UNIVERSIDAD DE CONCEPCIÓN
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

HIGH-DIMENSIONAL DECOY-STATE QUANTUM KEY DISTRIBUTION OVER 1.3 KM OF INSTALLED OPTICAL FIBER

POR: KEI BRAZ SAWADA

Tesis presentada a la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Concepción para optar al grado académico de Doctorado en Ciencias Físicas

Marzo 2025

Concepción, Chile

Profesor Guía: Gustavo de Aquino Moreira Lima

愚に暗く
foolishly, in the dark,
茨を掴む
he grabs a thorn:
蛍かな
hunting fireflies

— Matsuo Bashō, summer of 1680

Acknowledgments

The last four years have been a horizon-expanding journey during which many people contributed to the completion of this thesis, some of whom I met before my PhD and many of which I met afterwards.

I'd like to thank Stephen Walborn, who invited me over in 2020 and introduced me to the research group at UdeC, giving me the opportunity to start my work here and providing advice and feedback throughout the way as he always has.

Steve introduced me to Gustavo Lima, my PhD advisor, who accepted me as his student despite never having met me before, and thanks to his guidance I've learned and grown so much as a scientist. I thank Gustavo for his crucial support, both in research and helping me move to a new country.

I'm grateful to have worked with many new people at the lab who I'd like to thank: Daniel Martínez, who always lent an ear when I needed one and helped me immensely both in and out of the lab, Gustavo Santos and Nelson Villalba for all the help, long hours of work and trust in my judgment, and Jaime Cariñe for his technical support and upgrades to the experiment.

I also want to thank Esteban Sepúlveda for lending me a hand when I needed it, and Miriam Yang, Letícia Tacca, Sebastián Ayala and Jéssica Martins for the friendship, patience and support throughout these years.

To my parents, I'm thankful for the unconditional faith and trust placed in me and the daily conversations we've had that helped me feel not so far away from home.

Finally, I want to thank Adonai for all the help, for sharing their life with me, and the honor of letting me share my life with them.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

Resumen

HD-QKD (distribución cuántica de claves en altas dimensiones) es una alternativa a la QKD (distribución cuántica de claves) bidimensional con ventajas como una mayor transmisión de datos por pulso [54] y tolerancia al ruido [13, 66]. Se ha demostrado que las MCFs (fibras ópticas multi-núcleo) son una plataforma viable para realizar HD-QKD mediante codificación de fase entre los modos de la misma fibra [10]. Las MCFs también han atraído la atención de ingenieros debido a su mayor tasa de transmisión de datos y es probable que se conviertan en parte de la infraestructura de telecomunicaciones en el futuro [35, 50, 14, 51]. En esta tesis, presentamos un experimento de prueba de concepto de HD-QKD, ocupando BB84 con decoy states (estados señuelo), con una configuración de fibra óptica que utiliza 4C-MCFs (fibras ópticas de cuatro núcleos) en un ambiente realista. Presentamos la teoría de QKD y las motivaciones para los decoy states, así como los límites de seguridad para sistemas de diferentes dimensiones. Describimos el experimento en detalle, incluyendo la estabilización de fase activa, la preparación del estado, las tecnologías basadas en MCF, los canales y el sistema de detección. Reportamos una tasa de transmisión máxima de corto alcance de 7,8 kbit/s y una distancia máxima de transmisión de 107 km, así como una estabilidad de corto alcance de más de 16 horas. Se presenta una comparación de nuestro experimento con varios otros, demostrando que nuestros resultados son comparables a los de otros trabajos con tecnología de detección similar. También incluimos dos artículos donde utilizamos nuestra plataforma experimental para experimentos en que simulamos ruido no markoviano e implementamos tomografía de estado cuántico con una configuración, lo que demuestra la flexibilidad de nuestra plataforma y el

potencial para futuros trabajos.

Palabras clave – BB84, decoy states, distribución cuántica de claves, altas dimensiones, fibra multinúcleo, fibra instalada, estabilización de ruido de fase

Abstract

HD-QKD (high-dimensional quantum key distribution) is an alternative to two-dimensional QKD with advantages such as higher data transmission per pulse [54] and noise tolerance [13, 66]. It has been shown that MCFs (multicore fibers) are a viable platform for performing HD-QKD through phase encoding across modes of the same fiber [10]. MCFs have also gathered attention due to their increased data transmission rates and are likely to become part of classical telecom infrastructure in the future [35, 50, 14, 51]. In this thesis we report a proof-of-concept decoy-state BB84 HD-QKD experiment with an all-fiber setup using installed 4C-MCFs (four-core multicore fibers) in a realistic environment. We introduce the theory of QKD and the motivations for decoy states as well as the security bounds for systems with different dimensions. We describe the experiment in detail, including active phase stabilization, state preparation, MCF-based technologies, channels and the detection system. We report a maximum short-range key rate of 7.8 kbit/s and a maximum secure key transmission distance of 105 km, as well as a short-range stability of over 16 hours. A comparison of our experiment with several others is provided, showing that our results are comparable to other works with similar detection technology. We also include two papers where we used our experimental platform for experiments simulating non-Markovian noise and implementing single-setting quantum state tomography, showing the flexibility of our setup and potential for further work.

Keywords – BB84, decoy states, QKD, high-dimensional, multicore fiber, installed fiber, phase noise stabilization

1 INTRODUCTION

QKD (quantum key distribution) is a rapidly developing technology. Although it was first proposed in the 80s [5], its relevance grew with the development of Shor's algorithm in 1994 [67] and the rise of quantum computers, which threatened to break well-established, classical public-key cryptosystems. QKD emerged as an alternative where security was guaranteed not by mathematical formulas but by the laws of physics. While quantum computers are still in an early stage of development, QKD is currently one of the most mature quantum technologies [56, Flagship].

Classical computers encode information in voltages in an electrical circuit, but QKD systems, similar to quantum computers, have a wide variety of ways to encode information, and the best one is anyone's guess at the moment. Even the dimensionality of the information - also known as the base of a numeral system - is flexible, unlike in classical binary systems, and multiple advantages have been found in working with HD (high-dimensional) quantum systems, including higher information density, noise resilience and overcoming detector limitations in QKD [54, 13, 66], better sensitivity in quantum metrology [39, 74, 3] and efficiency in quantum computing [6, 37, 4]. These advantages often come at a cost, either in the difficulty of implementation or intrinsic features of the system. For example, in time-bin encoding (currently one of the most popular QKD platforms) a

fraction of $(d-1)/d$ photons are lost, where d is the system's dimension [2].

A natural candidate for use in HD systems is the MCF, a fiber consisting of multiple cores in the same cladding. By sending pulses of light through all cores of an MCF simultaneously, one can encode information in the phase difference across modes in different cores. MCFs avoid the dimensional scaling issues of time bins and have the additional advantage of being a topic of research in classical communication [57]. This is due to the fact that current single-core fibers are reaching their maximum data transmission capacity. Starting in 1982, technological breakthroughs caused the capacity of fibers to increase tenfold every four years, similar to Moore's law for computers; *SDM* (spatial division multiplexing) technology, which includes MCFs and *FMFs* (few-mode fibers), is expected to be the next step in that increase. The expected integration of MCFs into classical telecom infrastructure in the next few years [35, 50, 14, 51] would make them a convenient platform for quantum communication, as QKD could be implemented in existing fibers and even coexist with classical communication [18].

In this thesis I describe the successful implementation of a proof-of-concept four-dimensional QKD scheme over 1.3 km of installed 4C-MCF. The text is organized as follows: Chapter 2 introduces the theoretical framework of this thesis, including the basics of quantum mechanics, cryptography and the QKD protocol we used, known as the decoy states protocol, as well as the variables measured. Chapter 3 describes the experimental setup: state preparation and measurement, the MCF-specific technologies we used and

the channels. Chapter 4 reports our results, including data transmission rates, system stability, other relevant variables for practical QKD systems and a comparison with other QKD experiments. Chapter 5 summarizes our findings and concludes the main body of the thesis. The appendices contain two papers, one published [59] and one submitted [46], which I have worked on. They are connected to this work by dint of using the same experimental platform with some modifications.

My hope is for this thesis to serve not only as a detailed description of our findings, but also as a useful reference for others in the future who find themselves working with our experimental setup. There is still plenty that can be done with it.

2 THEORETICAL FRAMEWORK

2.1 Fundamentals of Quantum Mechanics

We begin by reviewing the basic formalism of quantum mechanics required to understand this thesis. An introductory knowledge of linear algebra is assumed.

2.1.1 Postulates

Quantum mechanics is based on a series of postulates whose order and number vary depending on the author. In this section, we will introduce the postulates as defined in Ref. [49], where a more detailed treatment of quantum mechanics is also provided.

> **Postulate 1**: Any isolated quantum system is fully described by a unit vector in a complex vector space.

In other words, an isolated system is described by a unit vector known as a state vector or state, written as $|\psi\rangle$. In this notation, $|\psi\rangle$ is commonly known as a *ket*. It exists in a type of vector space associated with the system,

known as a *state space* or *Hilbert space*. It is a subset of $\mathbb{C}^n$ (the space of vectors with n complex components) equipped with an inner product. The nature of this space depends on the system and finding it is a common problem in quantum mechanics.

The state can be expressed as a column matrix

$$|\psi\rangle = \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{pmatrix}. \tag{2.1.1}$$

The dual of $|\psi\rangle$, known as a *bra*, is defined as its conjugate transpose (also known as a Hermitian conjugate):

$$\langle\psi| = |\psi\rangle^\dagger = \begin{pmatrix} z_1^* & z_2^* & \cdots & z_n^* \end{pmatrix}. \tag{2.1.2}$$

The inner product of two vectors $|\psi\rangle$ and $|\phi\rangle$ is written as $\langle\psi|\phi\rangle$. A set of vectors $|v_1\rangle, \cdots, |v_n\rangle$ such that any vector in Hilbert space can be written as a linear combination of them is known as a *spanning set*. If they are also linearly independent, it is known as a *basis*. A particularly relevant one is the *computational basis*, defined as

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ |1\rangle = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ \cdots, |n\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}. \tag{2.1.3}$$

It is often preferable to use orthonormal bases, meaning their components

are unit vectors orthogonal to each other.

An important property of quantum states is that they can be in a superposition, such as $(|0\rangle + |1\rangle)/2$, unlike a classical bit that can only be in state 0 or 1. Quantum computers and communication systems frequently make use of this.

The *dimension d* of a system is the number of elements in the basis. Systems where $d = 2$ are known as *qubits*, while systems where $d > 2$ are known as *qudits* or *high-dimensional systems*.

The evolution of a quantum system over time is provided by the next postulate.

> **Postulate 2**: If an isolated quantum system is in state $|\psi\rangle$ at time t_0, its state $|\psi'\rangle$ at time t_1 is given by a unitary operator $U(t_1, t_0)$ depending only on t_1 and t_0 and acting on $|\psi\rangle$:
>
> $$|\psi'\rangle = U(t_1, t_0)\,|\psi\rangle\,. \tag{2.1.4}$$

The operator has to be a unitary matrix so that $|\psi'\rangle$ remains a unit vector, and therefore stays in the Hilbert space as it evolves. In the context of quantum information, unitary operators are analogous to the logic gates used in classical information. For qubits, three important types of unitary matrices are the *bit-flip matrix X* (which takes $|0\rangle$ to $|1\rangle$ and vice-versa, analogous to the NOT gate), the *phase-flip matrix Z* (which does nothing to $|0\rangle$ and takes $|1\rangle$ to $-|1\rangle$), and the *two-dimensional Hadamard matrix H*

defined as

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{2.1.5}$$

In the case of qudits, two important unitary operators in this thesis are the *phase transformation* $U(\theta_n)$,

$$U(\theta_n) = \frac{1}{\sqrt{d}} \begin{pmatrix} e^{i\theta_0} & 0 & \cdots & 0 \\ 0 & e^{i\theta_1} & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & e^{i\theta_n} \end{pmatrix}, \tag{2.1.6}$$

where all off-diagonal terms are 0, and the *d-dimensional Hadamard matrix*, defined as a square matrix whose entries are either $+1$ or -1 and whose rows are mutually orthogonal. In quantum information, Hadamard matrices are usually multiplied by a constant $1/\sqrt{d}$ to make them unitary [29].

The Schrödinger equation is the equivalent of Postulate 2 for continuous time, describing the time evolution in terms of a Hamiltonian operator. However, in this thesis we will only require the discrete postulate.

Operators can represent both the time evolution of a system and its physical quantities or observables such as position, momentum and energy. Unlike in classical physics, when measuring observables in quantum mechanics, their outcomes are probabilistic. The *expected value* (i.e. the statistical mean) of an operator A in a system in state $|\psi\rangle$ is then given by

$$\langle A \rangle = \langle \psi | A | \psi \rangle, \tag{2.1.7}$$

and the result of measuring A will always be an eigenvalue λ_i of A with probability $\langle\psi|\lambda_i\rangle\langle\lambda_i|\psi\rangle = |\langle\lambda_i|\psi\rangle|^2$, where $|\lambda_i\rangle$ is the eigenvector associated with λ_i. This is known as the *Born rule*. The next postulate formalizes this measurement process, introducing an important class of non-unitary operators: the measurement operators.

> **Postulate 3**: A measurement on a quantum system is described by a collection of *measurement operators* $\{M_m\}$, and the outcome of the measurement is assigned to the index m. If the state of the quantum system immediately before the measurement is $|\psi\rangle$, the probability of obtaining the outcome m is
>
> $$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle \tag{2.1.8}$$
>
> and after the measurement the system will be in the state
>
> $$|\psi'\rangle = \frac{M_m|\psi\rangle}{\sqrt{\langle\psi| M_m^\dagger M_m |\psi\rangle}}. \tag{2.1.9}$$

Given that all probabilities must add up to one, the $\{M_m\}$ must satisfy the *completeness equation*:

$$\sum_m M_m^\dagger M_m = I \tag{2.1.10}$$

$$\Rightarrow \sum_m p(m) = \sum_m \langle\psi| M_m^\dagger M_m |\psi\rangle = 1. \tag{2.1.11}$$

This postulate also explains why the $|\psi\rangle$ must be unit vectors: the last

equation is only true if $\langle\psi|\psi\rangle = 1$. This is known as the *normalization condition*, and the $|\psi\rangle$ are said to be *normalized*.

In qubit systems, one such example is measurement in the computational basis. In this case, the operators are $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$. A state $|\psi\rangle = a|0\rangle + b|1\rangle$ will then lead to a probability of obtaining outcome 0 given by $p(0) = |a|^2$, and a probability of outcome 1 given by $p(1) = |b|^2$. Measurements in other bases are also possible. From an experimental point of view, one can do this by building a system that applies a unitary transformation to a state and then measures in the computational basis. For example, the so-called *diagonal basis* is given by

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \tag{2.1.12}$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}, \tag{2.1.13}$$

and measuring $|\psi\rangle$ in this basis with $M_+ = |+\rangle\langle +|$ and $M_- = |-\rangle\langle -|$ is equivalent to applying a Hadamard matrix to $|\psi\rangle$ and then measuring with $\{M_0, M_1\}$. The diagonal and computational bases are said to be *mutually unbiased* with respect to each other. For example, if one prepares state $|+\rangle$ and measures in the computational basis, then one obtains outcomes 0 or 1 with equal probability. In other words, if a state is a component of a basis, measuring it in a mutually unbiased basis gives us a random result with no information that would allow us to identify the state.

Finally, the fourth postulate defines how Hilbert spaces of different quantum systems are combined.

Postulate 4: The state space of a composite system is the tensor product of the state spaces of its subsystems. The state $|\Psi\rangle$ of a collection of n systems in states $\{|\psi_i\rangle\}$ is $|\Psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$.

2.1.2 Density Matrices

In addition to the postulates, there is a useful mathematical construct known as the *density matrix* or *density operator*. For a system that is in one of a number of states $|\psi_i\rangle$, each with a respective probability p_i, it is given by

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i| \tag{2.1.14}$$

and is a square matrix. Its diagonal elements are known as *populations* and its off-diagonal elements are known as *coherences*.

The advantage of the density matrix is that it can represent statistical ensembles of states, which cannot be done with just one state vector. For example, suppose a machine produces an ensemble of qubits, which after measuring in the computational basis give us the results 0 or 1 with equal probability. There are then two possibilities: either all of the qubits are in a superposition $(a|0\rangle + b|1\rangle)/\sqrt{2}$ with $|a|^2 = |b|^2$, or the machine produces states $|0\rangle$ and $|1\rangle$ with 50% probability each. The density matrix allows us to distinguish these two cases on a mathematical level.

2.1.3 Second Quantization

Classical physics describes a system in terms of observable physical quantities, expressed as scalar, vector or tensor fields. Section 2.1.1 introduced what is sometimes known as first quantization [73]: the construction of a quantum theory where a system is described in terms of a wave function and its observables are linear operators. While many problems can be solved with this approach, it is missing an important feature of quantum systems: the indistinguishability of particles. Unlike in classical mechanics, it is not possible to "tag" a quantum particle so we can identify it among an ensemble of identical particles except by encoding information in some available degree of freedom. Hence, all photons with the same wave function and physical properties are identical. More than a formality, indistinguishability leads to observable effects in many experiments, a famous example being the Hong-Ou-Mandel effect [30].

Therefore, in this section we will introduce *second quantization*: the construction of a theory describing a system in terms of *Fock states* in a *Fock space*. A more detailed treatment can be found in Ref. [55].

Fock states describe how many particles are in a given state with no regard for which particles they are. They are typically written in the form $|n\rangle$, where n is the *occupation number* of the state. The two most fundamental operators acting on such a state are the *annihilation and creation operators* a and $a^\dagger$, defined as

$$a|n\rangle = \sqrt{n}\,|n-1\rangle\,, \tag{2.1.15}$$

$$a^\dagger |n\rangle = \sqrt{n+1}\,|n+1\rangle\,, \tag{2.1.16}$$

leading to the *number operator*

$$\begin{aligned} N|n\rangle &= a^\dagger a\,|n\rangle \\ &= n\,|n\rangle\,. \end{aligned} \tag{2.1.17}$$

In Section 2.4 we will use this approach to describe a special class of Fock state superpositions known as coherent states.

2.2 Fundamentals of Cryptography

The purpose of quantum key distribution is, of course, to securely distribute *keys*: sequences of numbers used by an *encryption algorithm* to encrypt data, making it difficult or even impossible to read without the *decryption key* to convert it back to its original state. Although this work does not deal with encryption algorithms themselves, to understand the context in which it is written it is useful to understand the broader idea of cryptography.

The aim of encryption is to hide information from unwelcome observers, a goal that has been pursued since at least 1500 BC in Mesopotamia [36], where a clay tablet was found with an encrypted recipe for pottery glaze. However, here we will focus on what is known as modern cryptography, a field founded by Claude Shannon in his 1949 paper [65].

An encryption algorithm takes a message, known as the *plaintext*, in the form of a string of numbers and combines that with another string of numbers, known as a key. The encrypted message is then known as the *ciphertext*.

Another string of numbers, known as the decryption key, is then combined with the ciphertext in some way to recover the plaintext. If the encryption and decryption keys are the same, the algorithm is said to be *symmetric-key*. If they are different, the algorithm is *asymmetric-key* or *public-key*. In the latter case the encryption key is known as the *public key* and the decryption key is known as the *private key*.

Ideally it should be impossible to decrypt a message without knowledge of the decryption key: this is known as *perfect secrecy*. In practice, an attacker can always perform a *brute-force attack*, i.e. one where they attempt to decrypt with every possible string of numbers until they find the right one. However, Shannon proved that perfect secrecy is possible with a *one-time pad*: a key that is completely random and at least as long as the plaintext [65]. Shannon also proved that any algorithm achieving perfect secrecy has at least the same requirements as a one-time pad. Intuitively, the one-time pad works because the ciphertext it produces has no statistical patterns for an attacker to exploit (assuming the algorithm itself is not vulnerable).

For example, the word "teeth" may be encrypted into "hpnzs", which (despite the plaintext having a repeated letter) is fully random and may be decrypted into any five-letter word such as "storm", "trust" or "moons" depending on the decryption key an attacker attempts. Therefore a one-time-pad-encrypted message of length ℓ can decrypt into any message of the same length with no way to know which one is the original.

The requirement for randomness comes from the fact that if the key is not completely random, an attacker may exploit some statistical property of the

key to drastically shrink the space of valid keys. The requirement for the key to be as long as the plaintext is actually equivalent to the randomness requirement, because otherwise it is necessary to repeat some part of the key, destroying the randomness. For the same reason, a one-time pad can never be reused. Randomness is an important resource not just in one-time pads but in all cryptography, and for this reason the generation of truly random numbers is an important application of quantum systems.

In practice, due to its length, a one-time pad is too cumbersome to use for all but the most critical applications. Hence the focus of much cryptographic research is not to design algorithms with perfect secrecy, but rather to create ones that can only be broken with an unreasonable amount of time to do so (centuries or more), even if the attacker uses methods better than brute force. This has led to the development of *AES* (Advanced Encryption Standard), currently the symmetric-key algorithm approved by the US government as the standard for encryption [15]. AES is available with different key sizes, and AES-256 (which uses a 256-bit key) is currently considered secure against attacks by quantum computers, although AES-192 and AES-128 are not [8].

