infty} (1 - r)^{n'+\Delta n} P_{1/(N-i+j)}(\Delta n) P_{(i-j)/N}^l(n') \\
 &= \binom{N-i+j}{j} \frac{q_{\text{link}}^j (1 - q_{\text{link}})^{N-i}}{1 - (1 - q_{\text{link}})^{N-i+j}} \langle (1 - r)^{n_{1/(N-i+j)}} \rangle \sum_{l=0}^{i-j} \langle (1 - r)^{n_{(i-j)/N}^l} \rangle.
 \end{aligned} \tag{7.90}$$

Since $n_{1/N}$ is geometric with $1/\langle n_{1/N} \rangle = 1 - (1 - q_{\text{link}})^N$, and since

$$\langle a^x \rangle = aq/(1 - a[1 - q]) \tag{7.91}$$

for any geometric variable x with $1/\langle x \rangle = q$ and $0 < a < 1$, we can write

$$\langle (1 - r)^{n_{i/N}^j} \rangle = \binom{N-i+j}{j} \frac{q_{\text{link}}^j (1 - q_{\text{link}})^{N-i} (1 - r)}{1 - (1 - r)(1 - q_{\text{link}})^{N-i+j}} \sum_{l=0}^{i-j} \langle (1 - r)^{n_{(i-j)/N}^l} \rangle. \tag{7.92}$$

for $i > 0$.

7.12.5 Recursive Relation

We will now proceed in the limit $q_{\text{link}}, r \ll 1$, since this is the regime that we are mostly interested in, and since this allows for some convenient approximations. Throwing out higher-order terms in both r and q_{link} , we get

$$\langle (1-r)^{n_{i/N}^j} \rangle \approx \binom{N-i+j}{j} \frac{q_{\text{link}}^j}{r + (N-i+j)q_{\text{link}}} \sum_{l=0}^{i-j} \langle (1-r)^{n_{(i-j)/N}^l} \rangle. \quad (7.93)$$

Now, we will argue that to leading order in q_{link} and r , we only need to consider the term for which $l = 1$, making it much easier to resolve the recurrence relation.

Let us for the moment represent $\langle (1-r)^{n_{i/N}^b} \rangle$ schematically by the tuple (a, b) . Then, any (i, j) is expressed as a sum over $(i-j, l_1)$'s, for $l_1 = 0, 1, \dots, i-j$. In turn each $(i-j, l_1)$ will be a sum over $(i-j-l_1, l_2)$'s for $l_2 = 0, 1, \dots, i-j-l_1$. Therefore, each term in the sum can be represented by a sequence

$$\text{term in sum} = ((a_0, b_0), (a_1, b_1), (a_2, b_2), \dots) \quad (7.94)$$

following the rule $a_{i+1} = a_i - b_i$ and the boundary condition $a_0 = i, b_0 = j$. Now, since

$$\langle (1-r)^{n_{i/N}^0} \rangle = \sum_{n=0}^{\infty} P_{i/N}^0(n)(1-r)^n = \sum_{n=0}^{\infty} \delta_{i,0} \delta_{n,0} (1-r)^n = \delta_{i,0}, \quad (7.95)$$

tuples of the form $(a, 0)$ can only occur in the sequence if $a = 0$. That means $b_i > 0$ for each tuple where $a_i \neq 0$. As a result, $a_{i+1} \leq a_i - 1$ unless $a_i = 0$. Furthermore, the $(0, 0)$ term itself does not contain a reference other (a, b) ; it simply has the value one. Thus, the recurrence relation terminates when $a_i = 0$ is reached.

As a consequence, we can rewrite the sequence above as

$$\text{term in sum} = ((i, j), (i-j, l_1), (i-j-l_1, l_2), \dots, (i-j-\sum_{i=1}^{K-1} l_i, l_K), (0, 0)), \quad (7.96)$$

for some $l_i > 0$ for $i = 1, 2, \dots, K$ and for some value K . This sequence can be thought of as a “path” from (i, j) to $(0, 0)$. Each path is uniquely defined by a sequence (l_1, l_2, \dots, l_K) , and each such sequence uniquely defines a path as long as it satisfies the condition

$$\sum_{i=1}^K l_i = i - j. \quad (7.97)$$

Note that as $l_i \geq 1$, this automatically imposes $K \leq i - j$. We denote the set of all sequences (l_1, l_2, \dots, l_K) that define a path from (i, j) to $(0, 0)$ by $\mathcal{L}_{i,j}$, which allows us to expand the

recurrence relation as

$$\begin{aligned}
\langle (1-r)^{n_{i/N}^j} \rangle &\approx \sum_{(l_1, \dots, l_K) \in \mathcal{L}_{i,j}} \binom{N-i+j}{j} \frac{q_{\text{link}}^j}{r + (N-i+j)q_{\text{link}}} \langle (1-r)^{n_{0/N}^0} \rangle \\
&\times \prod_{k=1}^K \binom{N-(i-j-\sum_{a=1}^{k-1} l_a) + l_k}{l_k} \frac{q_{\text{link}}^{l_k}}{r + (N-(i-j-\sum_{a=1}^{k-1} l_a) + l_k)q_{\text{link}}} \\
&= \sum_{(l_1, \dots, l_K) \in \mathcal{L}_{i,j}} \frac{q_{\text{link}}^{j+\sum_{k=1}^K l_k}}{r + (N-i+j)q_{\text{link}}} \prod_{k=1}^K \frac{1}{r + (N-(i-j-\sum_{a=1}^{k-1} l_a) + l_k)q_{\text{link}}} \quad (7.98) \\
&\times \binom{N-i+j}{j} \prod_{k=1}^K \binom{N-(i-j-\sum_{a=1}^{k-1} l_a) + l_k}{l_k} \\
&= \sum_{(l_1, \dots, l_K) \in \mathcal{L}_{i,j}} \frac{q_{\text{link}}^j}{\mathcal{O}((r+q_{\text{link}})^K)} \times \mathcal{O}(r^0 q_{\text{link}}^0).
\end{aligned}$$

For $r, q_{\text{link}} \ll 1$, this sum will be dominated by paths that have the largest K . As explained above, the maximum value that K can take is $i-j$. Furthermore, there is exactly one path that realizes this value, which is defined by $l_a = 1$ for $a = 1, 2, \dots, i-j$. When we keep only this path in the above equation, we find

$$\begin{aligned}
\langle (1-r)^{n_{i/N}^j} \rangle &\approx \binom{N-i+j}{j} \frac{q_{\text{link}}^j}{r + (N-i+j)q_{\text{link}}} \\
&\times \prod_{k=1}^{i-j} \binom{N-(i-j-(k-1)) + 1}{1} \frac{1}{r + (N-(i-j-(k-1)) + 1)q_{\text{link}}} \quad (7.99) \\
&= \binom{N-i+j}{j} \frac{q_{\text{link}}^{j-1}}{N-i+j} \prod_{k=N-i+j}^N \frac{k q_{\text{link}}}{r + k q_{\text{link}}}.
\end{aligned}$$

We must note that all of the above is only valid for $i > 0$, since the recursive relation (7.92) is not applicable for $i = 0$. In order to also incorporate equation (7.95), we write

$$\langle (1-r)^{n_{i/N}^j} \rangle \approx \left(\theta(j-1) + (r + N q_{\text{link}}) \delta_{i,0} \right) \binom{N-i+j}{j} \frac{q_{\text{link}}^{j-1}}{N-i+j} \prod_{k=N-i+j}^N \frac{k q_{\text{link}}}{r + k q_{\text{link}}}. \quad (7.100)$$

How can we interpret the dominance of terms corresponding to the “longest path”? What it means is that realizations of Protocol 7.1 for which multiple successes occur during the same round occur with suppressed probability, as shown by the fact that we only include $P_{i/N}^j$ ’s for which $j = 1$. This can also be intuitively expected: if for each quantum connection the probability of distributing a Bell state per round is very small ($q_{\text{link}} \ll 1$), there will be a large spread in the rounds during which the different Bell states are distributed. It will then be very unlikely that two Bell states are distributed during the exact same round. However, when r is large (close to 1), the quantity $(1-n)^n$ will decrease very

quickly with n . The average will then have much larger weight for small n than for large n . However, these terms with small n are exactly those that are excluded by the large spread implied by $q_{\text{link}} \ll 1$. In fact, if $r = 1 - \epsilon$ with $\epsilon \ll 1$, the only linear term in the average is the one corresponding to $n = 1$, which implies all Bell states being distributed collectively during the first round ($P_{i/N}^j$ with $j = i$). This explains why neglecting simultaneous successes requires both q_{link} and r to be small.