Even so, symmetric-key algorithms suffer from a fundamental difficulty: key distribution. If two people, commonly referred to as Alice and Bob, wish to communicate securely, they first need a protocol to distribute a key to each other in such a way that Eve, a spy, cannot obtain enough information about the key to decrypt their communications. This motivated the development of public-key cryptography, in which Alice and Bob each have a public (encryption) key and a private (decryption) key. They distribute only their

public keys while keeping their private keys secret. Without the private key, Eve is then unable to decrypt their messages.

For a public-key algorithm to be secure, it must be very difficult to calculate the private key given knowledge of the public key; much like decrypting a message, it must take an unreasonably long time to calculate with current technology. *RSA*, currently one of the most popular public-key algorithms, solves this problem by relying on the fact that multiplying two large prime numbers is somewhat easy, but if one only knows their product, it is difficult to find the primes. This is known as the *factoring problem*.

This status has been threatened by *Shor's algorithm* [68], which enables the efficient factoring of large numbers and also breaks the finite-field and elliptic-curve Diffie-Hellman key exchange algorithms [58], and the rise of quantum computers. Specifically, Shor's algorithm can factor a number N in a time proportional to a polynomial of $\log N$. This means that simply increasing the length of the key (and therefore of N) is not an efficient tactic for countering Shor's algorithm.

Shor's discovery spurred the field of *post-quantum cryptography*, where researchers design cryptosystems that are resistant to currently known quantum algorithms. In August 2024, NIST (the USA's National Institute of Standards and Technology) announced their first three standard post-quantum algorithms [48]. However, both post-quantum cryptography and quantum computation are in their infancy and these algorithms may be broken in the future, as occurred with one of the strongest candidates for a NIST standard [17].

Ultimately, when implemented well, classical, public-key cryptographic algorithms rely on currently known mathematics for their security. When implemented imperfectly, they are vulnerable to *side-channel attacks*: methods that rely on some physical aspect of the system leaking information, such as power consumption, electromagnetic radiation, dissipated heat and noise, and timing [70]. However, an alternative exists in the form of QKD: a method for sharing keys to be used in symmetric-key cryptography that relies on the laws of physics and is potentially much more resilient against both cryptanalysis and side-channel attacks. In Section 2.3, we review BB84, one of the most widely used QKD protocols and the basis for the decoy states protocol used in this thesis.

2.3 BB84

BB84, named after Charles Bennett and Giles Brassard who published it in 1984, is the first quantum key distribution protocol [5, 9]. Its security was rigorously proven by Peter Shor and John Preskil in 2000 [69]. In its modern form it has multiple stages including error correction and privacy amplification, but here we describe a simplified version of the protocol containing its fundamental features. A more complete description will be provided in Section 2.7.

In BB84, Alice wants to share a secret key with Bob by sending individual photons. She does this by encoding each bit of the key into a qubit $|0\rangle_B$ or $|1\rangle_B$, where B is a randomly-chosen basis for each qubit (out of two possible

mutually unbiased bases Z or X). [1]

She then sends the qubits to Bob, who measures each one in an independent randomly-chosen basis Z or X. After Alice finishes sending, they share the preparation and measurement bases of each photon through a public, authenticated channel (meaning no one can impersonate Alice or Bob) and discard any results where they do not match.[2] The latter process is known as *basis reconciliation* or *sifting*. In a perfect system, Alice and Bob would then share the same key with no errors.

While Alice sends photons, Eve, a spy, attempts an intercept-and-resend attack: she intercepts the photons, performs a measurement in the Z or X basis at random, then produces a photon with the same detected state in her measured basis and resends it to Bob. By doing this, Eve is effectively trying to make a copy of the state and pass it on to Bob without his knowledge. The idea behind the protocol's security is that, because cloning an unknown arbitrary quantum state is impossible [52, 78], Eve's attempt will inevitably introduce errors into the key. The fraction of bits with errors is known as the *QBER (quantum bit error rate)*, and forms the basis of the protocol's security: given the QBER, Alice and Bob can calculate the number of bits leaked to Eve, and if it is as large as the key, secure communication is impossible and they abort the protocol.

[1] The bits may be encoded, for example, in the polarization of each photon. The states $|0\rangle_Z$ and $|1\rangle_Z$ in the Z basis would represent the vertical and horizontal polarizations while the states $|0\rangle_X$ and $|1\rangle_X$ in the X basis would represent the diagonal and anti-diagonal polarizations.

[2] Strictly speaking, for authentication, Alice and Bob need to have a small secret key already shared between them. This could be done with post-quantum public-key cryptography (see Section 2.2). It would be spent after the BB84 protocol, but then they could simply use part of the new, larger secret key for authentication in the future. For this reason, BB84 is sometimes called by the less famous name "quantum key growing" [7].

Indeed, for the two-basis two-dimensional protocol, it has been shown [66] that secure communication is possible as long as the QBER is below 11%. This is true against both *individual attacks* (where Eve probes photons one by one, as in the attack described before) and *coherent attacks* (where Eve stores photons and performs some operation on them after basis reconciliation). Coherent attacks are stronger than individual ones: if one assumes Eve only performs individual attacks, the QBER threshold is $\sim 15\%$ [13].

However, even in the simplified form presented here, the protocol has a serious practical problem: the need to use single photons, which are expressed by the Fock state $|1\rangle$. This is in fact what makes the protocol quantum, for unlike a classical pulse of light, there is no way to separate part of a single photon and measure it. While single-photon sources exist, the most common and inexpensive (not to mention integrated in current telecom infrastructure) light source by far is the laser, which produces not a Fock state but a coherent state. We will study coherent states in more detail in Section 2.4.

2.4 Coherent States

Coherent (or canonical coherent) states are defined as the eigenstates of the annihilation operator,

$$a|\alpha\rangle = \alpha|\alpha\rangle, \tag{2.4.1}$$

where α is a complex number. As a consequence of this, its expansion in the basis of Fock states is [25]

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_n \frac{\alpha^n}{(n!)^{1/2}} |n\rangle \tag{2.4.2}$$

and, upon measuring in the Fock basis, the probability of detecting n photons is

$$P(n) = |\langle n|\alpha\rangle|^2 = e^{-|\alpha|^2} \sum_n \frac{|\alpha|^{2n}}{n!}. \tag{2.4.3}$$

This corresponds to the *Poissonian distribution*, which describes the probability of n events occurring in a given time interval if they occur, on average, $|\alpha|^2$ times during said interval. The mean of the distribution is $\mu = |\alpha|^2$, and therefore the average photon number is

$$\langle n\rangle = \mu \tag{2.4.4}$$

with variance given by [79]

$$\sigma_n^2 = \mu. \tag{2.4.5}$$

μ is also informally called the *intensity*. Given Eq. 2.4.1 and the fact that the Fock basis is orthogonal to the information encoding basis [24], Eve can take one or more photons out of a coherent state without disturbing it, thus spying without increasing the QBER, and therefore without being detected.

For this reason, BB84 with coherent states requires the phases of each pulse to be randomized. Then, using Eq. 2.4.2, the density matrix summed over

all phases is

$$\rho = \int_0^{2\pi} |\sqrt{\mu}e^{i\theta}\rangle \langle \sqrt{\mu}e^{i\theta}| \frac{d\theta}{2\pi} \tag{2.4.6}$$

$$= e^{-\mu} \sum_n \frac{\mu^n}{n!} |n\rangle \langle n|, \tag{2.4.7}$$

which is a statistical mixture of Fock states no longer subject to Eq. 2.4.1. However, using coherent states still opens up a vulnerability. In Section 2.5, we will review the assumptions this work makes about Eve's capabilities and how this enables her to perform what is known as a PNS (photon number splitting) attack.

2.5 Assumptions About Eve

As seen in Section 2.2, making overly-generous assumptions about a system introduces vulnerabilities, especially if one assumes a system is resistant to side-channel attacks. No matter how well-shielded it is, in principle a classical system can always be observed without disturbing it. For this reason, in QKD, it is necessary to make as few assumptions as possible about a practical system's security and to assume Eve has a generous amount of capabilities, including those that are infeasible with current technology but still allowed by the laws of physics and which may become achievable in the future.

The assumptions we have made in this work (common in QKD [69, 27, 43]) are that Eve can:

1. Fully control the channel from Alice to Bob, including the ability to:

   (a) Replace the entire channel (including detectors) with a noiseless, lossless one;

   (b) Receive any photons sent by Alice but not detected by Bob;

2. Perform a *QND (quantum non-demolition) measurement*, which counts the photons in a pulse without disturbing it in any way;

3. Separate a photon from a pulse and keep it (as it is or in a quantum memory) for as long as she needs to;

4. Do all of the above in a way undetectable to Alice and Bob except through the losses and QBER they measure (and not any measurable properties of the channel, which could be faked by Eve as well).

Point 1 has been criticized on the grounds that it is very unlikely to be done, given that fibers are already close to the physical limit of what can be achieved and other channel technologies are hardly any better [24]. However, the advantage of making these assumptions is that they automatically solve the question of how to tell whether losses and QBER are due to Eve or experimental imperfections: we simply take the most conservative route and assume it is all Eve.

2.6 Photon Number Splitting Attack

With the assumptions established in Section 2.5, Eve is able to launch what is known as a *PNS (photon number splitting) attack*. In its optimal form

[42], the attack consists of the following procedure:

1. Eve replaces the channel by a perfect, lossless one.

2. Eve intercepts all pulses sent by Alice and performs a QND photon counting measurement.

3. If a pulse contains one photon, Eve blocks it and Bob receives a vacuum state.

4. If a pulse contains multiple photons, Eve retains one and resends the rest to Bob.

5. Eve waits until Alice communicates her preparation bases, then measures her photons in said bases.

With this, Eve can obtain full information about every photon that arrives at Bob without increasing the QBER [43]. Surprisingly, it is still possible for Alice and Bob to establish a secure key [42, 33], although it is drastically smaller in both bit rate and maximum transmission distance compared to the decoy-state protocol used in this thesis [41].

One might object and say that, if Bob could count photons, he would expect to observe a Poissonian distribution as in Eq. 2.4.3. Bob would then either see zero- or multi-photon pulses, making it detectable. Even so, it has been shown [43] that Eve can improve this attack by controlling the channel to mimic a Poissonian distribution and remain undetected.

This attack has been known for a long time and many protocols were developed to protect against it. Notable ones include SARG04 [63], DPS [34], RRDPS [62] and COW [72]. However, recent results indicate these protocols provide little advantage over simply using BB84 with coherent states [61]. One of the most advantageous and widely used so far [61] is the decoy states protocol, which we will describe in Section 2.7.

2.7 Decoy States Protocol

The *decoy states protocol* consists of the BB84 protocol with two additions: Alice will change the intensities (i.e. average photon numbers) of her pulses at random, and before basis reconciliation, she will communicate the intensities to Bob. An intuitive explanation for why the protocol works is the following: Eve cannot know if an individual pulse she receives was sent from a coherent state source with intensity μ or ν. It is then impossible for her to accurately mimic Poissonian statistics without knowing the intensity it is supposed to have. Once Bob knows the intensity associated with each pulse, he can then calculate the transmittance associated with each intensity and check if the values are as they should be. For example, if Alice switches between a higher photon number μ and a lower photon number ν, when Eve performs the optimal PNS attack (from Section 2.6), the μ pulses will have some transmittance and the ν pulses, which are almost all zero-photon or single-photon, will almost always be blocked by Eve and have lower transmittance than expected.

To understand the protocol in more detail we must define the names we will use for different intensities. First, the states used to transmit information are

known as the *signal states*, and their intensity (or average photon number) μ is the *signal intensity*. The other states with intensity ν are known as *decoy states*. The original protocol defined $\mu < \nu$, but in general optimal results are obtained for $\mu > \nu$, so decoy states can be assumed to be weaker than signal states.

In theory, any number of different decoy intensities can be used, and in fact the optimal result is obtained from an infinite number of different $\{\nu_i\}$. However, it has been demonstrated [44] that nearly-optimal performance can be achieved using just two decoy states, with their intensities being ν and 0 (that is, vacuum states). Using only ν and not vacuum states is also an option, although it decreases performance and is outside the scope of this work. For the sake of clarity, we will only refer to states with intensity ν as decoy states; states with intensity 0 will be called *vacuum states*.

At this point, it is worth providing a full list of steps taken in the decoy state BB84 protocol, extending the informal description given in Section 2.3. The following protocol follows the scheme from Ref. [84] with minor changes.

1. **State preparation**: For each bit in her raw key, Alice randomly chooses the intensity and the basis to encode her bit. Alice will choose an intensity $I \in \{\mu, \nu, 0\}$, a random basis $B \in \{Z, X\}$, and a random state $|i\rangle_B$, $i \in \{0,1,2,3\}$. All states have equal probability of being chosen, although bases and intensities are not necessarily so.

2. **Measurement**: Bob measures the states in the Z or X basis randomly, with the same probabilities as the ones Alice used for encoding.

3. **Intensity announcement**: Over a classical, public, authenticated channel, Alice announces the intensities of each pulse sent. Bob can determine the transmittance of signal and decoy states, along with dark counts, and make an initial judgment of whether secure communication is possible.

4. **Basis reconciliation or sifting**: Over a classical, public, authenticated channel, Alice announces the basis of each pulse sent while Bob announces the locations of detected pulses and the basis used to measure each one. Alice and Bob discard all measurements with different bases.

5. **Error correction and verification**: Alice calculates some parity information of the sifted bits, encrypts that information with preshared keys, and sends it to Bob. Bob performs error correction and Alice and Bob then verify if their keys are identical. If the verification fails, they attempt error correction again or abort the protocol. Otherwise, Bob calculates the QBER using this data.

6. **Parameter estimation**: Bob uses the QBER and transmittance data to calculate the lower bound of the secret key transmission rate R.

7. **Privacy amplification**: Alice and Bob apply a universal hashing function to their keys. With this, a shorter but more secure key can be extracted [27].

In this work we will deal with steps 1 through 4 and step 6. The parity

information calculated in step 5 is not necessary to determine the QBER, as we can already obtain that information directly from the states we choose to prepare. Step 7 is useful for a practical application of a QKD system, but not necessary to characterize a system or calculate its key rate.

The key rate calculation relies on a model of the source, channel and detector. The model we shall use here follows Refs. [44, 84]. The source is a weak coherent state with phase-randomized pulses as per Eq. 2.4.7. The intensity is defined as the average photon number at the point where the pulses leave Alice's setup, which is assumed to be a secure black box.

The channel is an optical fiber with *channel transmittance* η_L given by

$$\eta_L = 10^{-\frac{\alpha L}{10}}, \tag{2.7.1}$$

where $\alpha = 0.2$ dB/km is the loss coefficient of the fiber and L, measured in km, is the length of the fiber.

The detector is assumed to be a *threshold detector* (meaning it can either detect or not detect, but cannot resolve a pulse's photon number). When considering Bob's setup as a whole, there are two transmittance factors: the *internal transmittance* from Bob's components η_{Bob} and Bob's *detector efficiency* η_D. The *total transmittance* η is then the product of all transmittance terms

$$\eta = \eta_L \eta_{Bob} \eta_D. \tag{2.7.2}$$

Given that photons are independent, the transmittance of an i-photon state is

given by

$$\eta_i = 1 - (1 - \eta)^i. \tag{2.7.3}$$

The *yield* Y_i of an i-photon state is the conditional probability of a detection by Bob given that Alice sends an i-photon state. Y_0 is the *rate of dark counts* per pulse, which is mostly due to Bob's detectors. For i-photon states the yield has a contribution from dark counts and from the actual signal,

$$Y_i \approx Y_0 + \eta_i. \tag{2.7.4}$$

The *gain* Q_i of an i-photon state is the product of the yield and the probability that Alice will send out an i-photon state:

$$Q_i = Y_i \frac{\mu^i}{i!} e^{-\mu}. \tag{2.7.5}$$

The gain of a coherent state with intensity μ is given by

$$Q_\mu = \sum_{i=0}^{\infty} Y_i \frac{\mu^i}{i!} e^{-\mu} \tag{2.7.6}$$

$$= Y_0 + 1 - e^{-\eta\mu} \tag{2.7.7}$$

and represents the probability of a detection at Bob given that Alice sent a state with intensity μ.

Eq. 2.7.7 relies on system characterization because it assumes we know Y_0 and η. Experimentally, it is estimated by [84]

$$Q_\mu \approx \frac{M_\mu}{N_\mu}, \tag{2.7.8}$$

where M_μ is the number of detections in Bob associated with μ pulses and N_μ is the number of μ pulses sent by Alice.

The error rate of i-photon states e_i is given by

$$e_i = \frac{e_0 Y_0 + e_{opt}\eta}{Y_i}, \tag{2.7.9}$$

where e_0 is the error associated with vacuum states and e_{opt} is the *optical error* associated with misalignment of the preparation and detection systems and channel noise, and is assumed to be a constant. For a d-dimensional system,

$$e_0 = 1/d \tag{2.7.10}$$

because the dark counts are random.

The QBER of a coherent state with intensity μ is given by

$$E_\mu = \frac{1}{Q_\mu}\sum_{i=0}^{\infty} e_i Y_i \frac{\mu^i}{i!} e^{-\mu} \tag{2.7.11}$$

$$= \frac{e_0 Y_0 + e_{opt}(1 - e^{-\eta\mu})}{Q_\mu}. \tag{2.7.12}$$

Once again, this equation is an expected value that relies on system characterization. Experimentally, the QBER is estimated by [84]

$$E_\mu \approx \frac{M_{E,\mu}}{M_\mu}, \tag{2.7.13}$$

where $M_{E,\mu}$ is the number of detections where a photon hit the incorrect

detector (i.e. where the outcome of Bob's measurement does not correspond to the state Alice sent).[3]

The *key rate (or secret key rate)* R is the amount of secure information, in bits, transmitted per pulse sent by Alice. It has been shown to be

$$R \geq q(R_0 + R_1 - R_{EC}), \tag{2.7.14}$$

where q is the fraction of pulses where Alice and Bob's bases agree, R_0 is the contribution from vacuum states, R_1 is the contribution from single-photon states, and R_{EC} is the number of bits Bob spends to perform error correction. Note that only single-photon or vacuum states can transmit information because multi-photon pulses are vulnerable to the PNS attack.

Refs. [27, 44, 38] provide a rigorous derivation of this formula. Here we analyze it in an informal way meant to build an intuitive understanding. Beginning with q, in the original two-basis BB84 protocol we have $q = 1/2$ because the states have a 50% probability of being in the Z or X basis, so Alice and Bob will disagree half of the time. However, it is possible to perform BB84 with a very small fraction of states in the X basis and the rest in the Z basis. This is known as the efficient BB84 protocol [40]. We then have $q \approx 1$, which is the value we shall use throughout this work.

R_0 is given by

$$R_0 = Q_0 \log_2 d, \tag{2.7.15}$$

[3] Eqs. 2.7.8 and 2.7.13 assume the gains and QBERs are independent of the basis and state. We take this for granted in this chapter for the sake of simplicity, but in Section 3.6 we will calculate them with more realistic assumptions.

where $Q_0 = Y_0$ is the gain of vacuum states and d is the system dimension. The $\log_2 d$ factor expresses the fact that a fully random d-dimensional state carries $\log_2 d$ bits of information: for example, a number written in base 4, such as 3, is written as 11 in binary, and so it requires $\log_2 4 = 2$ bits to express.

Note that the $\log_2 d$ term is only true if Alice maximizes the *Shannon entropy* of the states she sends,

$$H(X) = -\sum_x p(x) \log_2 p(x), \tag{2.7.16}$$

where X is a random state in a given basis and $p(x)$ is the probability of sending a state $|x\rangle$. This amounts to requiring all $p(x)$ to be equal.[4]

R_1 is given by

$$R_1 = Q_1 \left[\log_2 d - H_d(e_1)\right], \tag{2.7.17}$$

and the interpretation is similar to R_0, with Q_1 the gain of single-photon pulses. Here is a new term $H_d(e_1)$, where e_1 is the error associated with single-photon pulses and

$$H_d(x) = -x \log_2 \frac{x}{d-1} - (1-x)\log_2(1-x) \tag{2.7.18}$$

is the *d-dimensional modified Shannon entropy*, which arises from assuming that the error comes from a quantum depolarizing channel, generalized to d

[4] Incidentally, this is why QRNGs (quantum random number generators) are in demand: the more random the distribution is, the more information is transmitted per pulse. Further, without specialized hardware, classical computers only produce pseudo-random numbers that Eve can potentially exploit to find patterns in.

dimensions [66]. The $H_d(e_1)$ term then represents the amount of information from single-photon pulses lost due to errors.

The cost of error correction is given by

$$R_{EC} = Q_\mu H_d\left(E_\mu\right) f\left(E_\mu\right), \tag{2.7.19}$$

where the gain and QBER apply to all signal states. A higher QBER increases the number of bits used for error correction. $f(E_\mu)$ is the *error correction inefficiency*, which in our case is given by [19]

$$f(E_\mu) = 1.05. \tag{2.7.20}$$

Substituting Eqs. 2.7.15, 2.7.17 and 2.7.19 with $q \approx 1$ in Eq. 2.7.14, we have the key rate for d-dimensional systems [10]

$$R \geq Q_0 \log_2 d + Q_1 \left[\log_2 d - H_d\left(e_1\right)\right] - Q_\mu H_d(E_\mu) f(E_\mu). \tag{2.7.21}$$

Every term in this equation can be directly measured except for Q_1 and e_1, because Bob has no information about the photon number of individual pulses. If the system is characterized, Bob can use Eqs. 2.7.4, 2.7.5 and 2.7.9 to calculate Q_1 and e_1. However, in an actual QKD session they must be estimated using data from signal, decoy and vacuum pulses. To estimate the lower bound of R we must find the lower bound of Q_1 and the upper bound of e_1, which are given by [44, 10]:

$$Q_1^L = \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2}\left[Q_\nu e^\nu - \frac{\nu^2}{\mu^2} Q_\mu e^\mu - \frac{\mu^2 - \nu^2}{\mu^2} Y_0\right], \tag{2.7.22}$$

$$e_1^U = \frac{E_\nu Q_\nu \mu e^\nu - \mu e_0 Y_0}{\nu Q_1^L e^\mu}, \tag{2.7.23}$$

where μ is the intensity of signal states and ν is the intensity of decoy states. The final equation is then

$$R \geq Q_0 \log_2 d + Q_1^L \left[\log_2 d - H_d\left(e_1^U\right)\right] - Q_\mu H_d(E_\mu) f(E_\mu). \tag{2.7.24}$$

There are then two ways to calculate R:

1. The expected ("theoretical") key rate, given by characterizing the source, channel and detector (i.e. $\mu, \nu, e_{opt}, \eta_L, \eta_{Bob}, \eta_D, Y_0$) at a distance L and using the characterized parameters to plot a curve for R against L. R is calculated using Eqs. 2.7.1, 2.7.2, 2.7.4, 2.7.5, 2.7.7, 2.7.10, 2.7.9, 2.7.12 and 2.7.21. This represents the key rate in an Eve-free experiment.

2. The experimental key rate, given by the signal and decoy intensities μ, ν, the number of pulses sent by Alice N_I, the number of detections by Bob M_I and the number of detections at the wrong detector $M_{E,I}$ with intensity I where $I = \{\mu, \nu, 0\}$. R is calculated using Eqs. 2.7.1, 2.7.2, 2.7.8, 2.7.10, 2.7.13, 2.7.22, 2.7.23 and 2.7.24. This provides a single data point when plotting R against L and represents the key rate in an actual QKD session.

To make calculations easier due to the plethora of variables and functions involved, we provide here dependency graphs for both of these calculation methods. They are read in the following manner: $a \to b$ means that a is needed to calculate b. A branching arrow from a to b and c means a

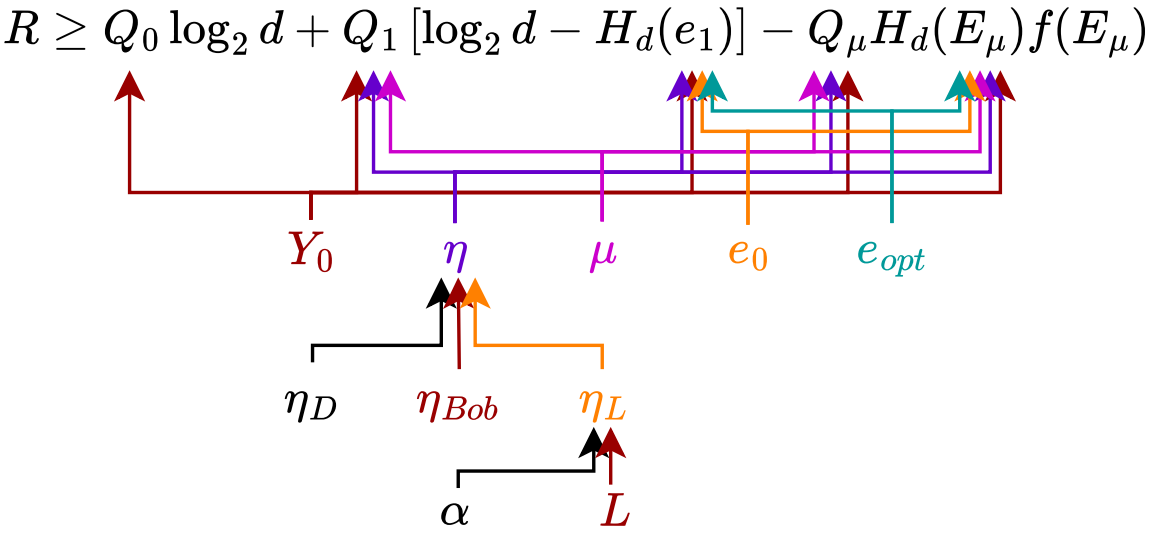


Figure 2.7.1: Dependency graph for the expected key rate.

is needed to calculate both. If a term does not have any arrows pointing towards it, it is independent and must be measured or defined.

2.8 Qudit Security Bounds

BB84 was originally proposed for two-dimensional systems. We have seen that high-dimensional systems have the advantage of encoding more information per state, but a different, less obvious advantage is their higher error tolerance.

BB84, along with a more general class of protocols using two or more MUBs, have a QBER threshold above which no secure communication is possible. The threshold depends on whether Eve is assumed to be capable of individual or coherent attacks, the dimension d, and whether one uses the 2-basis or $(d+1)$-basis protocol. Ref. [13] provides a calculation of the QBER thresholds for individual attacks and Ref. [66] provides the same for

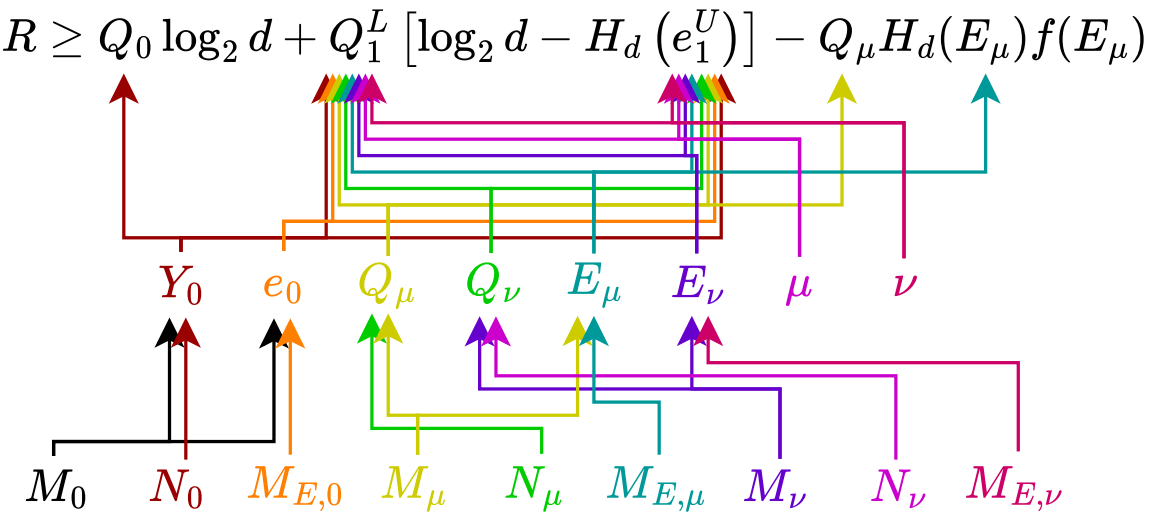


Figure 2.7.2: Dependency graph for the experimental key rate.

coherent attacks. Table 2.8.1 shows the thresholds for dimensions 2 through 5, illustrating how higher-dimensional states can tolerate higher QBERs. In this work we use the 2-basis protocol with $d = 4$, so the columns $E^{\text{coh}}_{\text{2-basis}}$ and $E^{\text{ind}}_{\text{2-basis}}$ apply.

d	$E^{\text{coh}}_{\text{2-basis}}$	$E^{\text{coh}}_{(d+1)\text{-basis}}$	$E^{\text{ind}}_{\text{2-basis}}$	$E^{\text{ind}}_{(d+1)\text{-basis}}$
2	11.00	12.62	14.64	15.64
3	15.95	19.14	21.13	22.67
4	18.93	23.17	25.00	26.66
5	20.99	25.94	27.64	29.23

Table 2.8.1: Values of the QBER E at which $R = 0$. d refers to the dimension. $E^{\text{coh}}_{\text{2-basis}}$ and $E^{\text{coh}}_{(d+1)\text{-basis}}$ refer to the QBER threshold under which the system is secure against coherent attacks, in the 2-basis protocol and $(d+1)$-basis protocol respectively. $E^{\text{ind}}_{\text{2-basis}}$ and $E^{\text{ind}}_{(d+1)\text{-basis}}$ refer to the QBER threshold under which the system is secure against individual attacks, in the 2-basis protocol and $(d+1)$-basis protocol respectively.

3 EXPERIMENTAL SETUP

3.1 State Encoding and Measurement Bases

Before studying the experiment itself, it is useful to understand how states are encoded and measured in a way that is mostly abstracted away from experimental details. In a 4-dimensional system, states are encoded either in the computational basis, given by

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \; |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \; |2\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \; |3\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \tag{3.1.1}$$

or in a basis of superpositions of computational basis states, where all four elements of the column vector are nonzero.

In our experiment, each element of the column vector represents the complex amplitude in one core of a multicore fiber (see Fig. 3.2.1). The information is encoded in the relative phases between light in each core, so we can only use bases different from the computational basis. The latter, however, is still relevant: all measurements are performed by mapping states from a given basis to the computational basis, then measuring in it, the measurement

operators being given by

$$M_i = |i\rangle \langle i| \text{ for } i = 0,1,2,3. \tag{3.1.2}$$

Computational basis measurements are performed by coupling each core to a detector, such that $|i\rangle$ will lead to a detection event in detector i for $i = \{0,1,2,3\}$.

Two MUBs, referred to as Z and X, are used to encode information. The former is defined by the states

$$|0\rangle_Z = \frac{1}{2}\begin{pmatrix}1\\1\\1\\1\end{pmatrix}, \qquad |1\rangle_Z = \frac{1}{2}\begin{pmatrix}1\\1\\-1\\-1\end{pmatrix},$$
$$|2\rangle_Z = \frac{1}{2}\begin{pmatrix}1\\-1\\1\\-1\end{pmatrix}, \qquad |3\rangle_Z = \frac{1}{2}\begin{pmatrix}1\\-1\\-1\\1\end{pmatrix}. \tag{3.1.3}$$

In this basis, readout is performed with a Hadamard matrix given by

$$M = \frac{1}{2}\begin{pmatrix}1 & 1 & 1 & 1\\ 1 & 1 & -1 & -1\\ 1 & -1 & 1 & -1\\ 1 & -1 & -1 & 1\end{pmatrix}, \tag{3.1.4}$$

such that a state $|i\rangle_Z$ will be mapped to the computational basis state $|i\rangle$, as in Eq. 3.1.1.

The X basis is defined by the states

$$|0\rangle_X = \frac{1}{2}\begin{pmatrix}-1\\1\\1\\1\end{pmatrix}, \qquad |1\rangle_X = \frac{1}{2}\begin{pmatrix}1\\-1\\1\\1\end{pmatrix},$$
$$|2\rangle_X = \frac{1}{2}\begin{pmatrix}1\\1\\-1\\1\end{pmatrix}, \qquad |3\rangle_X = \frac{1}{2}\begin{pmatrix}1\\1\\1\\-1\end{pmatrix}, \tag{3.1.5}$$

and readout is performed by applying a phase transformation $U(\pi)$ on the first element of the column vector followed by M,

$$MU(\pi) = \frac{1}{2}\begin{pmatrix}1&1&1&1\\1&1&-1&-1\\1&-1&1&-1\\1&-1&-1&1\end{pmatrix}\begin{pmatrix}e^{i\pi}&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix} \tag{3.1.6}$$
$$= \frac{1}{2}\begin{pmatrix}-1&1&1&1\\-1&1&-1&-1\\-1&-1&1&-1\\-1&-1&-1&1\end{pmatrix}, \tag{3.1.7}$$

followed by measurement in the computational basis as before.

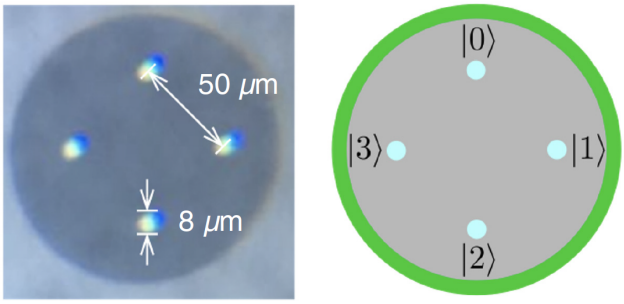


Figure 3.2.1: Left: cross-sectional image of an MCF showing distance between cores and core diameter. Right: MCF diagram with cores and their associated computational basis states. Figure reprinted from Ref. [26].

3.2 Multicore Fiber Components

Given that MCF technologies are not universally used in QKD, it is useful to study them individually to better understand the setup. This section provides an overview of the MCF technologies used in this experiment.

3.2.1 Four-Core Multicore Fiber

The 4C-MCF is the basic component through which photons propagate in the channels and is part of both Alice and Bob's setups. It is an optical fiber consisting of four cores embedded in the same cladding. Our fiber's core diameter is 8 μm and the cores are separated by 50 μm [20]. This distance is enough to make the crosstalk between cores approximately zero. The cores are single-mode when used with telecom wavelengths of 1500 to 1650 nm and their attenuation is 0.2 dB/km.

To perform modulation and measurement it is necessary to separate the cores into single-core fibers. This is done by the demultiplexer, described in Section 3.2.2.

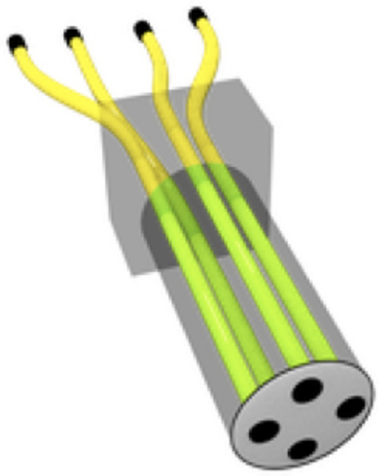


Figure 3.2.2: DMUX 3D model. Figure reprinted from Ref. [26].

3.2.2 Demultiplexer

Due to the fact that most optical fiber components are made for single-core fibers, it is often necessary to couple each core of an MCF to an SMF (single-core single-mode fiber) or vice-versa. This is accomplished by the *DMUX* (demultiplexer), shown in Fig. 3.2.2. This coupling is nearly one-to-one, with a crosstalk of < -45 dB [80]. The insertion loss from the DMUX's internal components is also small, being approximately 3.2%. However, the loss due to connectors, which varies between 0.3 and 3.1 dB at individual cores, is significant. Therefore, to implement the states in Eqs. 3.1.3 and 3.1.5, it is necessary to individually control the intensities in each SMF before insertion.

3.2.3 Four-Core Multicore Beam Splitter

The *4C-MBS* (four-core multicore beam splitter) is a device, shown in Fig. 3.2.3, consisting of an MCF that has been heated and stretched in such a way that the distance between cores is greatly reduced. With this, evanescent

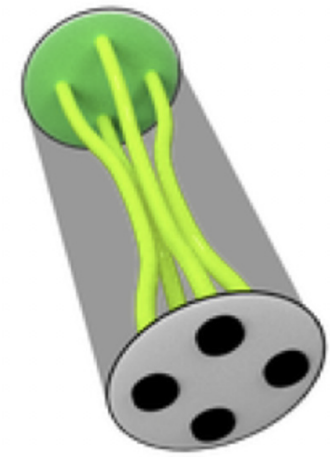


Figure 3.2.3: Four-core multicore beam splitter 3D model. Figure reprinted from Ref. [26].

light from each core can couple to any of the other cores so that it acts as an interferometer, implementing the Hadamard matrix given in Eq. 3.1.4.

In practice, the 4C-MBS cannot implement a perfect Hadamard matrix due to the different distances between its cores (one core will always have two closer neighbors and a more distant one) and fabrication imperfections. Hence a more accurate representation of its matrix is [12]

$$\tilde{M} = \begin{pmatrix} 0.499 & 0.501 & 0.499 & 0.499 \\ 0.501 & 0.491+0.08i & -0.496-0.06i & -0.498-0.01i \\ 0.499 & -0.495-0.06i & 0.498+0.03i & -0.499+0.03i \\ 0.499 & -0.499-0.01i & -0.499+0.03i & 0.499-0.01i \end{pmatrix}, \tag{3.2.1}$$

which has a fidelity of $F(\tilde{M},M) = \frac{1}{4^2}|\mathrm{Tr}(\tilde{M}^\dagger M)|^2 = 0.995 \pm 0.003$ relative to the ideal Hadamard matrix. Given its high fidelity, throughout this experiment we will assume $\tilde{M} \simeq M$.

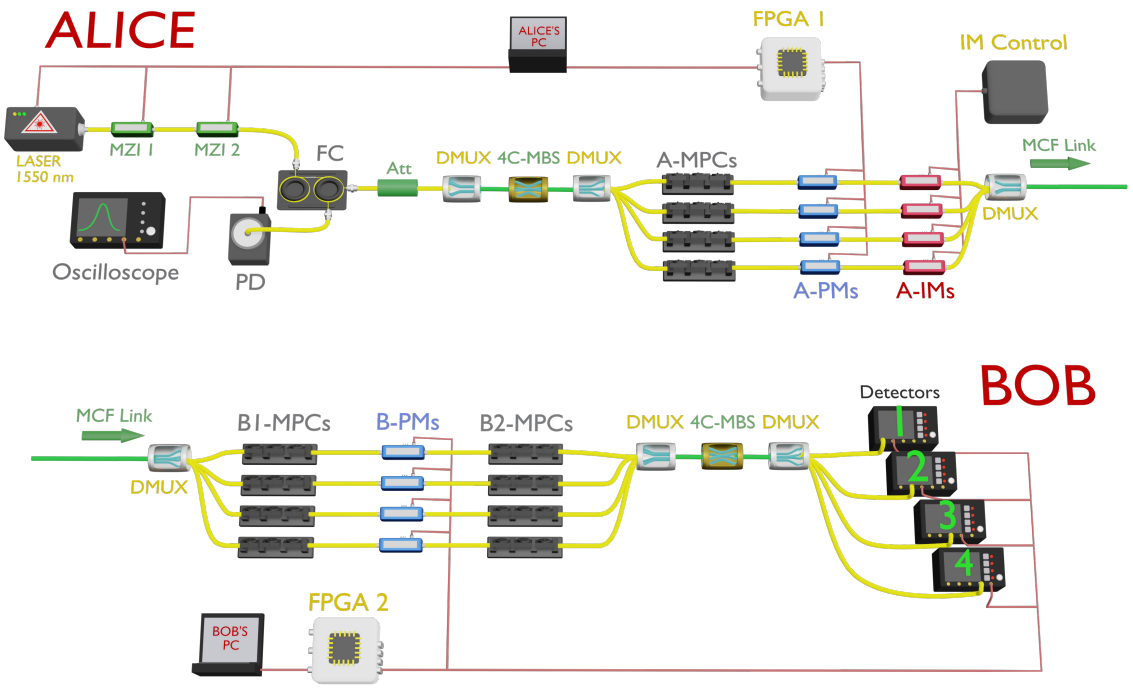


Figure 3.3.1: Experimental setup (Alice and Bob's stages). Yellow lines indicate SMFs. Green lines indicate 4C-MCFs. Red lines indicate electrical cables. Detectors are numbered from 1 to 4 in the figure for clarity, corresponding to detectors 0 through 3 in the text. FPGAs and detectors synchronized through separate cables (not shown for clarity).

3.3 Experimental Setup

Fig. 3.3.1 shows our setup. It is divided into three stages: state preparation, channel and state measurement (also known as source, channel and detection). Here we refer to these as Alice, channel, and Bob.

3.3.1 Alice

Alice's light source is a continuous, fiber-coupled 1550 nm laser. At its output there are two fiber-based MZIs (Mach-Zehnder interferometers) connected in series. Both MZIs are used to control the amplitude of the

mode. MZI 1's transmittance oscillates at 2 MHz, making it a source of pulsed light. MZI 2 implements the signal, decoy or vacuum states by changing its transmittance whenever the system prepares a state.

A fiber coupler (FC) divides the light into two fibers. One is connected to a photodiode (PD), allowing the user to monitor the pulse's shape through an oscilloscope and minimize non-pulsed amplitude. The other fiber is connected to attenuators (Att), bringing the average photon number per pulse to less than 1.

The attenuator is then connected to a DMUX, a 4C-MBS and a DMUX in reverse. The other three DMUX inputs are disconnected. This 4C-MBS distributes the light from one core to all four cores.