Finally, before we move on, we are interested to know whether equation (7.100) also holds for $r = 0$. This does not follow from the above, because the use of equation (7.91) required $0 < r < 1$. For $r = 0$, Eq. (7.89) yields

$$\left\langle (1-r)^{n_{i/N}^j} \Big|_{r=0} \right\rangle = \sum_{n=0}^{\infty} P_{i/N}^j(n). \quad (7.101)$$

Using again equation (7.72) we find

$$\begin{aligned} \left\langle (1-r)^{n_{i/N}^j} \Big|_{r=0} \right\rangle &= \binom{N-i+j}{j} \frac{q_{\text{link}}^j (1-q_{\text{link}})^{N-i}}{1-(1-q_{\text{link}})^{N-i+j}} \sum_{n=0}^{\infty} \sum_{n'=0}^{n-1} P_{1/(N-i+j)}(n-n') P'_{(i-j)/N}(n') \\ &= \binom{N-i+j}{j} \frac{q_{\text{link}}^j (1-q_{\text{link}})^{N-i}}{1-(1-q_{\text{link}})^{N-i+j}} \sum_{\Delta n=0}^{\infty} P_{1/(N-i+j)}(\Delta n) \sum_{l=0}^{i-j} \sum_{n'=0}^{\infty} P_{(i-j)/N}^l(n') \\ &= \binom{N-i+j}{j} \frac{q_{\text{link}}^j (1-q_{\text{link}})^{N-i}}{1-(1-q_{\text{link}})^{N-i+j}} \sum_{l=0}^{i-j} \left\langle (1-r)^{n_{(i-j)/N}^l} \Big|_{r=0} \right\rangle \end{aligned} \quad (7.102)$$

which is exactly recursive relation (7.92) but with $r = 0$. Because

$$\left\langle (1-r)^{n_{i/N}^0} \Big|_{r=0} \right\rangle = \delta_{i,0}, \quad (7.103)$$

the recursive relation expresses any (i, j) in terms of $(0, 0)$'s, and these are expressed the same for both $r = 0$ and $0 < r < 1$. Because both the recursive relation and the final term $(0, 0)$ can be written the same, we conclude that it does not matter whether r is set to zero before or after resolving the recursion relation. Therefore,

$$\left\langle (1-r)^{n_{i/N}^j} \Big|_{r=0} \right\rangle = \left\langle (1-r)^{n_{i/N}^j} \Big|_{0 < r < 1} \right\rangle \Big|_{r=0}. \quad (7.104)$$

Thus, equation (7.100) is valid for $0 \leq r \ll 1$. This means that we do not need to treat the r_0 that we defined to be zero before any differently from the other r_i 's when calculating $G((r_1, r_2, \dots, r_M))$, and our results are still valid if $r_i = 0$ for some $0 < i < M$.

7.12.6 Counting Orders

Now, we can in principle substitute Eq. (7.100) into Eq. (7.87). However, if we limit ourselves to leading order in q_{link} and the various r_i variables (which we denote as all being of order $\mathcal{O}(r)$), this allows us to disregard part of the summation. In this section, we count orders to find that only $l_i = 1$ and $k_i = 0$ terms contribute to G at leading order. This allows us to more easily calculate G to leading order in the next section.

First of all, note that

$$\bar{r}_i \equiv 1 - \prod_{j=0}^i (1 - r_j) = \sum_{j=0}^i r_j + \mathcal{O}(r^2). \quad (7.105)$$

Therefore, each \bar{r}_i is of order $\mathcal{O}(r)$. Furthermore, from Eq. (7.100) we see that

$$\langle (1-r)^{n_{i/N}^j} \rangle = \left(\theta(j-1) + \delta_{i,0} \mathcal{O}(r + q_{\text{link}}) \right) \mathcal{O} \left(\frac{q_{\text{link}}^j}{(r + q_{\text{link}})^{i-j+1}} \right). \quad (7.106)$$

Substituting this into equation (7.87) yields

$$\begin{aligned} & G(r_1, r_2, \dots, r_M) \\ &= \prod_{i=1}^{M+1} \left[\sum_{k_i=0}^{N-c_i} \sum_{l_i=-k_i}^{c_i-c_{i-1}-k_{i-1}} \left(\theta(l_i-1) + \delta_{k_i, c_{i-1}+k_{i-1}-c_i} \right) \right. \\ & \quad \times \left(\theta(k_i + l_i - 1) + \delta_{c_i+k_i-c_{i-1}-k_{i-1}, 0} \mathcal{O}(r + q_{\text{link}}) \right) \\ & \quad \left. \times \mathcal{O} \left(\frac{q_{\text{link}}^{c_i+k_i-c_{i-1}-k_{i-1}}}{(r + q_{\text{link}})^{c_i-c_{i-1}-k_{i-1}-l_i+1}} \right) \right] \\ &= \prod_{i=1}^{M+1} \left[\sum_{k_i=0}^{N-c_i} \sum_{l_i=-k_i}^{c_i-c_{i-1}-k_{i-1}} \left(\theta(l_i-1) + \delta_{k_i, c_{i-1}+k_{i-1}-c_i} \mathcal{O}(r + q_{\text{link}}) \right) \right. \\ & \quad \left. \times \mathcal{O} \left(\frac{q_{\text{link}}^{c_i+k_i-c_{i-1}-k_{i-1}}}{(r + q_{\text{link}})^{c_i-c_{i-1}-k_{i-1}-l_i+1}} \right) \right]. \end{aligned} \quad (7.107)$$

Here, we have used the fact that for every term in the sum, $k_i \geq 0$, and thus $\theta(l_i-1)\theta(k_i+l_i-1) = \theta(l_i-1)$. Furthermore, the delta functions are the same, and squaring it gives the same delta function again. Cross terms $\theta \times \delta$ vanish, because the only term for which the delta function does not vanish has $l_i = -k_i \leq 0$, making the step function vanish. Now, we make use of the identity

$$\prod_i^N \left(\sum_{x_i} f(x_i) \right) = \sum_{x_1} \sum_{x_2} \dots \sum_{x_N} f(x_1) f(x_2) \dots f(x_N) = \prod_i \left(\sum_{x_i} \right) \prod_i \left(f(x_i) \right) \quad (7.108)$$

to split the product in “three parts” and hence collect part of the order counting in a way

that is very convenient, giving

$$\begin{aligned}
G(r_1, r_2, \dots, r_M) &= \prod_{i=1}^{M+1} \left[\sum_{k_i=0}^{N-c_i} \right] \prod_{i=1}^{M+1} \left[\mathcal{O} \left(\left(\frac{q_{\text{link}}}{r + q_{\text{link}}} \right)^{c_i + k_i - c_{i-1} - k_{i-1}} \right) \right] \\
&\times \prod_{i=1}^{M+1} \left[\sum_{l_i = -k_i}^{c_i - c_{i-1} - k_{i-1}} \left(\theta(l_i - 1) + \delta_{k_i, c_{i-1} + k_{i-1} - c_i} \mathcal{O}(r + q_{\text{link}}) \right) \mathcal{O} \left((r + q_{\text{link}})^{l_i + k_i - 1} \right) \right] \\
&= \prod_{i=1}^{M+1} \left[\sum_{k_i=0}^{N-c_i} \right] \mathcal{O} \left(\left(\frac{q_{\text{link}}}{r + q_{\text{link}}} \right)^{\sum_{i=1}^{M+1} (c_i + k_i - c_{i-1} - k_{i-1})} \right) \\
&\times \prod_{i=1}^{M+1} \sum_{l_i = -k_i}^{c_i - c_{i-1} - k_{i-1}} \left(\theta(l_i - 1) + \delta_{k_i, c_{i-1} + k_{i-1} - c_i} \mathcal{O}(r + q_{\text{link}}) \right) \mathcal{O} \left((r + q_{\text{link}})^{l_i + k_i - 1} \right). \tag{7.109}
\end{aligned}$$

This then allows us to make use of

$$\sum_{i=1}^{M+1} (c_i + k_i - c_{i-1} - k_{i-1}) = c_{M+1} + k_{M+1} - c_0 - k_0 = N, \tag{7.110}$$

since we manually defined $m_0 = k_0 = 0$ and $m_{M+1} = N$, and since the sum over k_{M+1} only runs over $k_{M+1} = 0$ (the last success cannot “overshoot” as all Bell states are already in place). Thus, this quantity is the same for every term and can safely be taken out of the sum.

Now, working out the θ and δ parts separately, we get

$$\begin{aligned}
G(r_1, r_2, \dots, r_M) &= \mathcal{O} \left(\left(\frac{q_{\text{link}}}{r + q_{\text{link}}} \right)^N \right) \prod_{i=1}^{M+1} \left[\sum_{k_i=0}^{N-c_i} \right] \prod_{i=1}^{M+1} \left[\sum_{l_i = -k_i}^{c_i - c_{i-1} - k_{i-1}} \mathcal{O} \left((r + q_{\text{link}})^{l_i + k_i - 1} \right) + \delta_{k_i, c_{i-1} + k_{i-1} - c_i} \right]. \tag{7.111}
\end{aligned}$$

The part where we sum over l_i now is clearly dominated by the term for which l_i is lowest, since a larger l_i means a larger order in $r + q_{\text{link}}$. Since this is $l_i = 1$, we find

$$\begin{aligned}
G(r_1, r_2, \dots, r_M) &= \mathcal{O} \left(\left(\frac{q_{\text{link}}}{r + q_{\text{link}}} \right)^N \right) \prod_{i=1}^{M+1} \left[\sum_{k_i=0}^{N-c_i} \right] \prod_{i=1}^{M+1} \left[\theta(c_i - c_{i-1} - k_{i-1} - 1) \mathcal{O} \left((r + q_{\text{link}})^{k_i} \right) + \delta_{k_i, c_{i-1} + k_{i-1} - c_i} \right], \tag{7.112}
\end{aligned}$$

where the step function is due to the summation over l_i being empty and hence zero for $c_i - c_{i-1} - k_{i-1} < 1$. This quantity will be dominated by terms which are products of δ 's,

and of θ 's with $k_i = 0$, since these terms do not carry an additional $\mathcal{O}(r + q_{\text{link}})$. Now note that the Kronecker δ function $\delta_{k_i, c_{i-1} + k_{i-1} - c_i}$ enforces $k_{i-1} \geq c_i - c_{i-1} > 0$. This implies two things. Firstly, it implies that any term that contains a $\theta(c_i - c_{i-1} - k_{i-1} - 1)$ for $i = j$ but a $\delta_{k_i, c_{i-1} + k_{i-1} - c_i}$ for $i = j + 1$ will be of higher order in $r + q_{\text{link}}$. Secondly, because $k_0 = 0$ by definition, it implies that all nonzero terms of the sum must “start” with a θ , i.e. include a $\theta(c_i - c_{i-1} - k_{i-1} - 1)$ for $i = 1$. Together, these two implications mean any leading terms cannot contain a δ ; they only contain θ 's. The only leading term with only θ 's is the one for which all k_i 's are 0. Combining this with what we found for the l_i 's, we can conclude that the leading contribution to G has $l_i = 1$ and $k_i = 0$ for $i = 0, 1, 2, \dots, M + 1$. This can again be interpreted as neglecting the possibility that multiple Bell states are distributed simultaneously.