Then fibers then pass through the A-MPCs (Alice's manual 3-paddle polarization controllers), which approximate the effect of a quarter-wave plate, a half-wave plate and a quarter-wave plate in series. They are manually adjusted to align the polarization with the polarizers at the input ports of the A-PMs (Alice's phase modulators), maximizing transmittance.

Each of these PMs, which we will refer to as A-PM 0, A-PM 1, A-PM 2 and A-PM 3, receives two voltages, known as the bias and amplitude voltages. The bias remains constant, while the amplitude is modulated by FPGA 1 via DACs (digital-to-analog converters) and amplifiers. With this, Alice can perform a phase transformation (Eq. 2.1.6) in which the phase shift is proportional to the applied amplitude voltage.

The A-PMs are responsible for two roles:

1. They stabilize the phase noise in order to prepare the fiducial state $|0\rangle_Z$.

2. Once $|0\rangle_Z$ is prepared with an acceptable fidelity, the QKD session begins. The PMs then perform another phase transformation to prepare the selected state.

In the following two sections we will examine these processes more closely, beginning with phase noise stabilization.

3.3.1.1 Phase Noise Stabilization System

In order to prepare the fiducial (or reference) state $|0\rangle_Z$, according to Eq. 3.1.3, the relative phase between the light on all four cores must be zero.

This seldom happens naturally: even if this configuration occurs by chance at a given moment in time, changes in temperature and tension in the cores eventually shift the phases out of alignment. Realistically, at a given instant t, the state Bob receives can be written as

$$|\psi(t)\rangle = \frac{1}{2}\begin{pmatrix} e^{i\theta_0(t)} \\ e^{i\theta_1(t)} \\ e^{i\theta_2(t)} \\ e^{i\theta_3(t)} \end{pmatrix}, \tag{3.3.1}$$

where $\theta_0(t), \theta_1(t), \theta_2(t)$ and $\theta_3(t)$ are environment-induced phases in each core. Our goal is to find the phase transformation $U(\theta_i(t))$ for $i = 0, 1, 2, 3$,

written as

$$U(\theta_i) = \begin{pmatrix} e^{-i\theta_0(t)} & 0 & 0 & 0 \\ 0 & e^{-i\theta_1(t)} & 0 & 0 \\ 0 & 0 & e^{-i\theta_2(t)} & 0 \\ 0 & 0 & 0 & e^{-i\theta_3(t)} \end{pmatrix}, \tag{3.3.2}$$

such that

$$U(\theta_i)\,|\psi\rangle = |0\rangle_Z\,. \tag{3.3.3}$$

The $\theta_i(t)$ were found to be stable over periods of at least 0.1 s. The noise's frequency is then low enough that these phases can be found with an active phase noise stabilization system. The stabilization system we use is based on an adaptive-step perturb-and-observe algorithm [1]. It is a simple and robust system that deals better with nonlinearities compared to a more complex PID system and can be implemented on a Digilent Nexys A7 FPGA.

Before the algorithm begins, we choose a detector such that FPGA 1 will attempt to maximize its detection rate by changing the amplitude voltages at Alice's PMs. This is equivalent to preparing a certain state. For example, maximizing the detections I_0^{out} on detector 0 is equivalent to preparing $|0\rangle_Z$, because when Bob applies the 4C-MBS matrix M, we have

$$M\,|0\rangle_Z = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \tag{3.3.4}$$

meaning only the first core has non-zero optical power.

The algorithm to find $\theta_i(t)$ then consists of the following steps:

1. The error is defined as $\Delta = |I_k^{out} - I_{ref}|$, where I_{ref} is a reference value for the detections. If $\Delta > \tau$, where τ is a manually set value known as the *threshold*, the stabilization system is activated and proceeds to the next step. Otherwise, the algorithm stops.

2. FPGA 1 shifts the (amplitude) voltage on A-PM i. The new value is $V_i' = V_i + C \cdot \delta \cdot \text{sig}(\Delta I_{ik}^{out})$, where V is the previous voltage, C is a constant factor, δ is a manually-adjustable step size and $\text{sig}(\Delta I_{ik}^{out})$ is the sign of the change in detections compared to the previous cycle. [1] This leads to a phase shift in path i.

3. Repeat Step 2 with PM $i+1$ until all PMs have been adjusted, then advance to the next step.

4. Return to Step 1.

While the algorithm is active, the QKD session is interrupted. When $\Delta \leq \tau$,

[1] This is done so that if a change in voltage causes the counts to decrease, the algorithm will change the voltage in the opposite direction.

the algorithm is deactivated and the QKD session begins, leading to the second role of the A-PMs: state preparation, described in Section 3.3.1.2. The system will then perform measurements for 0.1 s. This period of time is defined as one *experimental realization*.

The value of τ is a crucial setting for the experiment, as it defines approximately how large of a QBER the user is willing to accept. Lowering τ decreases both the QBER and the number of measurements per minute, because the stabilization system has more difficulty lowering Δ. If τ is too low, the system will be unable to measure at all, because the dominant error will come from alignment errors (especially polarization alignment errors that decrease visibility) or dark counts (if attenuation is very high) rather than phase noise. The stabilization system can only compensate for the latter.

The system is practically unable to achieve $\Delta \leq \tau$ when $\tau < 0.05C$, where C is the total number of detections in a given experimental realization. Therefore, we have chosen $\tau = 0.05C$ as the smallest τ to perform measurements with and the main value of τ to represent our results.

3.3.1.2 State Preparation

When $\Delta \leq \tau$, the QKD session begins: FPGA 1 controls the A-PMs to prepare a state. It is selected from Alice's PC, which communicates with FPGA 1 through a USB cable. To prepare the state, FPGA 1 keeps constant the voltages used to prepare $|0\rangle_Z$ and adds another voltage to perform a phase transformation, so that the total phase applied by A-PM i is $\varphi_i - \theta_i(t)$, where φ_i for $i = \{0,1,2,3\}$ is the phase selected by Alice. FPGA 1 also

asserts a signal that enables FPGA 2 to perform a measurement. This lasts for one experimental realization, defined as a period of time lasting 0.1 s.

During this time, $2 \cdot 10^5$ pulses with the selected state are sent by Alice, while Bob measures in a given basis. Each experimental realization is treated as one sample for the purposes of calculating the average photon number, gain and QBER. The phases φ_i used to prepare each state are given in Table 3.3.3 in Section 3.3.3.1, where details of the measurement process are also discussed.

After the A-PMs, there are four A-IMs (Alice's intensity modulators) which are manually adjusted with potentiometers to equalize the intensities in each fiber. The fibers are then connected to a DMUX and coupled into an MCF, concluding Alice's section of the experiment.

3.3.2 Channels

Once the MCF leaves Alice's setup, it may go through three MCF links depending on how the experiment is configured. These are referred to as follows:

- Back-to-back: in this configuration the MCF is a short patch cord contained in the laboratory.

  - Back-to-back, simulated η_L: a special back-to-back scenario (not a physically distinct channel) where we simulate higher attenuations by decreasing the intensity with MZI 2. With this method it is possible to obtain R in an ideal environment.

- 6^{th} floor installed fiber: this MCF runs from the laboratory, which is on the 2^{nd} floor, to the 6^{th} floor of the same building (the Faculty of Physical and Mathematical Sciences at the University of Concepción) and back to the laboratory.

- Faculty of Engineering installed fiber: this MCF runs from the laboratory to the University of Concepcion's Faculty of Engineering building and back.

Channels 2 and 3 are shown in Fig. 3.3.2.

Performing experiments with installed fiber, as opposed to a large fiber spool inside the lab, is an important test of a system's capabilities. This is due to the fact that decoy state models assume [44, 10] the only effect of increasing the fiber length L is to increase η_L, decreasing Q_μ and Q_ν. This explains why R drops to zero at a certain distance: as attenuation increases, detections due to states decrease and dark counts begin to dominate detections, increasing the QBER until secure communication is impossible (see Eqs. 2.7.7 and 2.7.12 and Section 2.8). However, the optical error e_{opt} is assumed to be independent of L. Realistically, in installed fiber, mechanical and thermal noise from the environment is expected to affect the refractive index of the cores, changing the path length and their relative phases. Therefore, it is important to compare the results from installed fibers with their expected values from theory and characterization data.

As the pulses propagate through the channels, they are attenuated by a factor η_L. The attenuation and total length L of each channel are given

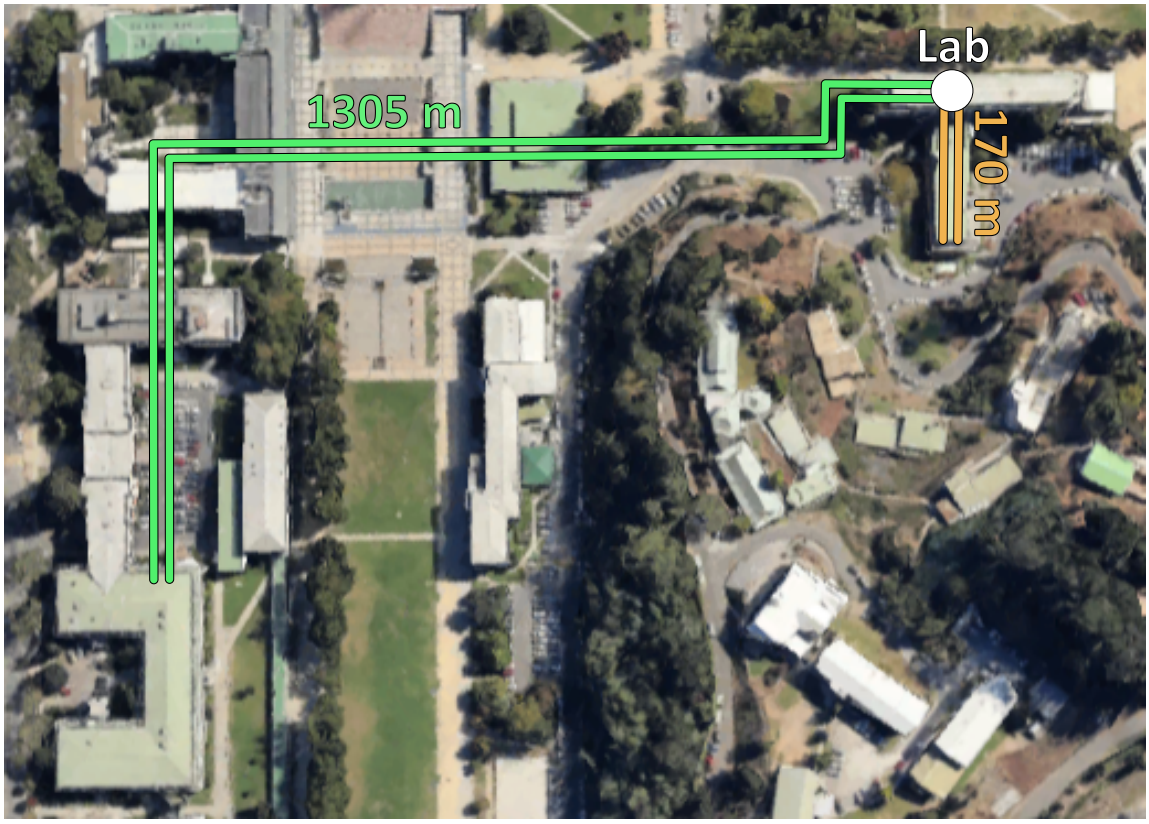


Figure 3.3.2: Map of installed fibers at the University of Concepción's campus at Concepción, Chile. Orange lines indicate the 6$^{\text{th}}$ floor channel. Green lines indicate the Faculty of Engineering channel. Numbers indicate the total path length including return paths. Vertical sections of fiber from the laboratory to the 6$^{\text{th}}$ floor and Faculty of Engineering buildings not shown.

Channel	η_L (dB)	L (m)
Back-to-back	2.160	< 10
Back-to-back, simulated η_L	Adjustable	< 10
6$^{\text{th}}$ floor	9.363	170
Faculty of Engineering	10.695	1305

Table 3.3.1: Channels and their corresponding values of η_L (including the insertion losses from Bob's DMUX) and L (including the return path). η_L obtained by averaging the attenuation associated with each MCF core.

in Table 3.3.1. In all three of them, the main sources of loss are not the fibers themselves (which have an attenuation of only ~ 0.2 dB/km) [20] but their connections and fusions. Connections increase losses no matter the type of fiber, but in MCFs this difficulty is more noticeable, as the cores are not centered on the cladding axis and misalignments can cause light to have large insertion losses, or even core-dependent losses. Therefore, whenever one connects two MCFs, they must be manually rotated to maximize transmittance. Fusions likewise increase losses and care must be taken to align the cores before fusing them.

All these factors mean that η_L is uncorrelated with L in these channels. For this reason, in this work we have chosen to plot R as a function of η_L rather than L. Furthermore, because η_L is dependent on the core to some degree, we have measured the attenuation associated with each core and taken η_L as their average.

In the following two sections we will describe the path taken by each installed fiber and the losses at each point.

3.3.2.1 6^{th} Floor Installed Fiber

Fig. 3.3.3 shows the path losses at each stage of the 6^{th} floor channel, measured by connecting a laser to input 1 of the DMUX and disconnecting all other inputs. Room 204-A is where Alice and Bob's setups are located in the Faculty of Physical and Mathematical Sciences. Rooms 204-B and 203 are neighboring rooms. Once the fiber leaves Room 203, it passes through the building's structure to the 6^{th} floor. It is then connected to another fiber that runs through the same route in the opposite direction, returning to Room

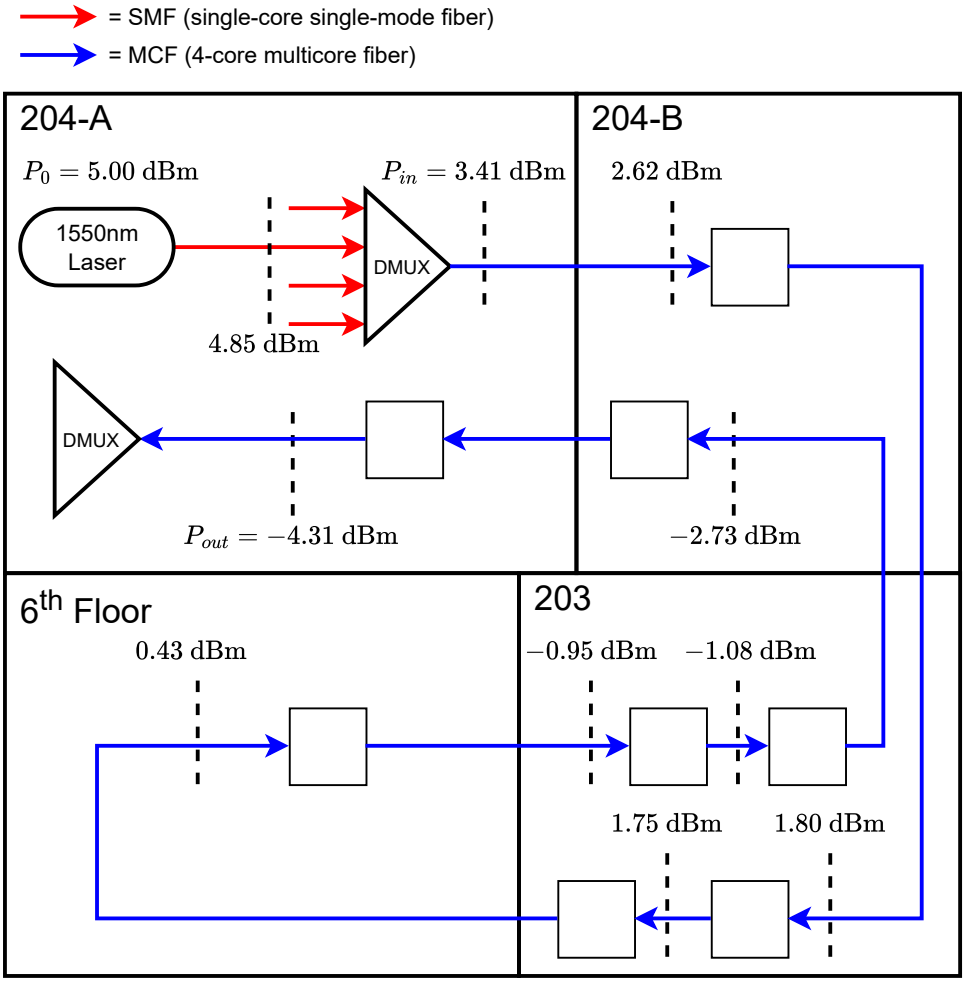


Figure 3.3.3: Path of the fiber running from the laboratory to the 6$^{\text{th}}$ floor and back with losses (measured with core 1 of the MCF) at each connection. White squares represent connections. Numbers at dotted lines represent the intensities at each connection, taken using a laser to characterize the channel. Paths not to scale and (except for connections) do not represent the actual geometry of the fiber.

203. Notably, the paths between Room 203 and the 6th floor and back are by far the longest segments in this channel even though their losses are only 2.70 dB in total, whereas the total attenuation is 9.363 dB, illustrating the earlier argument for η_L being uncorrelated to L.

3.3.2.2 Faculty of Engineering Installed Fiber

Fig. 3.3.4 shows the path losses at each stage of the Faculty of Engineering channel, measured by connecting a laser to input 1 of the DMUX and disconnecting all other inputs. Rooms 204-A, 204-B and 203 are the same as described in Section 3.3.2.1.

In this path segment, the fiber passes through the building's structure, then underground across the university plaza and into the 2nd floor of the Faculty of Engineering building. It is then connected to another fiber running through the same route, returning to Room 203.

This channel represents more realistically the conditions of a fiber network in a city. The plaza (Fig. 3.3.5) is exposed to the elements and is regularly crossed by cars and large numbers of people, making it a useful location to evaluate the effects of the environment on the stabilization system and the fidelity distribution.

3.3.3 Bob

Bob's setup is located in the same room as Alice's. The incoming MCF is connected to a DMUX, coupling light from each core into a single-core fiber. The DMUX, treated as part of the path, adds 1.22 dB to η_L. The B1-MPCs (Bob's first MPC set) are then used to adjust the incoming light's

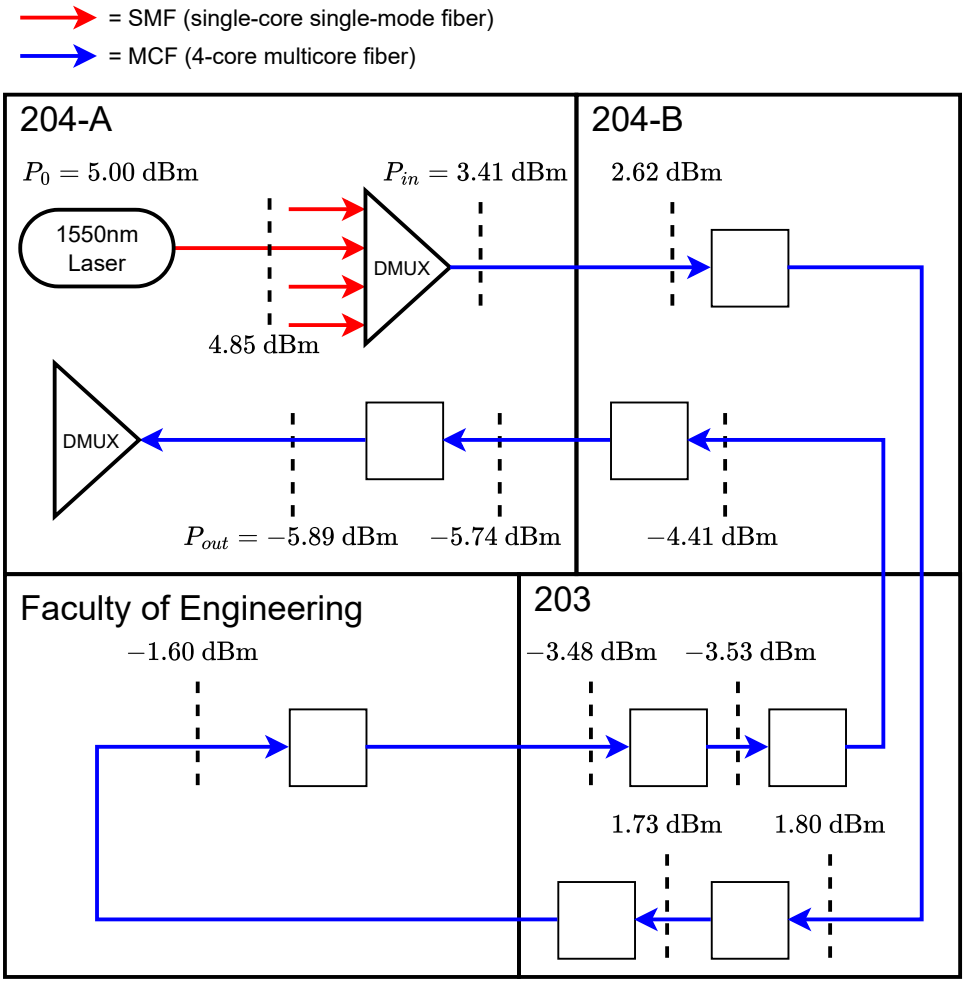


Figure 3.3.4: Path of the fiber running from the laboratory to the Faculty of Engineering and back with losses (measured with core 1 of the MCF) at each connection. White squares represent connections. Numbers at dotted lines represent the intensities at each connection, taken using a laser to characterize the channel. Paths not to scale and (except for connections) do not represent the actual geometry of the fiber.