7.12.7 Calculating G

Now, we are ready to calculate G to leading order. Only keeping $l_i = 1$, $k_i = 0$ in Eq. (7.87) and then filling in Eq. (7.100), we find

$$\begin{aligned}
 G(r_1, r_2, \dots, r_M) & \approx \prod_{i=1}^{M+1} \left\langle (1 - \bar{r}_{i-1})^{n_{(c_i - c_{i-1})/(N - c_{i-1})}} \right\rangle \\
 & \approx \prod_{i=1}^{M+1} \left[\left(\theta(1 - 1) + (\bar{r}_{i-1} + N q_{\text{link}}) \delta_{c_i - c_{i-1}, 0} \right) \right. \\
 & \quad \times \binom{N - c_i + 1}{1} \frac{1}{N - c_i + 1} \prod_{k=N - c_i + 1}^{N - c_{i-1}} \frac{k q_{\text{link}}}{\bar{r}_{i-1} + k q_{\text{link}}} \left. \right] \\
 & = \prod_{i=1}^M \prod_{k=c_i+1}^{c_{i+1}} \frac{(N + 1 - k) q_{\text{link}}}{\bar{r}_i + (N + 1 - k) q_{\text{link}}} \\
 & \approx \prod_{i=1}^M \prod_{k=c_i+1}^{c_{i+1}} \frac{(N + 1 - k) q_{\text{link}}}{\sum_{j=1}^i r_j + (N + 1 - k) q_{\text{link}}}.
 \end{aligned} \tag{7.113}$$

Here, we have used the fact that $r_0 \equiv 0$ (and thus $\bar{r}_1 = 0$) to drop the lowest term in the product. This can also be rewritten as

$$G(r_1, r_2, \dots, r_M) \approx \prod_{k=1}^N \frac{(N + 1 - k) q_{\text{link}}}{\sum_{c_i < k} r_i + (N + 1 - k) q_{\text{link}}}. \tag{7.114}$$

7.12.8 Lower Bound

Apart from the leading-order approximation of the function G derived above, we can also derive a lower bound. At the core of the approximation lies the fact that, to leading order in q_{link} and r , we are able to ignore all events for which multiple Bell states are distributed during the same round. That function G obtained by ignoring these events is an average over a sub-normalized probability distribution, and thus provides a lower bound on the real function. In turn, using a lower bound of the function G to evaluate the fidelity

(Eq. (7.23)) gives a lower bound on the real fidelity. Even so, the result Eq. (7.114) is not necessarily a lower bound on the function G . The reason for this is that, in order to work consistently at leading order, we have thrown out some additional terms that are not linked to ignoring multiple simultaneous successes. Some of these terms would lower the function G if they were kept, and thus Eq. (7.114) is only a lower bound if the effect of throwing out these terms is smaller than the effect of throwing out events corresponding to multiple simultaneous successes. We do not know if this is generally the case.

In this section, we derive a lower bound by repeating the above calculation without throwing out these additional terms. That means that we are not working at leading order, but just deriving a lower bound by throwing out all contributions to G due to multiple distributed Bell states during the same round. We start by lower-bounding the expected value $\langle (1-r)^{n_{i/N}^j} \rangle$. To this end, we use the recursive relation Eq. (7.92). Because the factor in front of the summation is a positive quantity, and because each term of the sum is ultimately expressed in terms of $\langle (1-r)^{n_{i/N}^0} \rangle = 1$ (see Eq. (7.95)), we can conclude that

$$\langle (1-r)^{n_{i/N}^j} \rangle \geq 0. \quad (7.115)$$

Because of this, Eq. (7.92) tells us

$$\langle (1-r)^{n_{i/N}^j} \rangle \geq \binom{N-i+j}{j} \frac{q_{\text{link}}^j (1-q_{\text{link}})^{N-i} (1-r)}{1-(1-r)(1-q_{\text{link}})^{N-i+j}} \langle (1-r)^{n_{(i-j)/N}^1} \rangle. \quad (7.116)$$

This inequality can be applied recursively until reaching

$$\langle (1-r)^{n_{i/N}^1} \rangle = \frac{1}{N} \frac{q_{\text{link}} (1-q_{\text{link}})^{N-1} (1-r)}{1-(1-r)(1-q_{\text{link}})^N}. \quad (7.117)$$

This is exactly the “leading order path” discussed in Section 7.12.5 and yields, in analogue to Eq. (7.99),

$$\begin{aligned} \langle (1-r)^{n_{i/N}^j} \rangle &\geq \binom{N-i+j}{j} \frac{q_{\text{link}}^j (1-q_{\text{link}})^{N-i} (1-r)}{1-(1-r)(1-q_{\text{link}})^{N-i+j}} \\ &\quad \times \prod_{k=1}^{i-j} \binom{N-i+j+k}{1} \frac{q_{\text{link}} (1-q_{\text{link}})^{N-i+j+k-1} (1-r)}{1-(1-r)(1-q_{\text{link}})^{N-i+j+k}}. \end{aligned} \quad (7.118)$$

We will now focus on the case $j = 1$, since this will ultimately be the only type of term occurring in the lower bound for G (after all, $j > 1$ would correspond to distributing multiple Bell states during the same round). We then find

$$\begin{aligned} \langle (1-r)^{n_{i/N}^1} \rangle &\geq \prod_{k=0}^{i-1} (N-i+k+1) \frac{q_{\text{link}} (1-q_{\text{link}})^{N-i+k} (1-r)}{1-(1-r)(1-q_{\text{link}})^{N-i+k+1}} \\ &= \prod_{k=N-i+1}^N \frac{k q_{\text{link}} (1-q_{\text{link}})^{k-1} (1-r)}{1-(1-r)(1-q_{\text{link}})^k}. \end{aligned} \quad (7.119)$$

Now, we can use Eq. (7.119) in combination with Eq. (7.87) to bound G . Because all terms in the sum of Eq. (7.87) are positive, we can write (analogously to Eq. (7.113))

$$\begin{aligned}
 G(r_1, r_2, \dots, r_M) &\geq \prod_{i=1}^{M+1} \left\langle (1 - \bar{r}_{i-1})^{n_{(c_i - c_{i-1})/(N - c_{i-1})}} \right\rangle \\
 &\geq \prod_{i=1}^{M+1} \prod_{k=N - c_i + 1}^{N - c_{i-1}} \frac{k q_{\text{link}} (1 - q_{\text{link}})^{k-1} (1 - \bar{r}_{i-1})}{1 - (1 - \bar{r}_{i-1})(1 - q_{\text{link}})^k} \\
 &= \prod_{i=0}^M \prod_{k=c_i + 1}^{c_{i+1}} \frac{(N + 1 - k) q_{\text{link}} (1 - q_{\text{link}})^{N-k} (1 - \bar{r}_i)}{1 - (1 - \bar{r}_i)(1 - q_{\text{link}})^{N+1-k}}.
 \end{aligned} \tag{7.120}$$

This can be rewritten as

$$G(r_1, r_2, \dots, r_M) \geq \prod_{k=1}^M \frac{(N + 1 - k) q_{\text{link}} (1 - q_{\text{link}})^{N-k} \prod_{c_i < k} (1 - r_i)}{1 - (1 - q_{\text{link}})^{N+1-k} \prod_{c_i < k} (1 - r_i)}. \tag{7.121}$$

7.13 Expected Value of Distribution Time

In this section, we use the tools developed in Section 7.12 to prove the equation

$$\langle n_{i/N} \rangle \approx \frac{1}{q_{\text{link}}} \sum_{k=N+1-i}^N \frac{1}{k} \tag{7.122}$$

is true up to leading order in q_{link} . Here, $n_{i/N}$ is the number of rounds required to distribute i Bell states over N quantum connections. That is, it is the i^{th} largest value out of $\{n_1, n_2, \dots, n_N\}$, where we remind the reader that each n_j is a geometrically-distributed random variable with mean $\frac{1}{q_{\text{link}}}$. Additionally, we provide the upper bound

$$\langle n_{i/N} \rangle \leq \sum_{k=N+1-i}^N \frac{1}{1 - (1 - q_{\text{link}})^k}. \tag{7.123}$$

We note that it directly follows from Eq. (7.122) that

$$\langle n_{N/N} \rangle \equiv \langle n_{\text{all}} \rangle \equiv \langle \max\{n_1, n_2, \dots, n_N\} \rangle \approx \frac{H_N}{q_{\text{link}}}, \tag{7.124}$$

where H_N is the N^{th} harmonic number, is valid up to leading order in q_{link} . This is a well-known result [10, 51, 52]. Additionally, Eq. (7.123) can be used to upper bound $\langle n_{N/N} \rangle$. However, the bound is less tight than the existing bound given in Eq. (7.15).

We now explain the intuition behind Eq. (7.122). If $k > 1$ connections try to establish entanglement, the first success will occur sooner than when only one connection is trying. For one connection, the time it takes is on average $\frac{1}{q_{\text{link}}}$ (this is the expected value of the geometric distribution). But when there are k connections trying, there is a “boost factor”; entanglement is generated exactly k times faster, and therefore the time required is on

average only $\frac{1}{kq_{\text{link}}}$. In the limit $q_{\text{link}} \rightarrow 0$, it is very unlikely that multiple Bell states are distributed during the same round, and therefore one can repeatedly use this argument to go from success to success. The rest of this section is dedicated to proving Eq. (7.122), thereby making the intuitive argument exact.