Figure 3.3.5: University plaza. Figure reprinted from Ref. [23].

polarization to couple the light into the B-PMs (Bob's PMs) that follow. The B-PMs are controlled by FPGA 2 to implement a phase transformation, changing the measurement basis.

They are followed by the B2-MPCs (Bob's second MPC set), which play the crucial role of equalizing the polarization on all four fibers, erasing which-path information in order to maximize the interferometric visibility. After this, the four fibers are then coupled to a DMUX, a 4C-MBS, and another DMUX. Bob's PMs, together with the connection losses from these two DMUXes and a small loss due to the 4C-MBS, altogether attenuate the pulses by a factor of $\eta_{Bob} = 5.755$ dB.

Each of the DMUX outputs is connected to a time-gated idQuantique ID210 InGaAs *SPAD* (single-photon avalanche diode) detector triggered by a signal from FPGA 1. The B-PMs together with the 4C-MBS and detectors are capable of measuring in any MUB in a 4-dimensional Hilbert space. Each detector has a separately configured delay and gate width, the former due to slightly different path lengths after the 4C-MBS and the latter due to different response curves when plotting the detection rate as a function of laser intensity.

The detectors are configured for an efficiency $\eta_{det} = 7.5\%$. Although it can be set higher, the rate of dark counts increases quickly with the efficiency, and in this experiment it is more advantageous (in terms of increasing the maximum distance) to lower dark counts as much as possible rather than decreasing losses.

Y_0	f	e_{opt}	η_L	η_{Bob} (dB)	η_D	μ	ν
$1.52 \cdot 10^{-5}$	1.05	See Table 3.4.1	See Table 3.3.1	5.755	7.5%	See Table 3.5.1	0.1

Table 3.3.2: Experimental parameters. e_{opt} is setting-dependent (see Section 3.4). η_L is channel-dependent (see Section 3.3.2). μ is both setting and channel-dependent.

The parameters of this experiment are summarized in Table 3.3.2. Some of them take different values depending on the channel and experimental setting. The optical error e_{opt} depends on the threshold τ (see Section 3.3.1.1) and the experimental setting (Section 3.4), the path transmittance η_L depends on the selected channel (Section 3.3.2), and the signal state intensity μ must be numerically optimized to maximize the key rate R based on all the other parameters (Section 3.5).

3.3.3.1 Measurement Process

As stated in Section 3.3.1.2, when the stabilization algorithm successfully achieves $\Delta \leq \tau$, an experimental realization lasting 0.1 s begins. During this time, Alice prepares a selected state by modulating the phase at each A-PM, while Bob performs measurements in a basis he selects. To change the measurement basis, FPGA 2 applies a voltage to the B-PMs through DACs and amplifiers in order to implement a phase transformation. The required phases to prepare states and measure in each basis are given in Table 3.3.3.

The transformations required to measure in each basis are shown in Table 3.3.3. When measuring in the Z basis, all of the phases are equal to 0 and the only operator acting on the states is the 4C-MBS operator from Eq. 3.1.4, so that none of Bob's PMs are activated. Measurements in the X basis require a

State	φ_0	φ_1	φ_2	φ_3	α_0	α_1	α_2	α_3
$\|0\rangle_Z$	0	0	0	0	0	0	0	0
$\|1\rangle_Z$	π	π	0	0	0	0	0	0
$\|2\rangle_Z$	π	0	π	0	0	0	0	0
$\|3\rangle_Z$	0	π	π	0	0	0	0	0
$\|0\rangle_X$	π	0	0	0	π	0	0	0
$\|1\rangle_X$	0	π	0	0	π	0	0	0
$\|2\rangle_X$	0	0	π	0	π	0	0	0
$\|3\rangle_X$	π	π	π	0	π	0	0	0

Table 3.3.3: Phases implemented at the PMs on Alice and Bob's sides. For $i = \{0,1,2,3\}$, φ_i is implemented by A-PM i to prepare a given state and α_i is implemented by B-PM i in order to measure in the Z or X bases. Bob is assumed to measure in the same basis in which a state was prepared.

phase shift of $\alpha_0 = \pi$ in B-PM 0 to implement the matrix in Eq. 3.1.7. Every PM added increases errors due to electronic noise and alignment errors; given that it only requires a single PM, this choice of X basis introduces the least amount of error.

3.4 Experimental Settings

Depending on what one wishes to determine, the choice of certain experimental parameters may be different. Two of them, in particular, are most relevant:

- The threshold τ used for the stabilization system. Our choice of this parameter determines the average QBER and number of experimental realizations per minute.

- The optical error e_{opt} taken from characterization data. Each value of e_{opt} leads to a different optimal μ as well as an expected R.

Throughout this experiment we have considered four possible settings:

Setting 1. $\tau = 0.05C,\ e_{opt} = \min\left(e_{opt}^{char}\right)$. This consists of setting the threshold to 5% of the total counts C of a given experimental realization (see Section 3.3.1.1) and assuming e_{opt} to be the smallest value in our sample of optical error from characterization, e_{opt}^{char}. This represents the overall best-case scenario for our system: an ideal phase-noise-free, fluctuation-free experiment.

Setting 2. $\tau = 0.05C,\ e_{opt} = \overline{e_{opt}^{char}}$. In this setting τ is the same as above, but e_{opt} is taken as the average value of e_{opt}^{char}. This is a realistic scenario that represents the conditions of an actual QKD session.

Setting 3. $\tau = 0.10C,\ e_{opt} = \min\left(e_{opt}^{char}\right)$. Similar to scenario 1, but with a threshold of $\tau = 10\%$ of the total counts. Used to compare the change in experimental realizations per minute and QBER relative to Setting 1.

Setting 4. $0.10C,\ e_{opt} = \overline{e_{opt}^{char}}$. Similar to Setting 2, but with a threshold of 10% of the total counts. Used to compare the increase in experimental realizations per minute and QBER relative to Setting 2.

These are summarized in Table 3.4.1 and we will be using the setting numbers as shorthand for each setting throughout this thesis. Settings 1 and 2 were used for our main results.

Setting	τ	e_{opt}	e_{opt} calculation method
1	$0.05C$	4.17%	Best case scenario
2	$0.05C$	11.21%	Statistical mean
3	$0.10C$	4.17%	Best case scenario
4	$0.10C$	13.12%	Statistical mean

Table 3.4.1: Experimental settings and their corresponding values of τ and e_{opt}.

3.5 Intensity Optimization

To find the optimal intensities $\mu_{optimal}$ and $\nu_{optimal}$ for signal and decoy states respectively, we fed characterization data to the formula for R and optimized $R(\mu, \nu, \eta_L)$ for a given experimental setting and η_L.

For $\eta_L = 10.695$ dB (as in the case of the Faculty of Engineering installed fiber), the optimization landscape is shown in Fig. 3.5.1. One can see that the smoothness of the function and lack of local minima and make the optimization straightforward.

The figure also shows that $\nu_{optimal}$ (in an unrestricted optimization) is typically very small (less than 10^{-7}). From an experimentalist's point of view, this poses a problem: the algorithm assumes one can determine ν, E_ν and Q_ν perfectly, but as ν decreases and channel losses increase, the intensity fluctuations degrade the accuracy of these measurements severely due to

both coherent state fluctuations and dark counts, affecting the accuracy of R. In order to compromise between optimization and experimental feasibility, we set the lower bound of $\nu_{optimal}$ to 0.1 in the optimization algorithm. In practice, this amounts to fixing $\nu_{optimal} = 0.1$. As Figs. 3.5.1 and 4.1.1 show, this lowers the experimental R, but not by a large factor, justifying the compromise.

As for $\mu_{optimal}$, it is dependent on characterization data and η_L. The optimal signal intensity for each setting and channel used in this experiment is given in Table 3.5.1.

Setting	Channel	$\mu_{optimal}$
1	Back-to-back	0.58
1	6^{th} floor installed fiber	0.57
1	Faculty of Engineering installed fiber	0.56
1	Back-to-back, simulated $\eta_L = 18$ dB	0.48
2	Back-to-back	0.24
2	6^{th} floor installed fiber	0.23
2	Faculty of Engineering installed fiber	0.23
2	Back-to-back, simulated $\eta_L = 14$ dB	0.20
3	Back-to-back	0.58
3	6^{th} floor installed fiber	0.57
3	Faculty of Engineering installed fiber	0.56
4	Back-to-back	0.16
4	6^{th} floor installed fiber	0.15
4	Faculty of Engineering installed fiber	0.15

Table 3.5.1: Optimized intensities $\mu_{optimal}$ of signal states used in this experiment. Optimizations performed with the restriction $\nu = 0.1$.

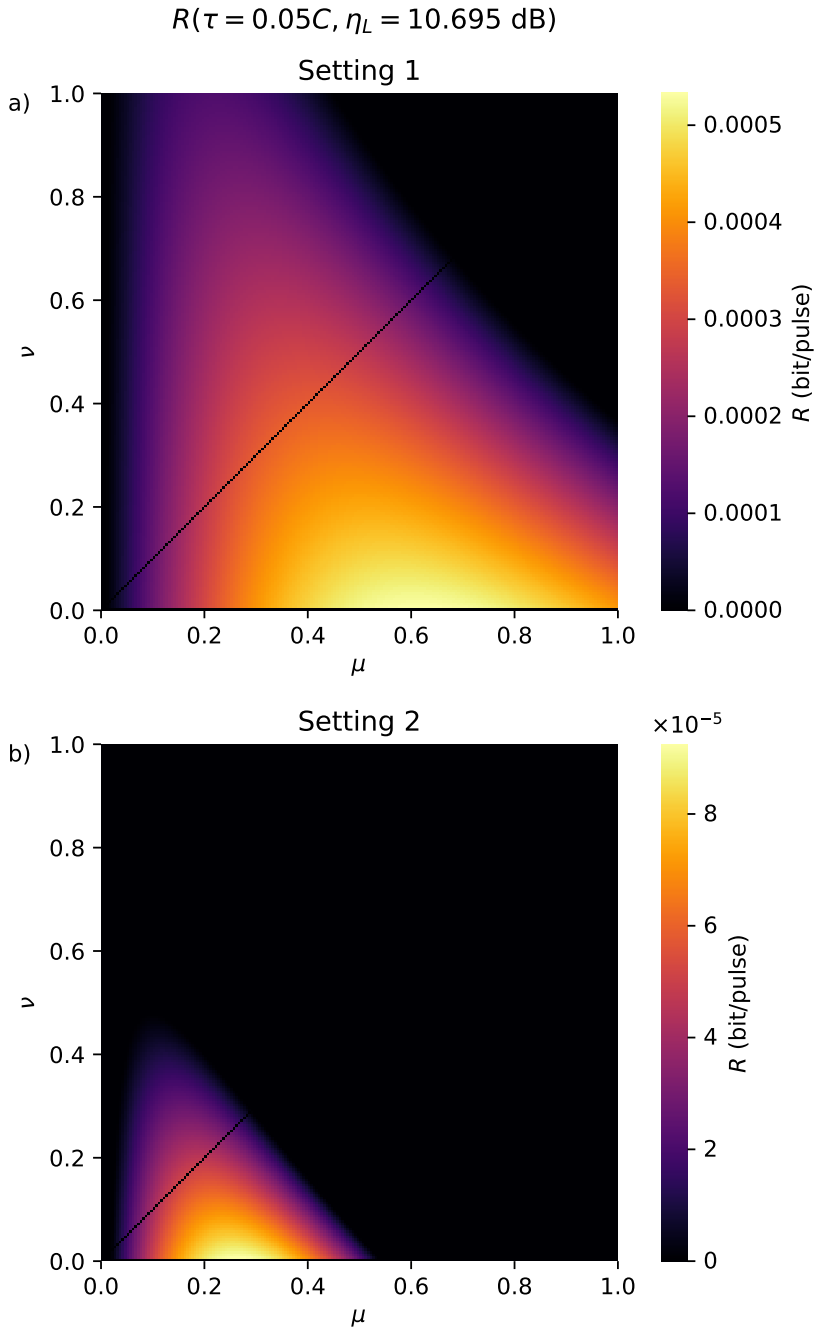


Figure 3.5.1: $R(\mu, \nu)$ in the $\tau = 0.05C$ case for Settings 1 and 2, with attenuation equal to the engineering faculty installed fiber. Data near the points where $\mu = \nu$ was removed due to high numerical errors in the calculation of R in this area.

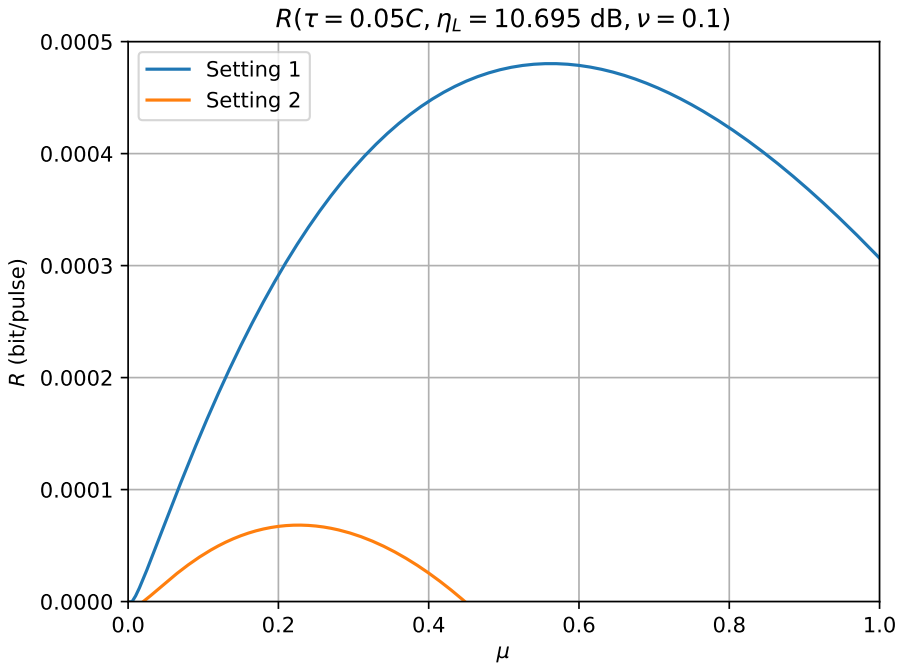


Figure 3.5.2: Cross section of Fig. 3.5.1 in the $\nu = 0.1$ abscissas of both insets.

Fig. 3.5.2 shows a slice of Fig. 3.5.1 at the abscissa $\nu = 0.1$ in both Settings 1 and 2. This figure illustrates the stability against errors in μ: for example, in Setting 1, an error of 0.1 leads to a decrease in R of less than 20% of its highest attainable value. It also illustrates the dependence of $\mu_{optimal}$ on e_{opt}: a lower optical error increases the optimal signal intensity.

Fig. 3.5.3 shows the dependence of $\mu_{optimal}$ and $\nu_{optimal}$ on η_L. One can see that $\nu_{optimal}$ is constant, while $\mu_{optimal}$ decreases gradually and drops to 0 when there is no value such that $R > 0$. In general μ must be higher than the values of ~ 0.15 commonly used in QKD experiments. Further, when $\nu_{optimal}$ is fixed to 0.1, $\mu_{optimal}$ is lower than in the unrestricted case, showing that the results of μ and ν are not independent.

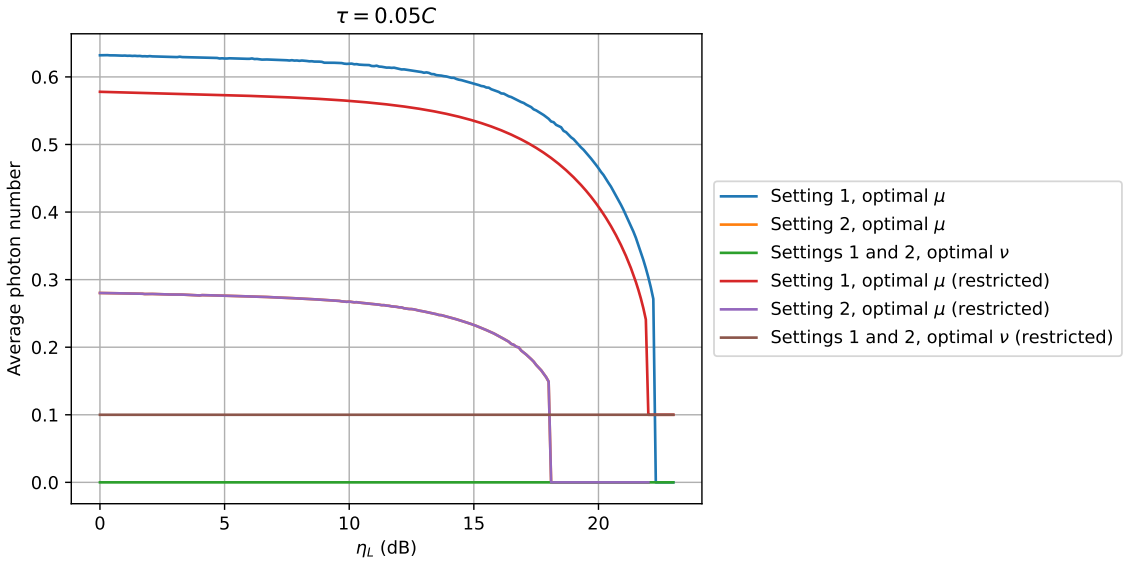


Figure 3.5.3: Optimal values of μ and ν as functions of η_L, in both unrestricted and restricted ($\nu > 0.1$) optimizations.

Figs. 3.5.4, 3.5.5 and 3.5.6 are the counterparts of Figs. 3.5.1, 3.5.2 and 3.5.3 for Settings 3 and 4. The same analysis applies.

3.6 Determination of Experimental Values

Decoy state security proofs make certain assumptions about the parameters of a system, such as all states and bases of pulses with a given intensity having the same gain and QBER. In practice, factors such as statistical fluctuations, imperfect fiber connections, and differences in state preparation can contradict these assumptions. Although the security proofs are still valid, some adaptation of the formulas is needed. In this section, we explicitly write out the equations used to calculate experimental parameters in terms of detector counts.

In a given experimental realization, Alice prepares a state $|i\rangle_B$ with $i \in$

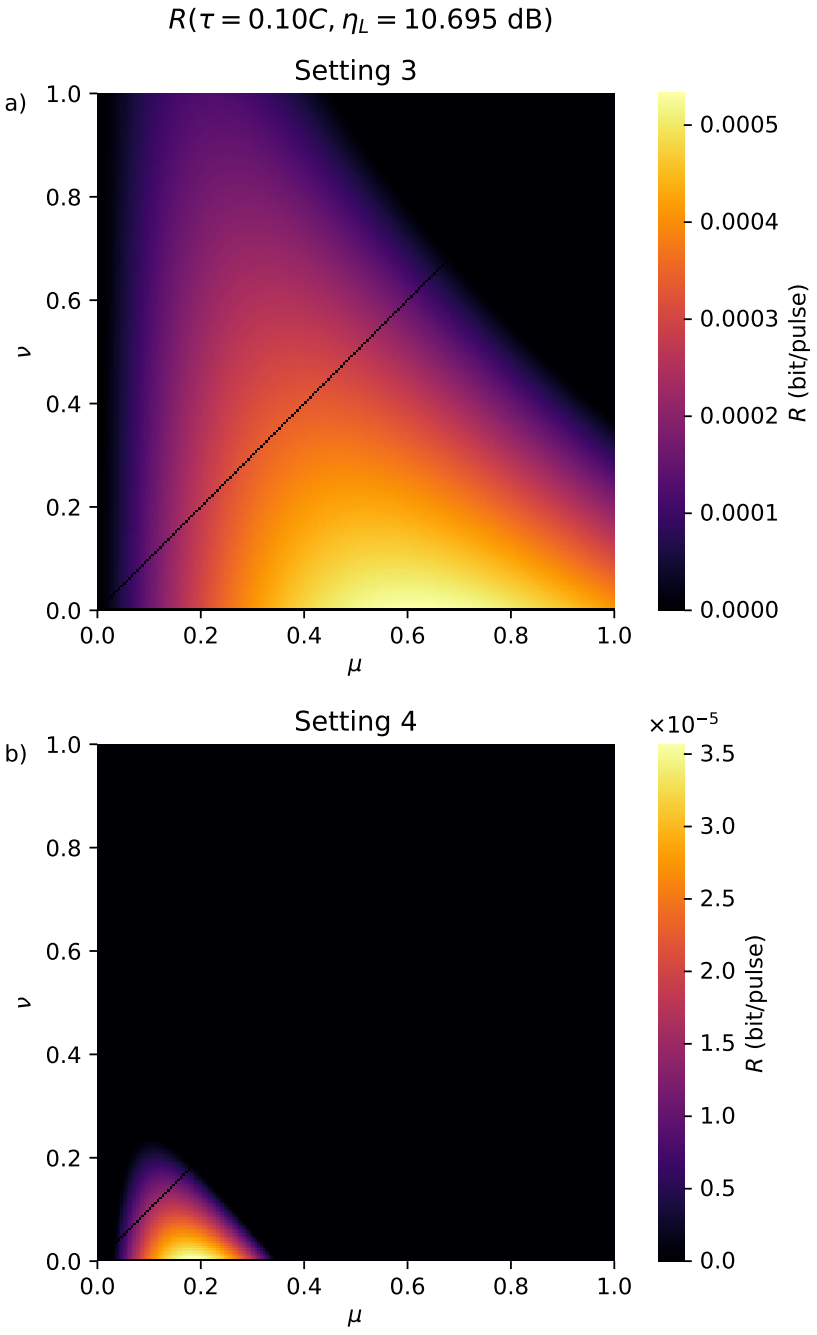


Figure 3.5.4: $R(\mu, \nu)$ in the $\tau = 0.10C$ case for Settings 1 and 2, with attenuation equal to the engineering faculty installed fiber. Data near the points where $\mu = \nu$ was removed due to high numerical errors in the calculation of R in this area.