7.13.1 Exact Recursion Relation

The random variable $n_{i/N}$ follows the probability distribution $P_{i/N}$ defined in Eq. (7.61). Key to deriving Eq. (7.122), is to determine the difference between $\langle n_{(i+1)/N} \rangle$ and $\langle n_{i/N} \rangle$, as it allows us to write a recursion relation. To this end, we first take the difference between their probability distributions. Using Eq. (7.66) yields

$$\begin{aligned} P_{(i+1)/N} - P_{i/N} &= \sum_{k=0}^{N-i-1} \sum_{l=1}^{i+1} P_{(k+i+1)/N}^{k+l} - \sum_{k=0}^{N-i} \sum_{l=1}^i P_{(k+i)/N}^{k+l} \\ &= \sum_{k=1}^{N-i} P_{(k+i)/N}^k - \sum_{l=1}^i P_{i/N}^l \\ &= \sum_{k=1}^{N-i} P_{(k+i)/N}^k - P'_{i/N}. \end{aligned} \quad (7.125)$$

From linearity of the average, it then follows directly that

$$\langle n_{(i+1)/N} \rangle - \langle n_{i/N} \rangle = \sum_{k=1}^{N-i} \langle n_{(k+i)/N}^k \rangle - \langle n'_{i/N} \rangle. \quad (7.126)$$

To evaluate Eq. (7.126), we first give an expression for $\langle n_{(k+i)/N}^k \rangle$. We use Eq. (7.72) to write

$$\langle n_{i/N}^j \rangle = \binom{N-i+j}{j} \frac{q_{\text{link}}^j (1-q_{\text{link}})^{N-i}}{1-(1-q_{\text{link}})^{N-i+j}} \sum_{n=1}^{\infty} \sum_{n'=0}^{n-1} n P_{1/(N-i+j)}(n-n') P'_{(i-j)/N}(n'). \quad (7.127)$$

This can be calculated by making the change of variables $n = n' + \Delta n$ and using the fact that $P_{1/(N-i+j)}(n)$ is a normalized probability distribution, giving

$$\begin{aligned} \langle n_{i/N}^j \rangle &= \binom{N-i+j}{j} \frac{q_{\text{link}}^j (1-q_{\text{link}})^{N-i}}{1-(1-q_{\text{link}})^{N-i+j}} \sum_{n'=0}^{\infty} \sum_{\Delta n=1}^{\infty} (n' + \Delta n) P_{1/(N-i+j)}(\Delta n) P'_{(i-j)/N}(n') \\ &= \binom{N-i+j}{j} \frac{q_{\text{link}}^j (1-q_{\text{link}})^{N-i}}{1-(1-q_{\text{link}})^{N-i+j}} \left(\langle n_{1/(N-i+j)} \rangle T_{(i-j)/N} + \langle n'_{(i-j)/N} \rangle \right). \end{aligned} \quad (7.128)$$

Here, we have defined

$$T_{i/N} \equiv \sum_{n=0}^{\infty} P'_{i/N}(n), \quad (7.129)$$

which is the total probability mass of the sub-normalized probability distribution $P'_{i/N}$ (and therefore always smaller than one). Then, resolving the summation in Eq. (7.126) yields

$$\sum_{k=1}^{N-i} \langle n_{(k+1)/N}^k \rangle = \left(\langle n_{1/(N-i)} \rangle T_{i/N} + \langle n'_{i/N} \rangle \right) \sum_{k=1}^{N-i} \binom{N-i}{k} \frac{q_{\text{link}}^k (1 - q_{\text{link}})^{N-i-k}}{1 - (1 - q_{\text{link}})^{N-i}}. \quad (7.130)$$

To deal with the final summation, we use the binomial theorem to write

$$\sum_{k=0}^{N-i} \binom{N-i}{k} q_{\text{link}}^k (1 - q_{\text{link}})^{N-i-k} = \left(q_{\text{link}} + (1 - q_{\text{link}}) \right)^{N-i} = 1. \quad (7.131)$$

Therefore,

$$\sum_{k=1}^{N-i} \binom{N-i}{k} q_{\text{link}}^k (1 - q_{\text{link}})^{N-i-k} = 1 - q_{\text{link}}^0 (1 - q_{\text{link}})^{N-i-0} = 1 - (1 - q_{\text{link}})^{N-i} \quad (7.132)$$

(note that the lower limit of the summation is one here as opposed to zero). From this, we conclude conveniently that

$$\sum_{k=1}^{N-i} \binom{N-i}{k} \frac{q_{\text{link}}^k (1 - q_{\text{link}})^{N-i-k}}{1 - (1 - q_{\text{link}})^{N-i}} = 1. \quad (7.133)$$

This brings Eq. (7.126) into the form

$$\langle n_{(i+1)/N} \rangle - \langle n_{i/N} \rangle = \langle n_{1/(N-i)} \rangle T_{i/N}. \quad (7.134)$$

This recursive relation can be written down in a closed form, as long as we leave the $T_{i/N}$ explicit. We then find

$$\langle n_{i/N} \rangle = \langle n_{1/N} \rangle + \sum_{k=1}^{i-1} T_{k/N} \langle n_{1/(N-k)} \rangle. \quad (7.135)$$

It was remarked in Section 7.12.2 that $\langle n_{1/N} \rangle$ is geometrically distributed with $1/\langle n_{1/N} \rangle = 1 - (1 - q_{\text{link}})^N$. Therefore, we can also write this result at

$$\langle n_{i/N} \rangle = \frac{1}{1 - (1 - q_{\text{link}})^N} + \sum_{k=1}^{i-1} \frac{T_{k/N}}{1 - (1 - q_{\text{link}})^{N-k}}. \quad (7.136)$$

7.13.2 Upper Bound

Now, we use Eq. (7.136) to derive an upper bound on $\langle n_{i/N} \rangle$. Because $T_{i/N}$ is the total probability mass of a sub-normalized probability function, we have $T_{i/N} \leq 1$. From this, it follows directly that Eq. (7.123) is true.

7.13.3 Leading Order

Finally, we use Eq. (7.136) to show that Eq. (7.122) is valid up to leading order in q_{link} . Because, to leading order,

$$\frac{1}{1 - (1 - q_{\text{link}})^N} \approx \frac{1}{N q_{\text{link}}}, \quad (7.137)$$

to leading order we can write Eq. (7.136) as

$$\langle n_{i/N} \rangle \approx \frac{1}{q_{\text{link}}} \left(\frac{1}{N} + \sum_{k=1}^{i-1} \frac{T_{k/N}}{N-k} \right). \quad (7.138)$$

This exactly reduces to Eq. (7.122) if we can show that $T_{k/N} \approx 1$ to leading order in q_{link} .

To calculate $T_{i/N}$, we use yet another recursion relation. First, using Eq. (7.65), we can write (for $i \geq 1$)

$$T_{i/N} = \sum_{l=1}^i \sum_{n=1}^{\infty} P_{i/N}^l(n). \quad (7.139)$$

Then, using Eq. (7.72), making once more the change in variables $n \rightarrow n' + \Delta n$, and making use of the normalization of $P_{1/N}(n)$,

$$\begin{aligned} T_{i/N} &= \sum_{l=1}^i \binom{N-i+l}{l} \frac{q_{\text{link}}^l (1-q_{\text{link}})^{N-i}}{1-(1-q_{\text{link}})^{N-i+l}} \sum_{n=1}^{\infty} \sum_{n'=0}^{\infty} P_{1/(N-i+l)}(n-n') P'_{(i-l)/N}(n') \\ &= \sum_{l=1}^i \binom{N-i+l}{l} \frac{q_{\text{link}}^l (1-q_{\text{link}})^{N-i}}{1-(1-q_{\text{link}})^{N-i+l}} \sum_{\Delta n=1}^{\infty} P_{1/(N-i+l)}(\Delta n) \sum_{n'=0}^{\infty} P'_{(i-l)/N}(n') \\ &= \sum_{l=1}^i \binom{N-i+l}{l} \frac{q_{\text{link}}^l (1-q_{\text{link}})^{N-i}}{1-(1-q_{\text{link}})^{N-i+l}} T_{(i-l)/N}. \end{aligned} \quad (7.140)$$

7

This recursion relation can be completely resolved if $T_{0/N}$ is known. From the definition of $P'_{0/N}$ (Eq. (7.69)), we have

$$T_{0/N} = \sum_{n=0}^{\infty} \delta_{n,0} = 1. \quad (7.141)$$

Now we will resolve the recursion relation to leading order in q_{link} . We note that

$$\frac{(1-q_{\text{link}})^{N-i}}{1-(1-q_{\text{link}})^{N-i+l}} = \frac{1}{(N-i+l)q_{\text{link}}} + \mathcal{O}(q_{\text{link}}^0), \quad (7.142)$$

and therefore

$$T_{i/N} = \left(1 + \mathcal{O}(q_{\text{link}})\right) T_{(i-1)/N} + \sum_{l=2}^i \mathcal{O}(q_{\text{link}}) T_{(i-l)/N}. \quad (7.143)$$

Thus,

$$T_{i/N} \approx T_{(i-1)/N} \quad (7.144)$$

to leading order. This holds for every $i \geq 1$ until we hit $T_{0/N} = 1$. Therefore,

$$T_{i/N} \approx 1 \quad (7.145)$$

up to leading order in q_{link} . This is exactly what we needed to show, and therefore we can conclude that Eq. (7.122) is indeed valid up to leading order in q_{link} .

References

- [1] R. V. Meter, J. Touch, and C. Horsman, *Recursive quantum repeater networks*, Progress in Informatics , 65 (2011).
- [2] J. Wallnöfer, M. Zwerger, C. Muschik, N. Sangouard, and W. Dür, *Two-dimensional quantum repeaters*, Physical Review A **94**, 052307 (2016).
- [3] A. Pirker, J. Wallnöfer, and W. Dür, *Modular architectures for quantum networks*, New Journal of Physics **20**, 053054 (2018).
- [4] V. Caprara Vivoli, J. Ribeiro, and S. Wehner, *High-fidelity Greenberger-Horne-Zeilinger state generation within nearby nodes*, Physical Review A **100**, 032310 (2019).
- [5] A. Pirker and W. Dür, *A quantum network stack and protocols for reliable entanglement-based networks*, New Journal of Physics **21**, 033003 (2019).
- [6] S. C. Benjamin, D. E. Browne, J. Fitzsimons, and J. J. L. Morton, *Brokered graph-state quantum computation*, New Journal of Physics **8**, 141 (2006).
- [7] E. T. Campbell, J. Fitzsimons, S. C. Benjamin, and P. Kok, *Adaptive strategies for graph-state growth in the presence of monitored errors*, Physical Review A **75**, 042303 (2007).
- [8] C. Kruszynska, S. Anders, W. Dür, and H. J. Briegel, *Quantum communication cost of preparing multipartite entanglement*, Physical Review A **73**, 062328 (2006).
- [9] S. de Bone, R. Ouyang, K. Goodenough, and D. Elkouss, *Protocols for Creating and Distilling Multipartite GHZ States With Bell Pairs*, IEEE Transactions on Quantum Engineering **1**, 1 (2020).
- [10] T. Coopmans, S. Brand, and D. Elkouss, *Improved analytical bounds on delivery times of long-distance entanglement*, Physical Review A **105**, 012608 (2022).
- [11] T. Coopmans, R. Knegjens, A. Dahlberg, D. Maier, L. Nijsten, J. de Oliveira Filho, M. Papendrecht, J. Rabbie, F. Rozpędek, M. Skrzypczyk, L. Wubben, W. de Jong, D. Podareanu, A. Torres-Knoop, D. Elkouss, and S. Wehner, *NetSquid, a NETwork Simulator for QUantum Information using Discrete events*, Communications Physics **4**, 1 (2021).
- [12] P. Nain, G. Vardoyan, S. Guha, and D. Towsley, *On the Analysis of a Multipartite Entanglement Distribution Switch*, Proceedings of the ACM on Measurement and Analysis of Computing Systems **4**, 23:1 (2020).
- [13] P. Nain, G. Vardoyan, S. Guha, and D. Towsley, *Analysis of a tripartite entanglement distribution switch*, Queueing Systems: Theory and Applications **101**, 291 (2022).
- [14] G. Vardoyan, S. Guha, P. Nain, and D. Towsley, *On the Capacity Region of Bipartite and Tripartite Entanglement Switching*, ACM SIGMETRICS Performance Evaluation Review **48**, 45 (2021).

- [15] G. Vardoyan, S. Guha, P. Nain, and D. Towsley, *On the Stochastic Analysis of a Quantum Entanglement Distribution Switch*, IEEE Transactions on Quantum Engineering **2**, 1 (2021).
- [16] M. Cuquet and J. Calsamiglia, *Growth of graph states in quantum networks*, Physical Review A **86**, 042304 (2012).
- [17] M. Epping, H. Kampermann, and D. Bruß, *Large-scale quantum networks based on graphs*, New Journal of Physics **18**, 053036 (2016).
- [18] A. Dahlberg and S. Wehner, *Transforming graph states using single-qubit operations*, Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences **376**, 20170325 (2018).
- [19] H. Yamasaki, A. Pirker, M. Murao, W. Dür, and B. Kraus, *Multipartite entanglement outperforming bipartite entanglement under limited quantum system sizes*, Physical Review A **98**, 052313 (2018).
- [20] C. Meignant, D. Markham, and F. Grosshans, *Distributing graph states over arbitrary quantum networks*, Physical Review A **100**, 052333 (2019).
- [21] L. Bugalho, B. C. Coutinho, F. A. Monteiro, and Y. Omar, *Distributing Multipartite Entanglement over Noisy Quantum Networks*, Quantum **7**, 920 (2023).
- [22] A. Fischer and D. Towsley, *Distributing Graph States Across Quantum Networks*, in *2021 IEEE International Conference on Quantum Computing and Engineering (QCE)* (2021) pp. 324–333.
- [23] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, Physical Review Letters **70**, 1895 (1993).
- [24] G. Vardoyan, S. Guha, P. Nain, and D. Towsley, *On the exact analysis of an idealized quantum switch*, Performance Evaluation **144**, 102141 (2020).
- [25] H.-F. Wang, X.-Q. Shao, Y.-F. Zhao, S. Zhang, and K.-H. Yeon, *Schemes for the generation of multipartite entanglement of remote atoms trapped in separate optical cavities*, Journal of Physics B: Atomic, Molecular and Optical Physics **42**, 175506 (2009).
- [26] F. Grasselli, H. Kampermann, and D. Bruß, *Conference key agreement with single-photon interference*, New Journal of Physics **21**, 123002 (2019).
- [27] N. Kalb, *Diamond-based quantum networks with multi-qubit nodes*, (2018), 10.4233/uuid:249753ae-9000-446a-9375-63c1e1165cc1.
- [28] C. Cabillo, J. I. Cirac, P. García-Fernández, and P. Zoller, *Creation of entangled states of distant atoms by interference*, Physical Review A **59**, 1025 (1999).
- [29] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, *Inside Quantum Repeaters*, IEEE Journal of Selected Topics in Quantum Electronics **21**, 78 (2015).

- [30] J. Calsamiglia and N. Lütkenhaus, *Maximum efficiency of a linear-optical Bell-state analyzer*, Applied Physics B **72**, 67 (2001).
- [31] W. P. Grice, *Arbitrarily complete Bell-state measurement using only linear optical elements*, Physical Review A **84**, 042331 (2011).
- [32] G. W. Lin, X. B. Zou, X. M. Lin, and G. C. Guo, *Heralded quantum memory for single-photon polarization qubits*, EPL (Europhysics Letters) **86**, 30006 (2009).
- [33] S. Langenfeld, S. Welte, L. Hartung, S. Daiss, P. Thomas, O. Morin, E. Distante, and G. Rempe, *Quantum Teleportation between Remote Qubit Memories with Only a Single Photon as a Resource*, Phys. Rev. Lett. **126**, 130502 (2021), 2105.04338 .
- [34] S. D. Barrett and P. Kok, *Efficient high-fidelity quantum computation using matter qubits and linear optics*, Physical Review A **71**, 060310(R) (2005).
- [35] H. Bernien, B. Hensen, W. Pfaff, G. Koolstra, M. S. Blok, L. Robledo, T. H. Taminiau, M. Markham, D. J. Twitchen, L. Childress, and R. Hanson, *Heralded entanglement between solid-state qubits separated by three metres*, Nature **497**, 86 (2013).
- [36] P. C. Humphreys, N. Kalb, J. P. J. Morits, R. N. Schouten, R. F. L. Vermeulen, D. J. Twitchen, M. Markham, and R. Hanson, *Deterministic delivery of remote entanglement on a quantum network*, Nature **558**, 268 (2018), 1712.07567 .
- [37] N. Kalb, A. A. Reiserer, P. C. Humphreys, J. J. W. Bakermans, S. J. Kamerling, N. H. Nickerson, S. C. Benjamin, D. J. Twitchen, M. Markham, and R. Hanson, *Entanglement Distillation between Solid-State Quantum Network Nodes*, Science **356**, 928 (2017).
- [38] M. Pompili, S. L. N. Hermans, S. Baier, H. K. C. Beukers, P. C. Humphreys, R. N. Schouten, R. F. L. Vermeulen, M. J. Tiggelman, L. dos Santos Martins, B. Dirkse, S. Wehner, and R. Hanson, *Realization of a multinode quantum network of remote solid-state qubits*, Science **372**, 259 (2021).
- [39] L. Slodička, G. Hétet, N. Röck, P. Schindler, M. Hennrich, and R. Blatt, *Atom-Atom Entanglement by Single-Photon Detection*, Physical Review Letters **110**, 083603 (2013).
- [40] L. J. Stephenson, D. P. Nadlinger, B. C. Nichol, S. An, P. Drmota, T. G. Ballance, K. Thirumalai, J. F. Goodwin, D. M. Lucas, and C. J. Ballance, *High-Rate, High-Fidelity Entanglement of Qubits Across an Elementary Quantum Network*, Physical Review Letters **124**, 110501 (2020).
- [41] J. Yin, Y.-H. Li, S.-K. Liao, M. Yang, Y. Cao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, S.-L. Li, R. Shu, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, X.-B. Wang, F. Xu, J.-Y. Wang, C.-Z. Peng, A. K. Ekert, and J.-W. Pan, *Entanglement-based secure quantum cryptography over 1,120 kilometres*, Nature , 1 (2020).