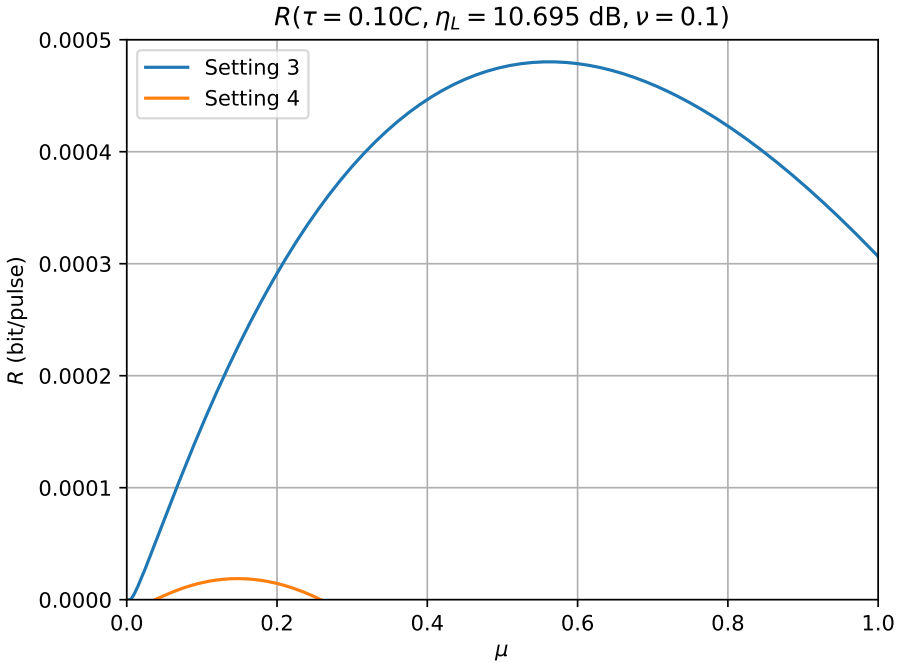


Figure 3.5.5: Cross section of Fig. 3.5.4 in the $\nu = 0.1$ abscissas of both insets.

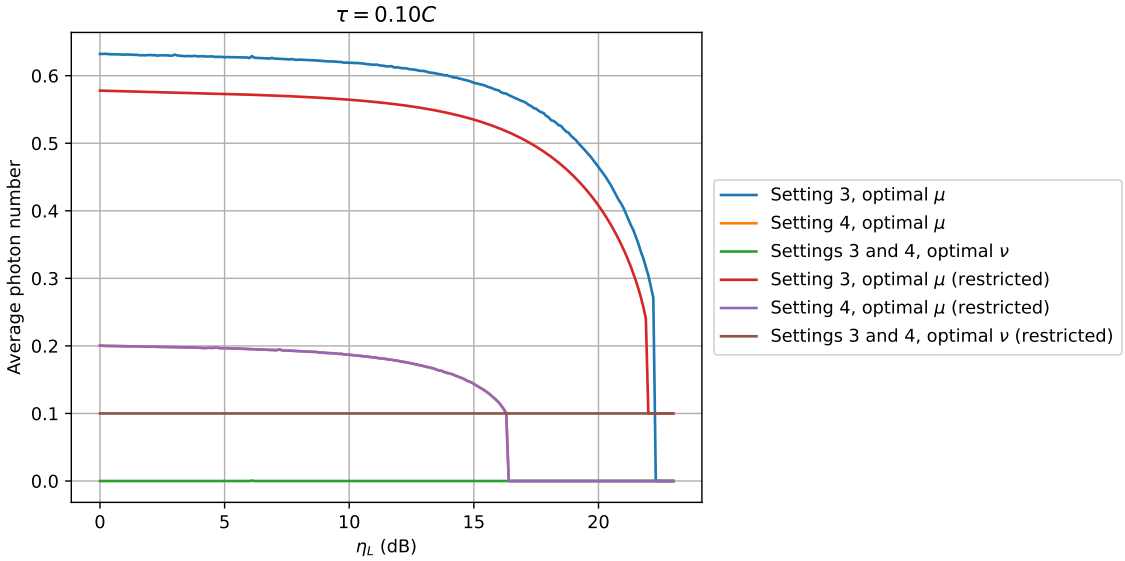


Figure 3.5.6: Optimal values of μ and ν as functions of η_L, in both unrestricted and restricted ($\nu > 0.1$) optimizations.

$\{0,1,2,3\}$, basis $B \in \{Z,X\}$, and intensity $I \in \{\mu,\nu,0\}$, and sends it to Bob. The total number of detections by Bob is given by $M_{I,B,i}$ and the number of detections at the incorrect detectors is given by $M_{E,I,B,i}$. The QBER associated with this state and realization is then [84]

$$E_I\left(|i\rangle_B\right) = \frac{M_{E,I,B,i}}{M_{I,B,i}}. \tag{3.6.1}$$

We shall see later that depending on the setting (see Section 3.4), we may average this QBER over many experimental realizations or select the best value out of all of them. Either case provides a value of $E_I\left(|i\rangle_B\right)$ to be used for calculations.

When selecting the best (lowest) value, the overall QBER of this intensity is then its average across all bases and states.

$$E_I = \frac{1}{8}\sum_{B\in\{Z,X\}}\sum_{i=0}^{3} E_I\left(|i\rangle_B\right), \tag{3.6.2}$$

with the fidelity being defined in terms of the QBER for the signal state

$$F = 1 - E_\mu. \tag{3.6.3}$$

When averaging over many experimental realizations, given that some states may be prepared more frequently than others, the QBER is given by the weighted average

$$E_I = \frac{\sum_{B\in\{Z,X\}}\sum_{i=0}^{3} N_{I,B,i} E_I\left(|i\rangle_B\right)}{\sum_{B\in\{Z,X\}}\sum_{j=0}^{3} N_{I,B,j}}, \tag{3.6.4}$$

where $N_{I,B,i}$ is the number of pulses sent by Alice in state $|i\rangle_B$ with intensity I.

When selecting the gain's best (highest) value, it is similarly defined as [84]

$$Q_I\left(|i\rangle_B\right) = \frac{M_{I,B,i}}{N_{I,B,i}}, \tag{3.6.5}$$

$$Q_I = \frac{1}{8}\sum_{B\in\{Z,X\}}\sum_{i=0}^{3} Q_I\left(|i\rangle_B\right). \tag{3.6.6}$$

As in Eq. 3.6.4, when averaging over experimental realizations, the gain is given by its weighted average

$$Q_I = \frac{\sum_{B\in\{Z,X\}}\sum_{i=0}^{3} N_{I,B,i} Q_I\left(|i\rangle_B\right)}{\sum_{B\in\{Z,X\}}\sum_{j=0}^{3} N_{I,B,j}}. \tag{3.6.7}$$

3.7 Error Calculations

In this section we describe the methods used to calculate the errors of the experimentally determined variables: Y_0, η_L, η_{Bob}, η_{det}, Q_μ, Q_ν, E_μ and E_ν.

The error of Y_0 is calculated in the usual way, by taking the standard deviation of the samples of Y_0. As for the η attenuation factors, given that multiple samples from power meters resulted in the same values, the error is taken to be the smallest digit of the display. When taking its upper bound this results in $\sigma_\eta = 0.02\eta$.

Depending on the setting, the errors of the gains and QBERs for each intensity are calculated in one of two ways. In the case of Settings 2 and 4, where their values are the sample means, the errors of the gains (Eq. 3.6.1) and QBERs (Eq. 3.6.5) are their sample standard deviations. Given that eight states are prepared and measured in total, the gains and QBERs of each state are averaged over many experimental realizations and their errors are propagated accordingly in Eqs. 3.6.4 and 3.6.7.

However, in Settings 1 and 3, the sample has only one data point (the lowest QBER point). The source of the error is then different from Settings 2 and 4: it is due to Poissonian statistics of detector counts rather than phase noise. The Poisson distribution at a detector i is uniquely determined by its mean counts C_i, and its standard deviation is $\sigma_{C_i} = \sqrt{C_i}$. Therefore, we can propagate this error in Eqs. 3.6.1 and 3.6.5, with

$$M_{I,B,i} = \sum_{j=0}^{3} C_j, \tag{3.7.1}$$

$$M_{E,I,B,i} = \sum_{j=0, j\neq i}^{3} C_j, \tag{3.7.2}$$

to obtain the gain and QBER errors.

4 RESULTS AND DISCUSSION

4.1 Key Rates

Fig. 4.1.1 shows the key rates in the $\tau = 0.05C$ case. This is the main result of this thesis and contains the data from Settings 1 and 2. In both cases, there is a solid curve showing the expected R given the restriction $\nu = 0.1$ and a dashed curve showing the asymptotic R representing the highest achievable value of R. The asymptotic R was found to be numerically equal to the R obtained by optimizing μ and ν with no restrictions. Given that we set $\nu = 0.1$, the solid lines represent the expected R in our experiment.

The back-to-back data points include data from $\eta_L = 2.16$ dB and, with simulated attenuation, $\eta_L = 18$ dB (in Setting 1) or $\eta_L = 14$ dB (in Setting 2). The points showing installed fiber data include both 6^{th} floor and Faculty of Engineering data (η_L given in Tab. 3.3.1).

Multiplying the key rate per pulse by the clock rate, we arrive at the results in Tab. 4.1.1. The maximum ranges for Settings 1 and 2, taking the fiber's attenuation to be 0.2 dB/km, are 107 km and 84 km respectively. The

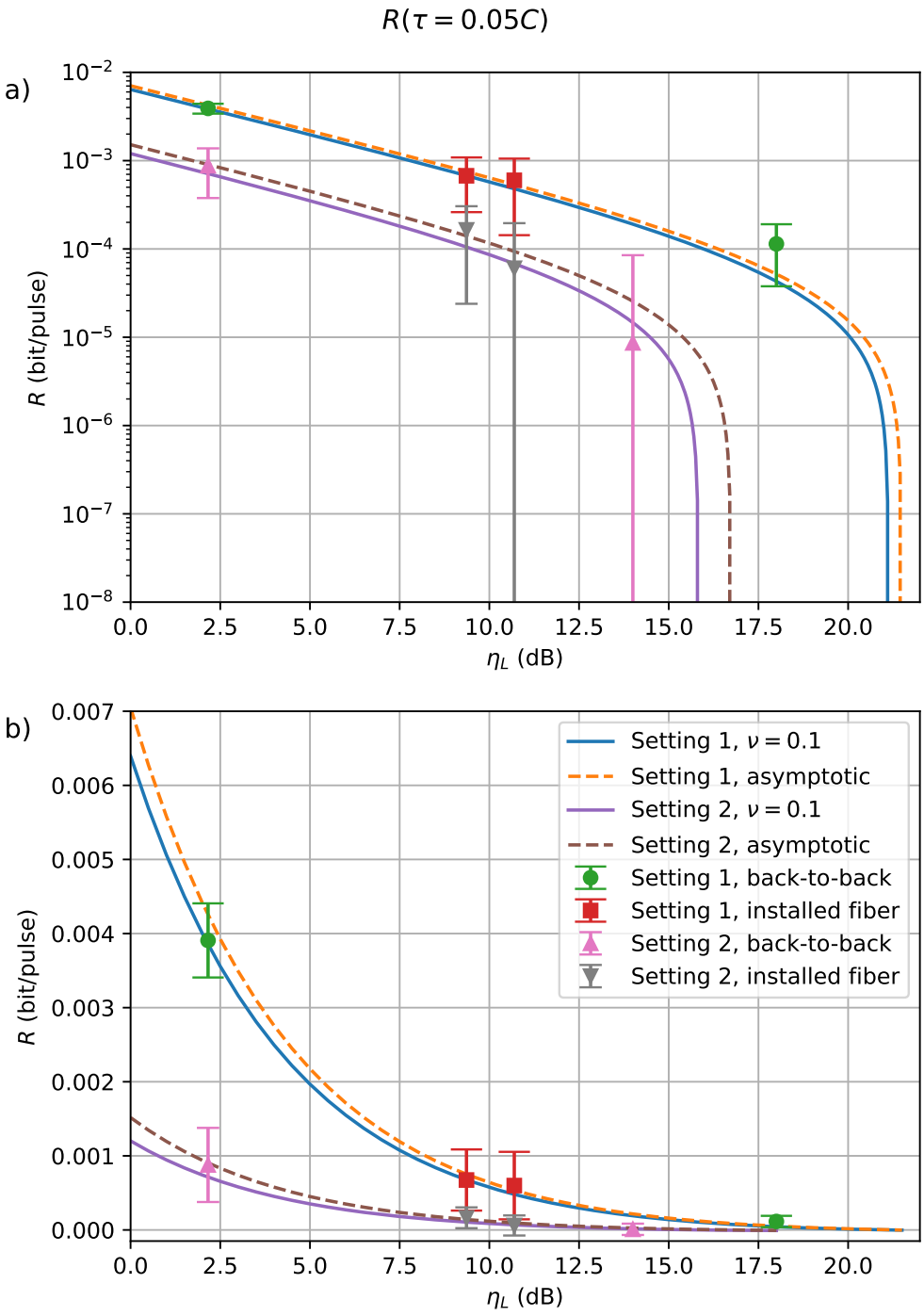


Figure 4.1.1: Key rates in the $\tau = 0.05C$ settings. Insets a) and b) show the same data in linear and log scales respectively. Legend on inset b) applies to both insets. Curves show expected values.

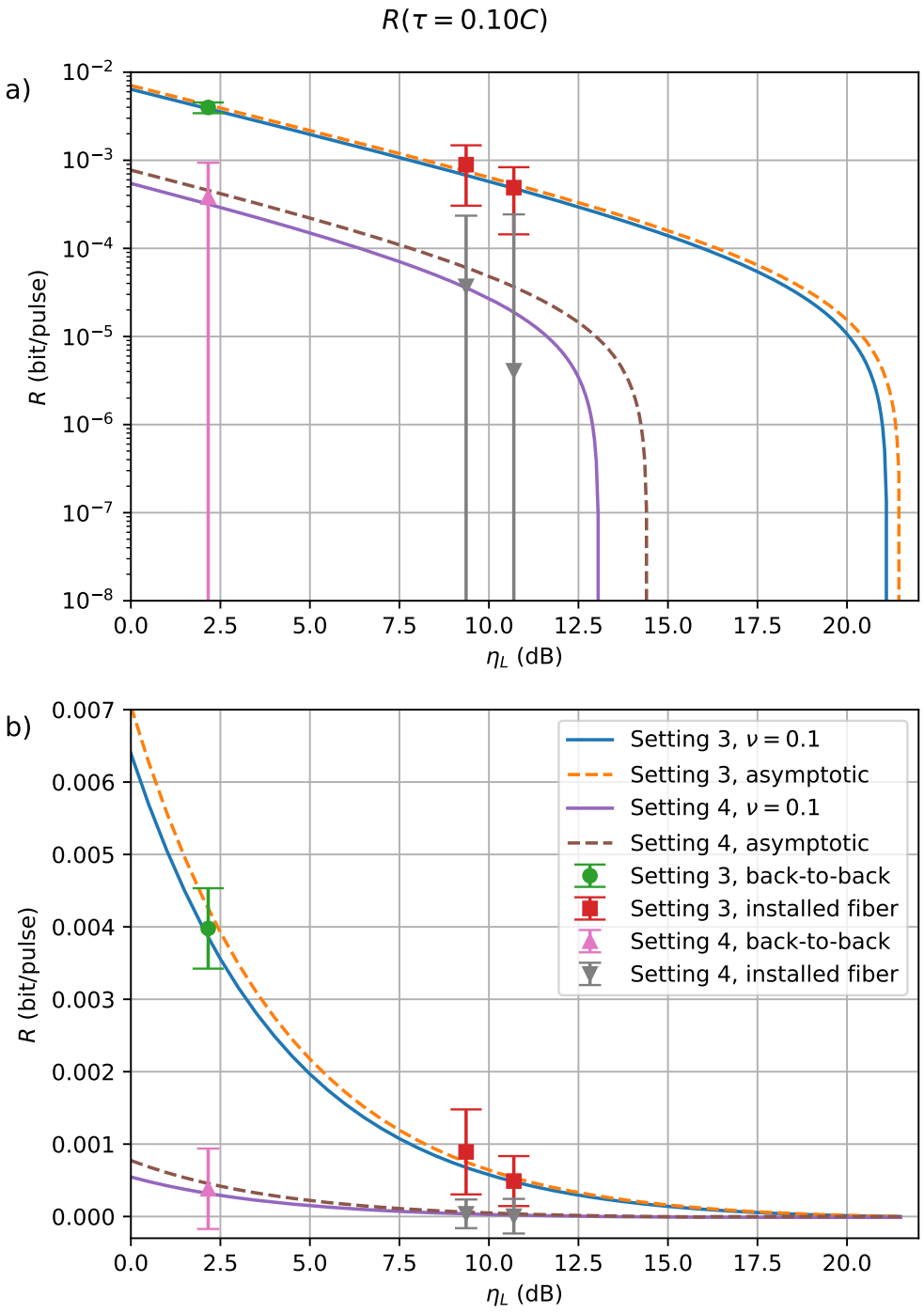


Figure 4.1.2: Key rates in the $\tau = 0.10C$ settings. Insets a) and b) show the same data in linear and log scales respectively. Legend on inset b) applies to both insets. Curves show expected values.

Channel	τ	Max. R (kbit/s)	Avg. R (kbit/s)
Back-to-back	0.05	7.815	1.754
6^{th} floor	0.05	1.348	0.329
Faculty of Engineering	0.05	1.197	0.121
Back-to-back	0.10	7.957	0.766
6^{th} floor	0.10	1.784	0.074
Faculty of Engineering	0.10	0.979	0.008

Table 4.1.1: Key rates for each channel and value of τ.

system is able to transmit a 256-bit key (for use in the AES-256 protocol, for example) in 2.1 s through the Faculty of Engineering channel, through an attenuation equivalent to 53 km of 0.2 dB/km-attenuated fiber.

The key rate error bars σ_R decrease with η_L, as shown in inset b) of Fig. 4.1.1, although inset a) shows that the relative error σ_R/R increases. This is due to the fact that higher η_L decreases the detector counts. Due to Poissonian statistics, the ratio between the counts' standard deviation and mean increases when counts decrease, which affects both the QBER and gain errors, as shown in Figs. 4.2.1 and 4.3.1. Error bars are rarely included in key rate plots in other experiments, and when they are, it is often in the low η_L regime where they remain small [10, 16, 83]; our error bars are therefore not especially high compared with other works.

Although the results show very good agreement with the expected R for $\nu = 0.1$, a noticeable phenomenon happens in Setting 1 when $\eta_L = 18$ dB. In this regime, R is within the error bars but well above the expected value. In Section 4.2 we will study this more closely.