- [42] Y. Yu, F. Ma, X.-Y. Luo, B. Jing, P.-F. Sun, R.-Z. Fang, C.-W. Yang, H. Liu, M.-Y. Zheng, X.-P. Xie, W.-J. Zhang, L.-X. You, Z. Wang, T.-Y. Chen, Q. Zhang, X.-H. Bao, and J.-W. Pan, *Entanglement of two quantum memories via fibres over dozens of kilometres*, Nature **578**, 240 (2020).
- [43] S. Zippilli, G. A. Olivares-Rentería, G. Morigi, C. Schuck, F. Rohde, and J. Eschner, *Entanglement of distant atoms by projective measurement: The role of detection efficiency*, New Journal of Physics **10**, 103003 (2008).
- [44] T. E. Northup and R. Blatt, *Quantum information transfer using photons*, Nature Photonics **8**, 356 (2014).
- [45] N. Sinclair, E. Saglamyurek, H. Mallahzadeh, J. A. Slater, M. George, R. Ricken, M. P. Hedges, D. Oblak, C. Simon, W. Sohler, and W. Tittel, *Spectral Multiplexing for Scalable Quantum Photonics using an Atomic Frequency Comb Quantum Memory and Feed-Forward Control*, Physical Review Letters **113**, 053603 (2014).
- [46] S. Guha, H. Krovi, C. A. Fuchs, Z. Dutton, J. A. Slater, C. Simon, and W. Tittel, *Rate-loss analysis of an efficient quantum repeater architecture*, Physical Review A **92**, 022357 (2015).
- [47] W. Pfaff, B. Hensen, H. Bernien, S. B. van Dam, M. S. Blok, T. H. Taminiau, M. J. Tiggelman, R. N. Schouten, M. Markham, D. J. Twitchen, and R. Hanson, *Unconditional quantum teleportation between distant solid-state qubits*, Science **345**, 532 (2014).
- [48] M. Pompili, C. D. Donne, I. te Raa, B. van der Vecht, M. Skrzypczyk, G. Ferreira, L. de Kluijver, A. J. Stolk, S. L. N. Hermans, P. Pawełczak, W. Kozłowski, R. Hanson, and S. Wehner, *Experimental demonstration of entanglement delivery using a quantum network stack*, npj Quantum Information **8**, 121 (2022), 2111.11332 .
- [49] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, tenth ed. (Cambridge University Press, USA, 2011).
- [50] N. K. Bernardes, L. Praxmeyer, and P. van Loock, *Rate analysis for a hybrid quantum repeater*, Physical Review A **83**, 012323 (2011).
- [51] E. Shchukin, F. Schmidt, and P. van Loock, *Waiting time in quantum repeaters with probabilistic entanglement swapping*, Physical Review A **100**, 032322 (2019).
- [52] F. Schmidt and P. van Loock, *Memory-assisted long-distance phase-matching quantum key distribution*, Physical Review A **102**, 042614 (2020).
- [53] B. Eisenberg, *On the expectation of the maximum of IID geometric random variables*, Statistics & Probability Letters **78**, 135 (2008).
- [54] G. Avis, *NetSquid-Factory*, <https://gitlab.com/softwarequtech/netsquid-snippets/netsquid-factory> (2022).
- [55] *NetSquid-Magic*, <https://gitlab.com/softwarequtech/netsquid-snippets/netsquid-magic> (2022).

- [56] *NetSquid-NetConf*, <https://gitlab.com/softwarequtech/netsquid-snippets/netsquid-netconf> (2022).
- [57] S. Haroche and J.-M. Raimond, *Exploring the Quantum: Atoms, Cavities and Photons*, Oxford Graduate Texts (Oxford Univ. Press, Oxford, 2006).
- [58] P. Wang, C.-Y. Luan, M. Qiao, M. Um, J. Zhang, Y. Wang, X. Yuan, M. Gu, J. Zhang, and K. Kim, *Single ion qubit with estimated coherence time exceeding one hour*, *Nature Communications* **12**, 233 (2021).
- [59] A. Bermudez, X. Xu, R. Nigmatullin, J. O’Gorman, V. Negnevitsky, P. Schindler, T. Monz, U. G. Poschinger, C. Hempel, J. Home, F. Schmidt-Kaler, M. Biercuk, R. Blatt, S. Benjamin, and M. Müller, *Assessing the Progress of Trapped-Ion Processors Towards Fault-Tolerant Quantum Computation*, *Physical Review X* **7**, 041061 (2017).
- [60] C. D. Bruzewicz, J. Chiaverini, R. McConnell, and J. M. Sage, *Trapped-Ion Quantum Computing: Progress and Challenges*, *Applied Physics Reviews* **6**, 021314 (2019).
- [61] T. P. Harty, D. T. C. Allcock, C. J. Ballance, L. Guidoni, H. A. Janacek, N. M. Linke, D. N. Stacey, and D. M. Lucas, *High-Fidelity Preparation, Gates, Memory, and Readout of a Trapped-Ion Quantum Bit*, *Physical Review Letters* **113**, 220501 (2014).
- [62] C. F. Roos, M. Chwalla, K. Kim, M. Riebe, and R. Blatt, ‘*Designer atoms*’ for quantum metrology, *Nature* **443**, 316 (2006).
- [63] A. H. Myerson, D. J. Szwer, S. C. Webster, D. T. C. Allcock, M. J. Curtis, G. Imreh, J. A. Sherman, D. N. Stacey, A. M. Steane, and D. M. Lucas, *High-Fidelity Readout of Trapped-Ion Qubits*, *Physical Review Letters* **100**, 200502 (2008).
- [64] B. Vogell, B. Vermersch, T. E. Northup, B. P. Lanyon, and C. A. Muschik, *Deterministic quantum state transfer between remote qubits in cavities*, *Quantum Science and Technology* **2**, 045003 (2017).
- [65] V. Krutyanskiy, M. Meraner, J. Schupp, V. Krcmarsky, H. Hainzer, and B. P. Lanyon, *Light-matter entanglement over 50 km of optical fibre*, *npj Quantum Information* **5**, 1 (2019).
- [66] A. Borne, T. E. Northup, R. Blatt, and B. Dayan, *Efficient ion-photon qubit SWAP gate in realistic ion cavity-QED systems without strong coupling*, *Optics Express* **28**, 11822 (2020).
- [67] M. Meraner, A. Mazloom, V. Krutyanskiy, V. Krcmarsky, J. Schupp, D. A. Fioretto, P. Sekatski, T. E. Northup, N. Sangouard, and B. P. Lanyon, *Indistinguishable photons from a trapped-ion quantum network node*, *Physical Review A* **102**, 052614 (2020).
- [68] J. Schupp, V. Krcmarsky, V. Krutyanskiy, M. Meraner, T. E. Northup, and B. P. Lanyon, *Interface between Trapped-Ion Qubits and Traveling Photons with Close-to-Optimal Efficiency*, *PRX Quantum* **2**, 020331 (2021).

- [69] S. C. Connell, J. Scarabel, E. M. Bridge, K. Shimizu, V. Blums, M. Ghadimi, M. Lobino, and E. W. Streed, *Ion-Photonic Frequency Qubit Correlations for Quantum Networks*, Journal of Physics B: Atomic, Molecular and Optical Physics **54**, 175503 (2021), 2104.05189 [physics, physics:quant-ph] .
- [70] T. Walker, S. V. Kashanian, T. Ward, and M. Keller, *Improving the indistinguishability of single photons from an ion-cavity system*, Physical Review A **102**, 032616 (2020).
- [71] D. L. Moehring, P. Maunz, S. Olmschenk, K. C. Younge, D. N. Matsukevich, L.-M. Duan, and C. Monroe, *Entanglement of single-atom quantum bits at a distance*, Nature **449**, 68 (2007).
- [72] A. Sørensen and K. Mølmer, *Entanglement and quantum computation with ions in thermal motion*, Physical Review A **62**, 022311 (2000).
- [73] P. Schindler, D. Nigg, T. Monz, J. T. Barreiro, E. Martinez, S. X. Wang, S. Quint, M. F. Brandl, V. Nebendahl, C. F. Roos, M. Chwalla, M. Hennrich, and R. Blatt, *A quantum information processor with trapped ions*, New Journal of Physics **15**, 123012 (2013).
- [74] D. Kielpinski, C. Monroe, and D. J. Wineland, *Architecture for a large-scale ion-trap quantum computer*, Nature **417**, 709 (2002).
- [75] N. Sangouard, R. Dubessy, and C. Simon, *Quantum repeaters based on single trapped ions*, Physical Review A **79**, 042340 (2009).
- [76] C. Monroe and J. Kim, *Scaling the Ion Trap Quantum Processor*, Science **339**, 1164 (2013).
- [77] A. D. Pfister, M. Salz, M. Hettrich, U. G. Poschinger, and F. Schmidt-Kaler, *A quantum repeater node with trapped ions: A realistic case example*, Applied Physics B **122**, 89 (2016).
- [78] J. M. Pino, J. M. Dreiling, C. Figgatt, J. P. Gaebler, S. A. Moses, M. S. Allman, C. H. Baldwin, M. Foss-Feig, D. Hayes, K. Mayer, C. Ryan-Anderson, and B. Neyenhuis, *Demonstration of the trapped-ion quantum CCD computer architecture*, Nature **592**, 209 (2021).
- [79] M. Lee, J. Jeong, Y. Park, C. Jung, T. Kim, and D.-i. Cho, *Ion shuttling method for long-range shuttling of trapped ions in MEMS-fabricated ion traps*, Japanese Journal of Applied Physics **60**, 027004 (2021).
- [80] V. Kaushal, B. Lekitsch, A. Stahl, J. Hilder, D. Pijn, C. Schmiegelow, A. Bermudez, M. Müller, F. Schmidt-Kaler, and U. Poschinger, *Shuttling-based trapped-ion quantum information processing*, AVS Quantum Science **2**, 014101 (2020).
- [81] S. Santra, S. Muralidharan, M. Lichtman, L. Jiang, C. Monroe, and V. S. Malinovsky, *Quantum repeaters based on two species trapped ions*, New Journal of Physics **21**, 073002 (2019).
- [82] P. Dhara, N. M. Linke, E. Waks, S. Guha, and K. P. Seshadreesan, *Multiplexed quantum repeaters based on dual-species trapped-ion systems*, Physical Review A **105**, 022623 (2022).

- [83] M. Ruf, M. J. Weaver, S. B. van Dam, and R. Hanson, *Resonant Excitation and Purcell Enhancement of Coherent Nitrogen-Vacancy Centers Coupled to a Fabry-Perot Microcavity*, *Physical Review Applied* **15**, 024049 (2021).
- [84] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenbergh, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, *Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres*, *Nature* **526**, 682 (2015).
- [85] F. Rozpędek, R. Yehia, K. Goodenough, M. Ruf, P. C. Humphreys, R. Hanson, S. Wehner, and D. Elkouss, *Near-term quantum-repeater experiments with nitrogen-vacancy centers: Overcoming the limitations of direct transmission*, *Physical Review A* **99**, 052330 (2019).
- [86] S. B. van Dam, P. C. Humphreys, F. Rozpędek, S. Wehner, and R. Hanson, *Multiplexed entanglement generation over quantum networks using multi-qubit nodes*, *Quantum Science and Technology* **2**, 034002 (2017).
- [87] S. B. van Dam, J. Cramer, T. H. Taminiau, and R. Hanson, *Multipartite entanglement generation and contextuality tests using non-destructive three-qubit parity measurements*, *Physical Review Letters* **123**, 050401 (2019).
- [88] N. Kalb, P. C. Humphreys, J. J. Slim, and R. Hanson, *Dephasing mechanisms of diamond-based nuclear-spin memories for quantum networks*, *Physical Review A* **97**, 062330 (2018).
- [89] B. Li, T. Coopmans, and D. Elkouss, *Efficient Optimization of Cutoffs in Quantum Repeater Chains*, *IEEE Transactions on Quantum Engineering* **2**, 1 (2021).
- [90] S. Santra, L. Jiang, and V. S. Malinovsky, *Quantum repeater architecture with hierarchically optimized memory buffer times*, *Quantum Science and Technology* **4**, 025010 (2019).
- [91] W. Kozłowski, A. Dahlberg, and S. Wehner, *Designing a quantum network protocol*, *Proceedings of the 16th International Conference on Emerging Networking EXperiments and Technologies*, CoNEXT '20, 1 (2020).
- [92] F. Rozpędek, K. Goodenough, J. Ribeiro, N. Kalb, V. C. Vivoli, A. Reiserer, R. Hanson, S. Wehner, and D. Elkouss, *Parameter regimes for a single sequential quantum repeater*, *Quantum Science and Technology* **3**, 034002 (2018).
- [93] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and K. Nemoto, *Quantum communication without the necessity of quantum memories*, *Nature Photonics* **6**, 777 (2012).
- [94] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, *Ultrafast and Fault-Tolerant Quantum Communication across Long Distances*, *Physical Review Letters* **112** (2014), 10.1103/PhysRevLett.112.250501, 1310.5291 .

- [95] J. Borregaard, H. Pichler, T. Schröder, M. D. Lukin, P. Lodahl, and A. S. Sørensen, *One-Way Quantum Repeater Based on Near-Deterministic Photon-Emitter Interfaces*, *Physical Review X* **10**, 021071 (2020).
- [96] F. Rozpędek, K. Noh, Q. Xu, S. Guha, and L. Jiang, *Quantum repeaters based on concatenated bosonic and discrete-variable quantum codes*, *npj Quantum Information* **7**, 1 (2021).
- [97] K. Azuma, K. Tamaki, and H.-K. Lo, *All-photonic quantum repeaters*, *Nature Communications* **6**, 1 (2015).
- [98] M. Pant, H. Krovi, D. Englund, and S. Guha, *Rate-distance tradeoff and resource costs for all-optical quantum repeaters*, *Physical Review A* **95**, 012304 (2017).
- [99] K. Fukui, R. N. Alexander, and P. van Loock, *All-optical long-distance quantum communication with Gottesman-Kitaev-Preskill qubits*, *Physical Review Research* **3**, 033118 (2021).
- [100] A. Seri, D. Lago-Rivera, A. Lenhard, G. Corrielli, R. Osellame, M. Mazzer, and H. de Riedmatten, *Quantum Storage of Frequency-Multiplexed Heralded Single Photons*, *Physical Review Letters* **123**, 080502 (2019).
- [101] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, *Quantum repeater with encoding*, *Physical Review A* **79**, 032325 (2009).
- [102] Y. Jing and M. Razavi, *Quantum Repeater with Encoding on Nitrogen-Vacancy-Center Platforms*, *Physical Review Applied* **18**, 024041 (2022).
- [103] G. Avis, F. Rozpędek, and S. Wehner, *Replication data for: Analysis of Multipartite Entanglement Distribution using a Central Quantum-Network Node*, <https://doi.org/10.4121/19235937>.
- [104] M.-D. Choi, *Completely positive linear maps on complex matrices*, *Linear Algebra and its Applications* **10**, 285 (1975).
- [105] A. Jamiolkowski, *Linear transformations which preserve trace and positive semidefiniteness of operators*, *Reports on Mathematical Physics* **3**, 275 (1972).
- [106] S. Khatri and M. M. Wilde, *Principles of Quantum Communication Theory: A Modern Approach*, (2020), arXiv:2011.04672 .

Acknowledgments

For the completion of this dissertation I owe a debt of gratitude to everyone in my (quantum) network of mentors, collaborators, friends and loved ones. In the first place, this work would never have been possible without **Stephanie**. You have introduced me into the fascinating world of quantum communication and have always encouraged me to make the most of my PhD. The past four years I spent under your supervision have been rather eventful. Not only did we have to endure a pandemic, you also almost lost and then regained your eyesight, and your beautiful child Sara was born. At all times though you have been there to support me and inspire me with your powerful vision for a quantum internet. I always enjoy our scientific discussions and your amazing insight into a large variety of topics. Thank you for transforming me into a proper researcher.

I would also like to extend my thanks towards the people who agreed to read my thesis and then quiz me about it for an hour (i.e., my committee members). Thank you, **Ronald, Tracy, Barbara, Leo, Harold and Menno**.

Part of my PhD was spent trying to hack together a simulation of the quantum internet. As the “blueprint team” we were united by our daily struggles to debug virtual quantum networks and make sense of an agile workflow in a scientific project. Whether we were trying to put together a hackathon, align on programming philosophy in a conference call or prepare for a sprint review, we shed quite some sweat together. **Francisco**, you are not only my primary coauthor but also, “dare I say”, a friend. Not only have you optimized the requirements for quantum repeaters, but also my time in the office, both on a scientific and on a personal level. Where I can sometimes get a bit stressed, you never appear fazed and have a calming presence. I’m happy you often know to appreciate it when I make a bad pun and am always happy to return the favor. Don’t hesitate to call me sometime to discuss the etymology of some random word. **David**, I was entrusted with supervising you as a master student only shortly after I started my PhD. However, you quickly became a valued colleague, which was reflected in your subsequent upgrade from master student to PhD student. Your cheerful presence has made it a joy to work together and that pleasant interaction has extended also outside the office. I can always count on you being up for some “liquid bread”, and I hold you accountable for starting a Magic-the-Gathering frenzy in our office. Hopefully we (and Luna) will still get to play many games of Spirit Island together.

Many thanks also to the members of the blueprint team who were involved part time rather than full time. **Tim**, ik heb het altijd knap gevonden hoe je tijdens je PhD je al tot een soort miniPI hebt ontwikkeld. Waar we ook over praten, je lijkt altijd goede ideeën en inzichten te hebben. Ik geef jou echter wel de schuld dat sommige classes in de blueprint code van die ellenlange namen hebben :). **Axel**, despite doing two PhDs worth of work you always had time to review my code, from which I have learned so much. It is amazing how you solved so many problems (either scientific or practical) by just writing new software packages, and even at parties you have managed to teach me new things about VIM. **Hana**, it is crazy to think you were just doing your Bachelor’s when you first joined us, yet you

managed to not only pull much more than your weight but also integrate socially as if there was no age gap at all. You always seem to be doing a million things at the same time, yet excelling at all of them. Try not to stress about life too much, there is no doubt in my mind that you will do great things! **Julian**, hoewel je “slechts” een masterstudent was heb je niet alleen grote bijdragen geleverd aan onze simulaties, maar heb je daarnaast ook nog bedacht waar we in Nederland quantum repeaters moeten neerzetten. Ze hadden je wel twee diploma’s kunnen geven! Het was gaaf om te zien hoe je zelf de controle nam over je project, en je achtergrond in econometrie gaf je net een ander perspectief wat altijd interessante discussies opleverde. Leuk dat je nu via TNO toch weer bij QuTech betrokken bent geraakt! **Rob**, als geestelijk vader van NetSquid heb jij een belangrijk deel van de fundatie voor dit proefschrift gelegd. Ik heb enorm veel van je geleerd en heb vooral ook genoten van onze intensievere samenwerking in de context van EuroQCI. Je bent nu naar de VS vertrokken en hebt me al met het nodige advies verstrekt voor mijn eigen verhuizing, waarvoor dank! **Ariana**, even though I was not the “optimization guy” and didn’t touch the supercomputers too much, our interactions have still always been very interesting and helpful. It was great having you on the team. **Loek, Luc, Martijn, Adrià**, it was a pleasure having you involved with the blueprint in one way or the other. I wish you all the best in life.

I want to extend special thanks to **Filip**. When I first joined the group and knew more about quantum fields than about quantum information, you mentored me diligently and patiently. Even after you left Delft we have had opportunities to collaborate, which I enjoyed very much. I’m still amazed by your level of insight and really appreciate your inquisitive nature and drive to always obtain an in-depth understanding of things, even if the topic doesn’t really relate to your own research. I look forward to sitting across the hallway from you once more in Amherst!