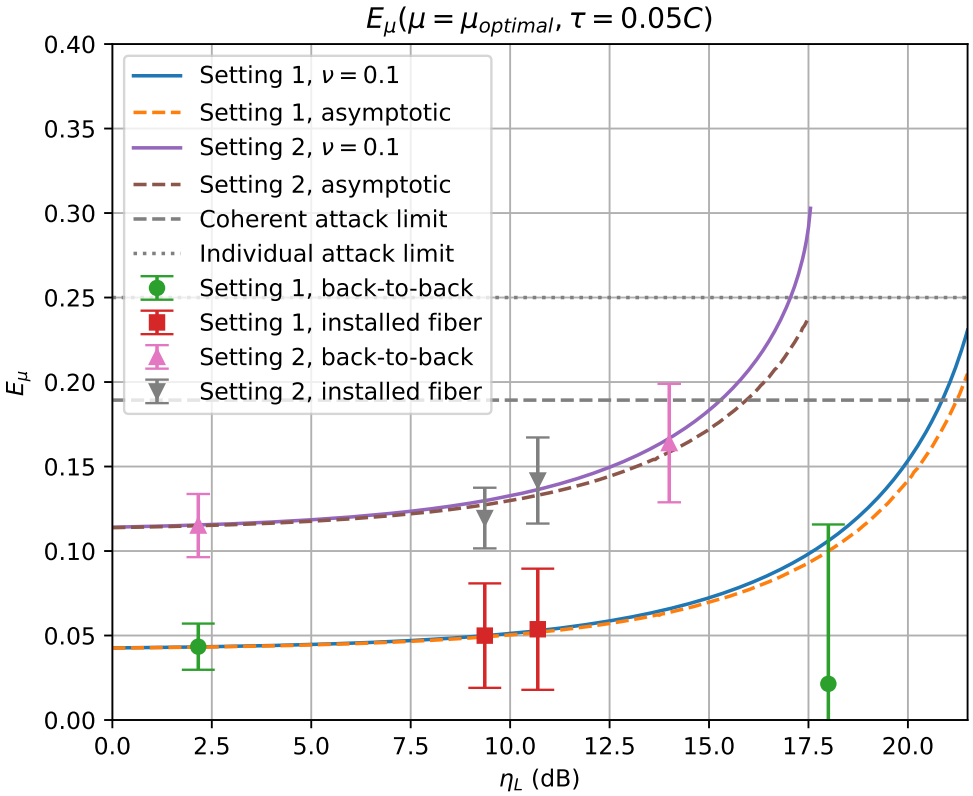


Figure 4.2.1: Average QBER as a function of η_L in the $\tau = 0.05C$ case. Curves show expected values and are cut off when it is no longer possible to find $\mu_{optimal}$.

Fig. 4.1.2 shows the key rate data for settings 3 and 4. Results from Setting 3 are similar to Setting 1, since the lowest QBER data points are essentially independent of τ, whereas Setting 4's key rate and maximum range (66 km) are lower due to the higher QBER.

4.2 QBER

Figs. 4.2.1 and 4.2.2 show the average E_μ as a function of η_L. As mentioned in Section 4.1, the key rate R becomes higher than expected for high η_L,

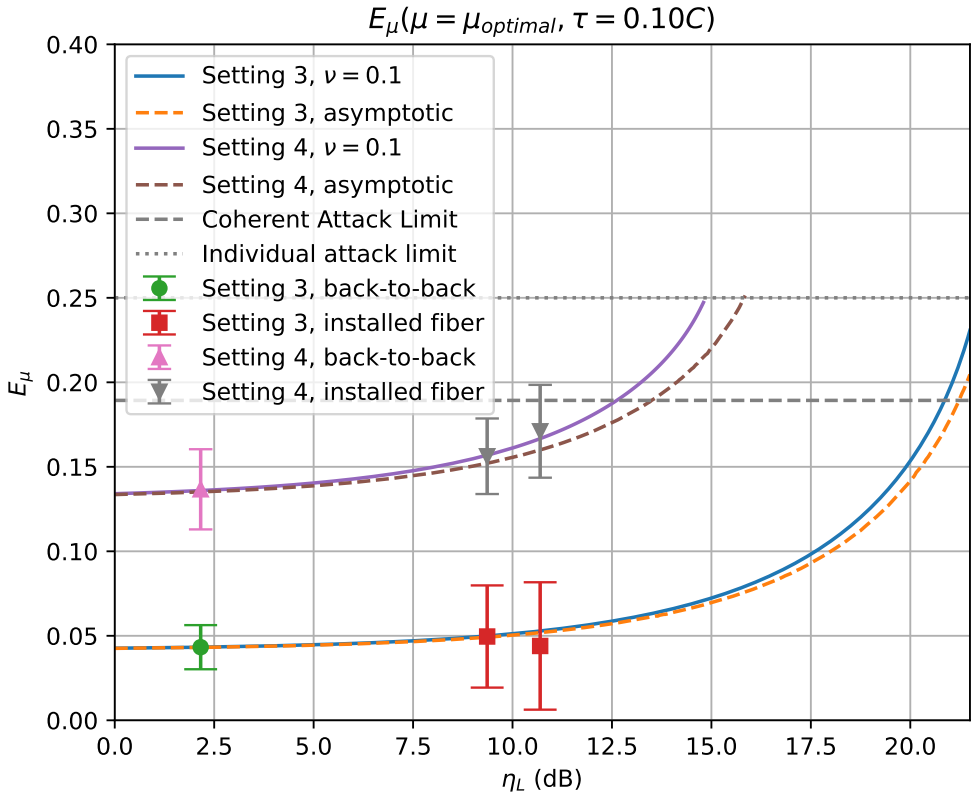


Figure 4.2.2: Average QBER as a function of η_L in the $\tau = 0.10C$ case. Curves show expected values and are cut off when it is no longer possible to find $\mu_{optimal}$.

and Fig. 4.2.1 shows why: the QBER becomes lower than expected at high attenuations. This occurs due to the fact that, when the number of detections in a given experimental realization becomes very small, fluctuations may create a scenario where E_μ or E_ν are much smaller than expected or even zero. For example, if the counts on detector i are given by C_i, an experimental realization at low η_L preparing the state $|0\rangle_Z$ may result in

$$C_0 = 1000,\ C_1 = 14,\ C_2 = 14,\ C_3 = 14, \tag{4.2.1}$$

giving us $E_\mu \approx 0.96$, but if it had been attenuated by 20 dB, the result would be

$$C_0 = 10,\ C_1 = 0,\ C_2 = 0,\ C_3 = 0, \tag{4.2.2}$$

leading to $E_\mu = 0$. In other words, when η_L is too high, the system loses the resolution to accurately determine the QBER.

This effect requires attention because, while decreasing E_μ simply increases R, a more serious phenomenon happens when E_ν is much lower than expected, i.e.

$$E_\nu < \frac{Y_0 e_0}{Q_\nu e^\nu}. \tag{4.2.3}$$

Then, in Eq. **??** we have $e_1^U < 0$, such that $H_d\left(e_1^U\right)$ becomes complex in Eq. 2.7.24, leading to nonphysical values of R. To solve this problem we calculated the expected value of E_ν from characterization data and selected the experimental realization closest to this value. This is justified by the fact that the estimation of R can be more pessimistic than the security proof

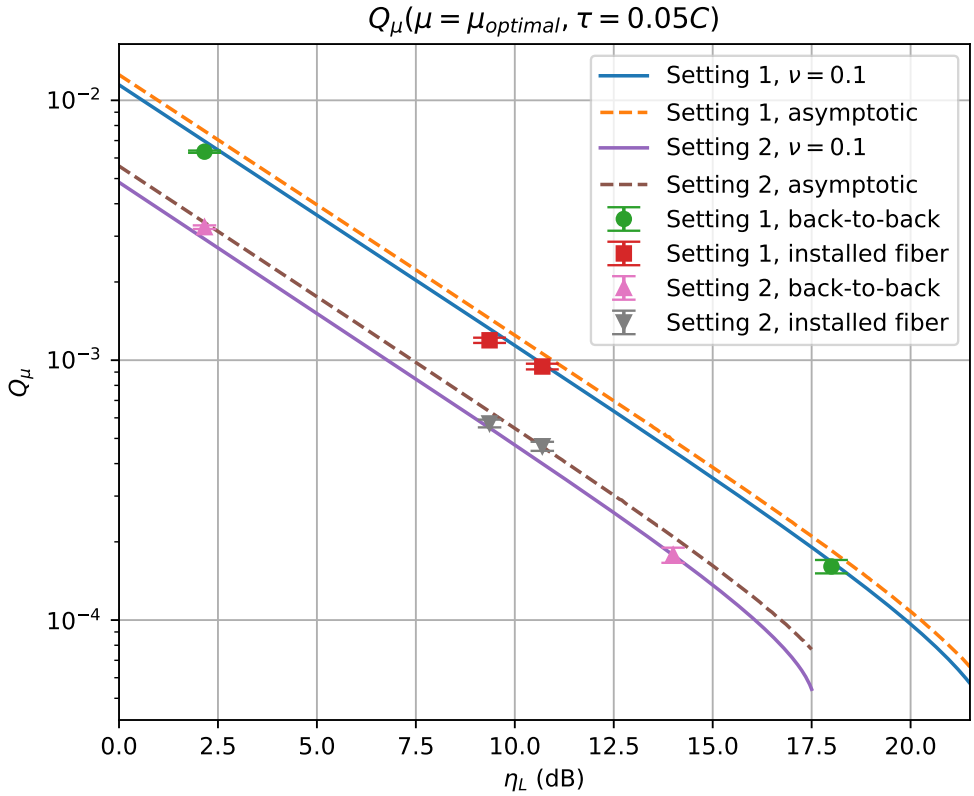


Figure 4.3.1: Average Q_μ as a function of η_L in the $\tau = 0.05C$ case. Curves show expected values and are cut off when it is no longer possible to find $\mu_{optimal}$.

demands (but not more optimistic), and so it is acceptable for Bob to report a higher QBER than measured (but not lower). Therefore, during parameter estimation Bob has the freedom to choose a sample with higher (but not lower) QBER than he otherwise would.

4.3 Gain

Figs. 4.3.1 and 4.3.2 show the average Q_μ as a function of η_L. The error bars in Q_μ are invariably very small and do not contribute significantly to

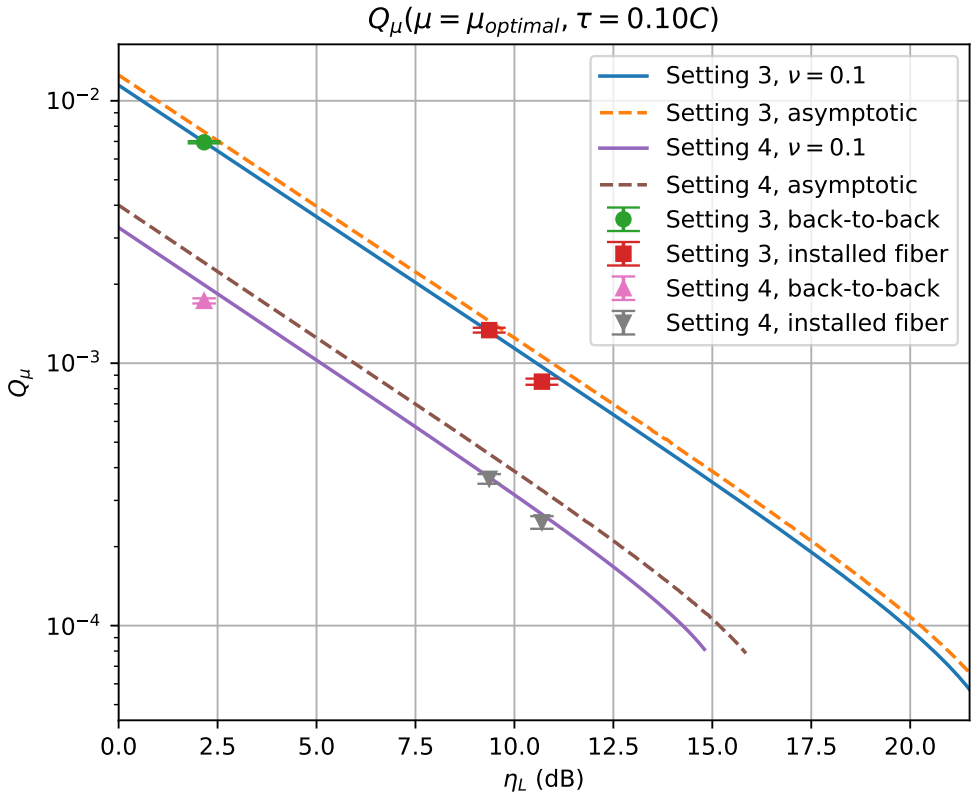


Figure 4.3.2: Average Q_μ as a function of η_L in the $\tau = 0.10C$ case. Solid lines show expected values. Curves show expected values and are cut off when finding $\mu_{optimal}$ is no longer possible.

the key rate error; however, the distance between the experimental Q_μ and the expected Q_μ does affect the actual value of R and occurs due to intensity fluctuations when implementing the desired μ.

4.4 Experimental Realizations per Minute

Installed fibers bring additional phase noise, which affects the system in different ways. One such way is when QBER measurements in an installed fiber show a larger variance, as shown in Figs. 4.2.1 and 4.5.1. The measurements in these figures illustrate the effect of phase noise during the period of one experimental realization, but another effect also occurs outside the measurement time: a decrease in the number of experimental realizations per minute achieved by the system, due to the stabilization system operating in a more noisy environment.

This decrease can be mitigated by increasing τ/C, which increases the number of realizations per minute, but as discussed in Section 3.3.1.1, the cost of doing so is a higher QBER. For this reason, the relationship between the realizations per minute and τ/C is worth experimental study. Fig. 4.4.1 shows the (experimentally determined) number of realizations per minute for different values of τ/C. These results are highly noisy, but their relationship is approximately linear for $0.05 \leq \tau/C \leq 0.20$. The back-to-back channel shows the highest number of realizations per minute, given it is the shortest and least exposed channel. However, the Faculty of Engineering channel consistently shows more realizations per minute than the 6^{th} floor channel. This is an unexpected result, as the former is much longer than the latter, and it indicates that the 6^{th} floor channel is in fact the least insulated from

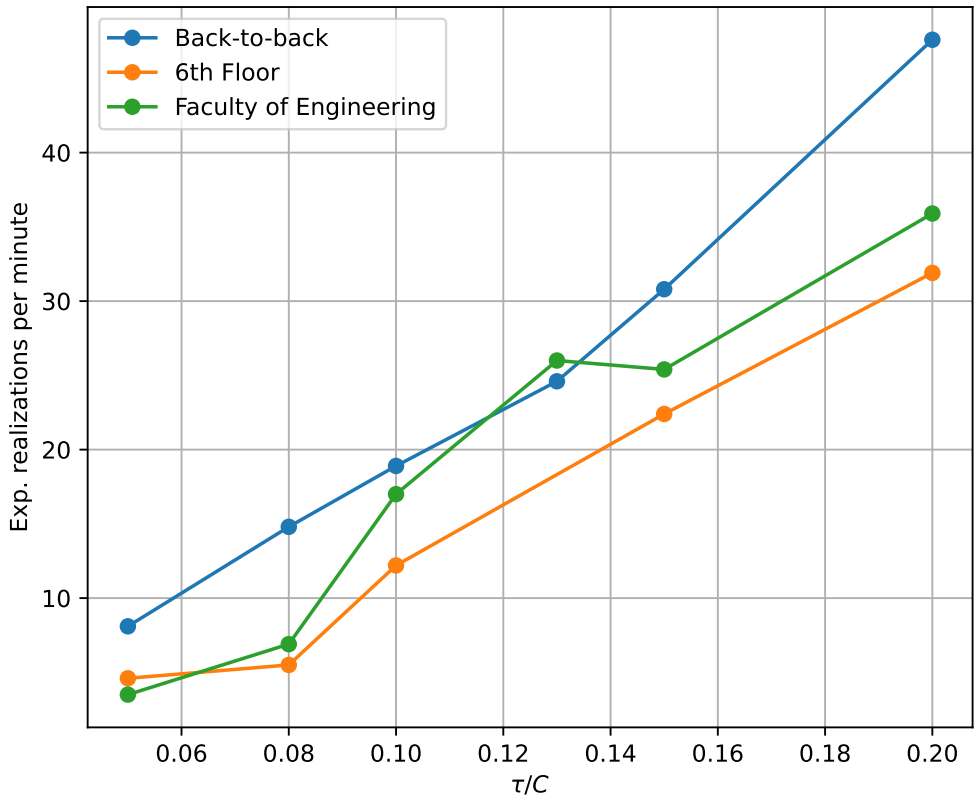


Figure 4.4.1: Experimental realizations per minute achieved by the stabilization algorithm as a function of the threshold τ divided by the total detector counts C. Data taken by preparing the $|3\rangle_X$ state.

noise in the time scales in which the stabilization system operates.

The number of realizations per minute is relevant to the system's operation in a realistic QKD application, because the key rates given in Section 4.1 and Figs. 4.1.1 and 4.1.2 assume the QKD session is active, while the stabilization-time-included key rates should also take into account the time the system spends stabilizing. Indeed, given Table 4.5.1 and the fact that, in the back-to-back channel with Setting 2, the system performed on average 4.83 experimental realizations per minute with an average of 1.75 kbit/s during the experimental realizations, the average key rate during this period is (14.13 ± 8.05) bit/s. Meanwhile, in the case of the 6^{th} floor and Faculty of Engineering channels, the realizations per minute are 1.92 and 2.15 respectively, so the average key rates are (1.05 ± 0.90) and (0.43 ± 0.97) bit/s respectively.

Note that in Setting 4, due to the higher number of realizations per minute of 14.09, 11.51 and 15.75 for back-to-back, 6^{th} floor and Faculty of Engineering channels respectively, the average key rates are (17.99 ± 26.08), (1.42 ± 7.60) and (0.15 ± 9.01) bit/s respectively. Although the statistical means are higher than in Setting 2, the error bars extend below $R = 0$, making them too large to be practical. Reducing fluctuations would potentially make Setting 4 superior to Setting 2 for short-range QKD.

However, knowing the key rate while the QKD session is active is still relevant, as any improvements made to the stabilization system in the future will cause the real-world key rate to approach this value. Further, these numbers are unstable, as the system may be easier or harder to stabilize

Channel	Experimental realizations	Fit mean	Fit standard deviation
Back-to-back	773	0.885	0.063
6^{th} floor	307	0.880	0.050
Faculty of Engineering	344	0.858	0.071

Table 4.5.1: Number of experimental realizations in a 160-minute period and fidelity fit moments for each channel.

depending on the environmental conditions. Given that other works report the key rate only while the session is active, we have elected to do the same and to use data from Fig. 4.1.1 to compare our results with others.

4.5 Fidelity Distributions

Each experimental realization results in a state fidelity sample, subject to statistical fluctuations. In Appendix C, we demonstrate that the fidelity follows a beta distribution. Fig. 4.5.1 shows the fidelity distributions for all three channels and their beta distribution fits, calculated using maximum likelihood estimation using data from all states and bases.

Table 4.5.1 shows some relevant properties of the data. The number of experimental realizations drops noticeably in installed fiber due to the higher phase noise affecting the stabilization system, as shown in both the table and Fig. 4.5.1, inset b). For the same reason, the fit mean drops significantly.

The results for standard deviations are less clear, but the Faculty of Engineering channel shows a noticeable broadening of the distribution compared to the 6^{th} floor, even though their attenuations are very close. This indicates that the Faculty of Engineering channel has higher phase

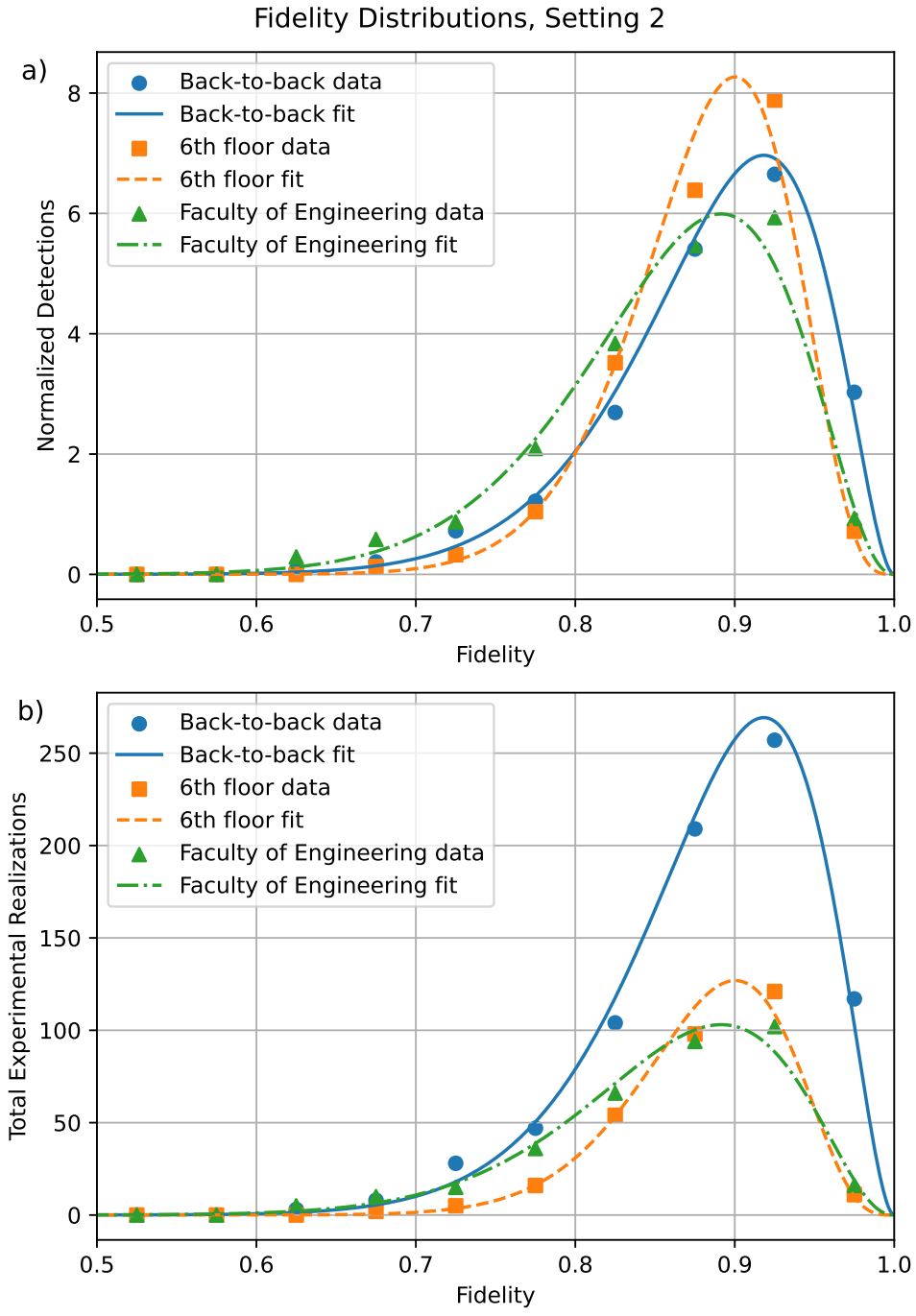


Figure 4.5.1: Fidelity distributions and beta distribution fits for the three channels in Setting 2. Inset a) shows normalized experimental realizations and distributions. Inset b) shows the total number of experimental realizations and distributions scaled to the data.

noise in the period of one experimental realization. These results challenge the assumption that e_{opt} is independent of the distance and open up the opportunity for further studies of errors in installed fibers.