Conversely I want to thank those who I have had the honor of mentoring. I have already mentioned the amazing **David** and **Julian**, who I adopted after their original supervisor (Filip) graduated. You were both very independent and self-reliant students who had already kick started their projects and integrated neatly into our team. I was able to take on the role of collaborator rather than supervisor and it has been a pleasure. **Flors**, you were the first student I mentored all the way from conceiving of a project to handing in a thesis. We went on a journey together through the world of one-way repeaters and error correction, and there is so much I have learned on the way. One thing I really appreciate about you is that you are never afraid to ask questions, which allowed you to also quickly learn a lot and us to have useful discussions. Thanks also for teaching me about Caganer and Tió de Nadal, knowing these exist makes my life just that little bit brighter. I hope you are having a great time doing a PhD in the mountains of Innsbruck and who knows, our paths may cross yet again in the future. **Emlyn**, after a somewhat rocky start of your project, you recovered wonderfully. You showed great flexibility in steering the topic of the research such that it works for you and ended up impressing the committee with your knowledge about quantum networks. Your easy-going character has made it very pleasant to work with you and to have you around. Being a “second-hand celiac” myself, it has also been great having someone to talk about the challenges and opportunities involved with finding (vegan) gluten-free food. **Soubhadra**, being your daily supervisor has been my first experience supervising a PhD student. I hope we managed to sufficiently kick start your project so that I will not be missed too much. Best of luck on the rest of

your PhD, it's a great and amazing adventure you are embarking on and you will do very well!

A big thank you also to those who contributed to this thesis by coauthoring some of the chapters above. Apart from those who have already been mentioned, thanks **Anders, Kaushik** and **Josh**. Also to those who contributed through useful discussions or by providing feedback on manuscripts, I owe you one, **Gayane, Álvaro, Bethany, Janice, Bart, Sophie, Matteo, Arian, Kian, Mariagrazia, Alejandro, Ben, Viktor, Simon, Dario, Maria** and **Markus**.

I count myself lucky to have been part of a scientific environment made up of such incredible people. Not only are you all very talented researchers, you are also great at having lunch and coffee together (strictly 12:00 - 13:00, of course). You are all part of the wonderful and safe environment in which I have been able to develop myself during my PhD. I will miss all the times we played board games, saw movies together, went on corona walks or just had food delivered to us while sunbathing in the Mekelpark.

Carlo, thanks for breaking down any stereotype of Italians I may have ever had. I don't think I have ever met anyone so well-organized and neat as you. You are a great ally in the quest of making this world a kinder place through veganism. We started and now will finish our PhDs around the same time. It has been a great journey together and I have enjoyed not only our time inside the office, but also outside the office (also with Julia).

Sébastien, het was tof om synchroon onze PhDs te doen. Bij het begin leek het even dat we vergelijkbare dingen gingen doen ("iets met GHZ states"), maar uiteindelijk liep het toch wel meer uit elkaar. Desalniettemin was het fantastisch om je als collega te hebben. Vaak mochten we als Nederlanders met onze bammetjes als eerste een tafel zoeken bij de lunch terwijl de rest iets kocht of opwarmde. Ik waardeer je droge humor en dat je altijd in bent voor een (bord)spelletje.

Kenneth, bedankt dat je me altijd scherp hebt gehouden door zelfs de pauzes met wetenschap en wiskunde te vullen. Je oprechte liefde voor het leren van nieuwe dingen is inspirerend en aanstekelijk. Ik kijk ernaar uit dat onze paden elkaar straks weer kruizen in Amherst.

Gayane, when you joined our group, that was a great infusion of new expertise, a new perspective and new ideas. I have always been happy to hear your thoughts not only on science itself but also on academia. Playing board games together has been a lot of fun and your new position as PI is much deserved. Thanks also for putting Amherst so clearly on my radar. Hopefully we (and Subhransu) get to interact again over there!

Álvaro, it has been a lot of fun to see you develop from a master student into a PhD student. Now you are so autonomous you even have your own grant! I always enjoy hanging out with you, but worry I'll never get to beat you at Smash Bros.

Bethany, I'm impressed with how you have taken charge of your own PhD and are formulating all these interesting questions. Hopefully we will get to answer at least one of those together. I have enjoyed the guilty pleasure of having whiteboard discussions with you when I really should have been finishing up my dissertation. Just keep doing what you do!

Janice, ik ben onder de indruk van wat je allemaal al voor elkaar aan het boksen bent met ion traps en BQC, allemaal met minimale begeleiding. Dat komt helemaal goed met jou! Je spontaniteit komt de groep echt ten goede en je vrolijkheid wordt zeer gewaardeerd. Je bent altijd bereid om iets op te pakken of ergens mee te helpen. En het is helemaal feest

wanneer je een vegan baksel meeneemt naar kantoor :).

Thomas, it is great having you as a new addition to the group. While we don't interact much scientifically, I'm happy to have had the chance to play D&D with you before I leave.

Luise and **Eric**, you have just started your PhDs in the new Vardoyan group but already you are great colleagues. Try to keep having fun at what you do and your PhDs will be great experiences that go by in the blink of an eye.

Scarlett, **Ravi**, **Bart** and **Siddhant**, you are in the primes of your PhDs! Enjoy this time while it lasts. I had a great time interacting with you and hope to do so again in the future.

Vicky, I'm happy I got the chance to know you better while exploring Chicago and Boston. Your unfiltered questions are great conversation starters. You are a blob of social glue from which QuTech really benefits.

Bas, **Victoria**, **Matt**, **Jérémy**, **Ben**, **Stefan**, **Gláucia**, **Mark** and **Jonas**, you played an important part in setting the scene of my pre-corona PhD life. Thanks for welcoming me into the group and the many great conversations that we have had.

I also want to thank **Ravi**, honorary member of our social group, and **Matt**, who mysteriously materialized in the Elkouss office at some point. Further thanks to the various interns and master's students who gave my PhD extra color, **Leon**, **Martijn**, **Luc**, **Lars**, **Bob**, **Yu**, **Adria**, **Yves**, **Sebastiaan**, **Matthijs**, **Antal** and **Bassem**. Finally, I would like to thank **Helena**, **Kanchan** and all the other management assistants who have made my PhD go that much more smoothly.

It was not only scientists who enabled me to start and finish this PhD. **Mam en Pap**, bedankt dat jullie altijd vertrouwen in me hebben gehad en me de vrijheid hebben gegeven om mezelf te onwikkelen. **Stijn** en **Lotte**, al bewandelen we misschien andere paden in het leven, ik ben blij jullie als broer en zus te hebben en weet dat ik altijd op jullie kan rekenen. **Hans**, **Daphne** en **Maarten**, bedankt dat jullie me altijd met open armen hebben verwelkomd en me een tweede familie hebben gegeven. **Anne**, **Niek** en **André**, wat is het fijn om jullie erbij te hebben! **Otto**, **David** en **Thijs**, ik ben blij dat we na al die jaren nog steeds goede vrienden zijn en hoop dat we dat kunnen vasthouden wanneer we niet alleen in verschillende steden, maar ook op verschillende continenten wonen.

Last but not least, **Eva**, bedankt dat je er al tien jaar lang altijd voor me bent en me steunt door dik en dun. Voor jou was een verborgen maar niet te onderschatten sleutelrol weggelegd in mijn PhD, en dat zeg ik niet alleen omdat jouw hand is terug te vinden in veel van de figuren in dit proefschrift. Het maakte me enorm blij dat je met me wilde trouwen. Kan je nagaan hoe ik me erover voel dat je het zelfs nog een "tweede" keer wil doen! Ik kijk er naar uit om samen de Atlantische oceaan over te steken. Het wordt een groot avontuur en hoewel we daar allebei veel zin in hebben, is het natuurlijk ook een beetje spannend. Maar zolang ik jou bij me heb weet ik zeker dat het prachtig wordt, waar we ook zijn.

Curriculum Vitæ

August Frederik Gerbrand (Guus) Avis

07-08-1994	Born in Bussum, the Netherlands
2007 - 2013	High School (Gymnasium) Het Stedelijk Zutphen, the Netherlands
2013 - 2016	Bachelors in Physics and Philosophy with Honours Programme University of Groningen, the Netherlands
2016 - 2018	Master in Theoretical Physics Utrecht University, the Netherlands <i>Thesis:</i> Adiabatic Modes in an Open Universe <i>Supervisor:</i> dr. E. Pajer
2018 - 2023	PhD in Quantum Networks QuTech, Delft University of Technology, the Netherlands <i>Thesis:</i> Shortcuts Towards Fiber-Based Quantum Networks <i>Promotor:</i> Prof. dr. S.D.C. Wehner <i>Promotor:</i> Prof. dr. ir. R. Hanson

List of Publications

7. Kah Jen Wo, **Guus Avis**, Filip Rozpędek, Maria Flors Mor-Ruiz, Liang Jiang, Anders S. Sørensen, Johannes Borregaard, *Resource-efficient fault-tolerant one-way quantum repeater with code concatenation*, in preparation.
6. **Guus Avis**, Robert Knegjens, Anders S. Sørensen, Stephanie Wehner, *Asymmetric node placement in fiber-based quantum networks*, preprint arXiv:2305.09635 (2023).
5. Francisco Ferreira da Silva*, **Guus Avis***, Joshua A. Slater, Stephanie Wehner, *Requirements for upgrading trusted-nodes to a repeater chain over 900 km of optical fiber*, preprint arXiv:2303.03234 (2023).
4. **Guus Avis***, Francisco Ferreira da Silva*, Tim Coopmans, Axel Dahlberg, Hana Jirovská, David Maier, Julian Rabbie, Ariana Torres-Knoop, Stephanie Wehner, *Requirements for a processing-node quantum repeater on a real-world fiber grid*, preprint arXiv:2207.10579 (2022).
3. **Guus Avis**, Filip Rozpędek, Stephanie Wehner, *Analysis of multipartite entanglement distribution using a central quantum-network node*, Phys. Rev. A 107, 012609 (2023).
2. Julian Rabbie, Kaushik Chakraborty*, **Guus Avis***, and S. Wehner, *Designing Quantum Networks Using Preexisting Infrastructure*, npj Quantum Inf 8, 5 (2022).
1. **Guus Avis**, Sadra Jazayeri, Enrico Pajer, Jakub Supel, *Spatial curvature at the sound horizon*, JCAP 02 034 (2020).

*These authors contributed equally.