4.6 Stability

QKD experiments require careful alignment before a QKD session and many components fall out of alignment within 24 hours. A QKD setup is of little use if it cannot maintain a given Q_μ and E_μ for sufficiently long to distribute a key. Therefore, in this section we will study the stability of our system over long QKD sessions.

In our system in particular, the reasons for instability can be classified in two types:

1. MZI 1 drifting as the applied voltage remains the same while its associated transmittance changes. This affects the overall μ in all MCF cores equally, and so has little effect on E_μ when $Q_\mu \gg Y_0$ (i.e. when dark counts are a small fraction of total counts).

2. Alice's IMs drifting and polarization drift from the MCF due to the environment. Both of them cause intensities to shift, the latter due to the polarizers at Bob's PMs filtering out more light when the incoming polarization is no longer aligned with them. Note that each core has an associated IM and polarization, both of which drift separately. This causes cores to have different μ and for this reason strongly affects E_μ as well.

Reference	R (bit/s)	R (bit/pulse)	Clock rate	Distance (km)	Max. distance (km)
This work	$1.21 \cdot 10^{2}$	$6.04 \cdot 10^{-5}$	2 MHz	1.3	107
Cañas et al. [10]	$4.31 \cdot 10^{-3}$	$4.31 \cdot 10^{-6}$	1 kHz	0.3	25

Table 4.7.1: Comparison of parameters of this work and its predecessor.

Notably, both of these drifts affect the intensity but not the polarization alignment. This is due to the polarizers embedded in Bob's PMs, which filter and equalize the polarizations such that, as long as the intensity in each core remains the same, good interferometric visibility is maintained over a period of weeks.

Figs. 4.6.1 and 4.6.2 show stability tests for the back-to-back and Faculty of Engineering channels over 16 hours. Insets a) and b) of Fig. 4.6.1 show that both μ and E_μ remain stable over the entire duration of the test. Meanwhile, inset a) of Fig. 4.6.2 shows that despite the noise μ remains stable over a period of 4 hours. The QBER, shown in inset b), remains stable for 12 hours. During this 4-hour period, the intensity drift does not affect R significantly due to the system's resistance against fluctuations in μ, as discussed in Section 3.5. Given the stabilization-time-included key rate of 0.43 bit/s mentioned in Section 4.4, the system would be able to transmit a 256-bit key for use in AES-256 in 10 minutes through the Faculty of Engineering channel, making its stability time more than sufficient for practical QKD.

4.7 Comparison with Other QKD Experiments

Comparing different QKD experiments is challenging due to the variety in experimental platforms, degrees of freedom, security proofs, maturity of different technologies and the manner in which results are reported. If

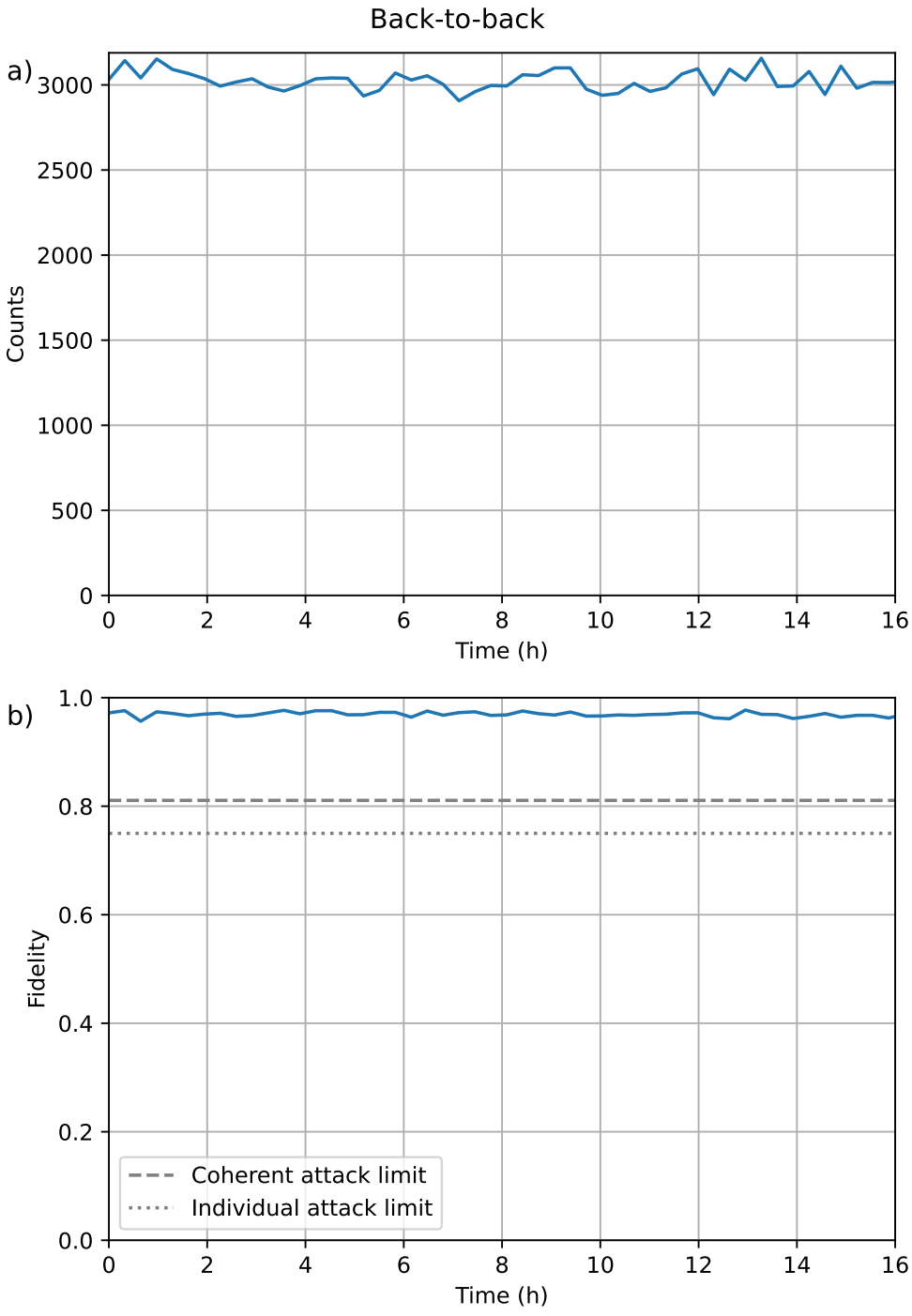


Figure 4.6.1: Back-to-back channel stability test performed by preparing state $|0\rangle_Z$. Inset a) shows the total number of counts over time. Inset b) shows the state fidelity.

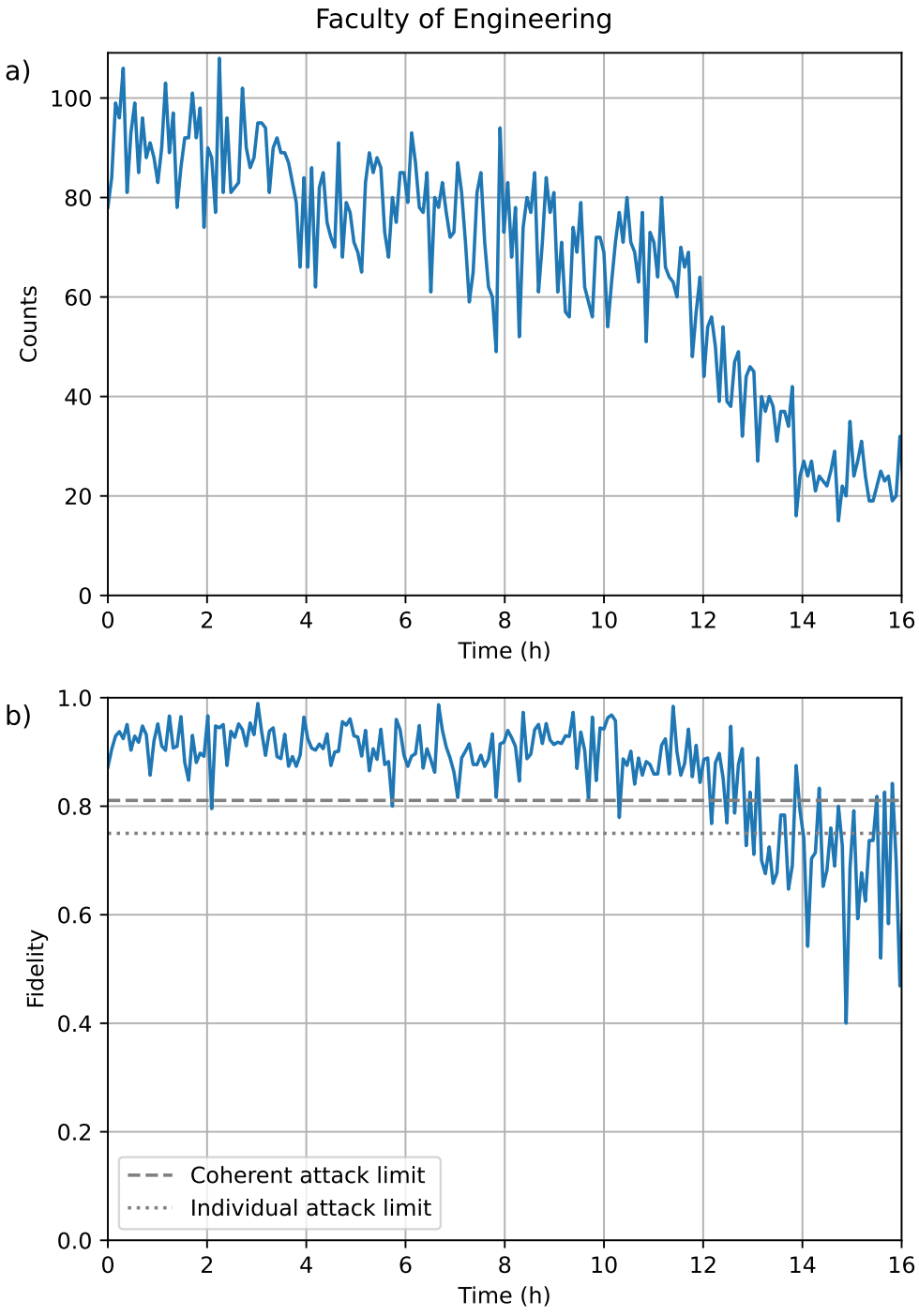


Figure 4.6.2: Faculty of Engineering channel stability test performed by preparing state $|0\rangle_Z$. Inset a) shows the total number of counts over time. Inset b) shows the state fidelity.

one compares the most important parameters (key rate, maximum distance, stability time), a given QKD method may outperform others, but can also be more costly, difficult to set up, or less compatible with existing telecom infrastructure compared to one with a lower key rate. Furthermore, a set of parameters by itself says little about the potential for future improvements.

The most natural candidate to compare this work to is Ref. [10], this setup's predecessor. In terms of results (see Table 4.7.1), this setup improves over it in nearly every way: the key rate in bit/s is increased by five orders of magnitude and in bit/pulse by an order of magnitude (despite the longer distance), the clock rate is increased by three orders of magnitude and the distance achieved is quadrupled. On a practical level, another significant improvement is the all-fiber setup as opposed to the previous, partially free-space setup, reducing injection losses and facilitating the implementation. The replacement of the single point-like SPD and pinhole with a set of four SPDs is also a major step forward, as the latter allow for a higher key rate (as per the equations from Ref. [10]). Furthermore, the pinhole was responsible for 24.5 dB of losses and its removal extends the maximum distance from 25 km to 107 km.

The maximum distance achievable is similar to other experiments with InGaAs SPADs, as it is heavily influenced by dark counts and (to a lesser degree) efficiency, both of which are dependent on detector technology. For example, using the decoy states protocol, Ref. [60] demonstrated phase encoded QKD over 107 km (of spooled fiber inside the lab) at 12 bit/s; Ref. [64] had similar results with 12.8 bit/s at 144 km; Ref. [53] similarly achieved communication at 102 km with spooled fiber. Results

from other protocols are also similar in that regard: using DPS-QKD, Ref. [31] achieved a key rate of 24 kbit/s over 100 km. With COW-QKD, Ref. [71] demonstrated QKD over 150 km and Ref. [76] over 25 km.

Although other experiments have shown key rates on the order of Mbit/s and longer distances of over 400 km, they are mainly due to four factors (not always all in the same experiment): ultra low loss fibers, low QBERs, the use of SNSPDs and high clock rates. Ultra low loss fibers are the simplest method to increase maximum distance, as they bring the channel attenuation down to ~ 0.14 dB/km [28].

As for the QBER, the way in which it is managed is very dependent on the state preparation method. In our case, the two main factors are polarization alignment errors in the B2-MPCs (see Fig. 3.3.1) and noise from the PMs. The former can be improved by replacing the manual adjustment with motorized three-paddle polarization controllers capable of smaller rotations, while the second requires improvements to the system's electronics to reduce noise. Taking data from Setting 1, the state with the lowest QBER was $|0\rangle_Z$ with $E_\mu(|0\rangle_Z) = 2.9\%$, where no phase shift was implemented, while the highest was state $|3\rangle_X$ with $E_\mu(|0\rangle_X) = 6.7\%$, meaning that the PMs altogether contribute at least 3.8% to the average QBER. This contribution increases to 12.3% in Setting 2.

The topic of SNSPDs and clock rates is more directly comparable between different encodings. Indeed, replacing our SPADs with SNSPDs while keeping everything else in the system as it is would increase the efficiency to $\sim 80\%$ and decrease the dark counts to ~ 0.1 Hz [54, 11], leading to a

maximum back-to-back key rate of 94 kbit/s, an average of 21 kbit/s, and a maximum distance of 258 km. However, SNSPDs would also allow for the use of high clock rates: much like the maximum distance, the frequency of our system is limited by the SPADs. Although some of them can operate at GHz frequencies in self-differentiating mode [81], typical gated infrared detectors such as ours can only reach up to 100 MHz due to their dead time [32]. SNSPDs, being able to operate at clock rates on the order of GHz, solve this issue. Hence, in addition to installing SNSPDs, increasing the frequency from 2 MHz to 1 GHz would boost the maximum back-to-back key rate to 47 Mbit/s and the average to 10 Mbit/s. Given that dead time currently limits the maximum key rate with SNSPDs and 2-dimensional encoding to 13.72 Mbit/s [54, 82], this would allow the system to potentially beat said limit.

5 CONCLUSION

In this thesis we studied the implementation of proof-of-concept high-dimensional QKD in a realistic environment. We showed how we achieved QKD over 1.3 km of installed fiber with an all-fiber system stable over several hours. Through system characterization we determined that the system's maximum distance is usable across large cities and is on par with other experiments using similar technology. With this, our conclusion is that high-dimensional phase-encoding QKD is a viable alternative to other encodings such as time-bin QKD, and has the potential to grow as a technology.

This conclusion from the fact that, even though we already achieved good results, there is still room for improvement at several parts of the experiment. Along with installing longer fibers, we can:

- Improve polarization alignment with motorized polarization controllers;
- Lower phase and intensity modulation noise by improving electronics;
- Increase the frequency up to 100 MHz with new FPGAs (leading not only to a higher key rate, but also more detections and more accurate

measurements as the system provides more counts per experimental realization);

- Install specialized LC-type MCF connectors to reduce insertion losses [47];
- Reduce fiber connections to decrease channel attenuation for the same fiber length;
- Perform a finite-key analysis to prevent decoy intensity from going to zero during optimization;
- Potentially replace the detectors with SNSPDs and increase the frequency even further, on the order of GHz.

Besides QKD, a major strength of our setup is its flexibility as a platform to perform other experiments. In Appendix A I reprint an article in which we used this setup to simulate non-Markovian noise. Appendix B contains another reprinted article showing how we adapted the setup to perform single-setting quantum state tomography by measuring in a higher-dimensional Hilbert space. Previous works with this setup (before I began studying at UdeC) include Refs. [45], where it was used to certify non-projective qudit measurements, and [75], where it was adapted to study superpositions of temporal orders of quantum gates. While taking measurements for this thesis we also performed preliminary work studying the effects of noise in installed fibers, shown in Section 4.5. Research in this direction can lead to a better understanding of noise models in MCFs,

which would allow the implementation of passive noise filters A, improving both classical and quantum communication infrastructure.

Future works could include more QKD experiments with improvements to the setup as well as studies of noise in MCFs in real environments under different weather conditions, time of day and other factors, as well as entirely new experiments.

BIBLIOGRAPHY

[1] Abarzúa, H., Melo, C., Restrepo, S. E., Vergara, S., Sbarbaro, D., Cañas, G., Lima, G., Saavedra, G., and Cariñe, J. (2024). Adaptive-step perturb-and-observe algorithm for multidimensional phase noise stabilization in fiber-based multi-arm mach–zehnder interferometers. *Algorithms*, 17(12).

[2] Alarcon, A., Argillander, J., Lima, G., and Xavier, G. B. (2021). Few-mode-fiber technology fine-tunes losses in quantum communication systems. *Physical review applied*, 16(3):034018.

[3] Albarelli, F., Barbieri, M., Genoni, M. G., and Gianani, I. (2020). A perspective on multiparameter quantum metrology: From theoretical tools to applications in quantum imaging. *Physics Letters A*, 384(12):126311.

[4] Babazadeh, A., Erhard, M., Wang, F., Malik, M., Nouroozi, R., Krenn, M., and Zeilinger, A. (2017). High-dimensional single-photon quantum gates: concepts and experiments. *Physical review letters*, 119(18):180510.

[5] Bennett, C. H. and Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical computer science*, 560:7–11.

[6] Bocharov, A., Roetteler, M., and Svore, K. M. (2017). Factoring with qutrits: Shor's algorithm on ternary and metaplectic quantum architectures. *Physical Review A*, 96(1):012306.

[7] Böhm, H. R., Böhm, P. S., Aspelmeyer, M., Brukner, Č., and Zeilinger, A. (2004). Exploiting the randomness of the measurement basis in

quantum cryptography: Secure quantum key growing without privacy amplification. *arXiv preprint quant-ph/0408179*.

[8] Bonnetain, X., Naya-Plasencia, M., and Schrottenloher, A. (2019). Quantum security analysis of aes. *IACR Transactions on Symmetric Cryptology*, 2019(2):55–93.

[9] Branciard, C., Gisin, N., Kraus, B., and Scarani, V. (2005). Security of two quantum cryptography protocols using the same four qubit states. *Phys. Rev. A*, 72:032301.

[10] Cañas, G., Vera, N., Cariñe, J., González, P., Cardenas, J., Connolly, P. W. R., Przysiezna, A., Gómez, E. S., Figueroa, M., Vallone, G., Villoresi, P., da Silva, T. F., Xavier, G. B., and Lima, G. (2017). High-dimensional decoy-state quantum key distribution over multicore telecommunication fibers. *Phys. Rev. A*, 96:022317.

[11] Caloz, M., Perrenoud, M., Autebert, C., Korzh, B., Weiss, M., Schönenberger, C., Warburton, R. J., Zbinden, H., and Bussières, F. (2018). High-detection efficiency and low-timing jitter with amorphous superconducting nanowire single-photon detectors. *Applied Physics Letters*, 112(6).

[12] Cariñe, J., Cañas, G., Skrzypczyk, P., Šupić, I., Guerrero, N., Garcia, T., Pereira, L., Prosser, M. A. S., Xavier, G. B., Delgado, A., Walborn, S. P., Cavalcanti, D., and Lima, G. (2020). Multi-core fiber integrated multi-port beam splitters for quantum information processing. *Optica*, 7(5):542–550.

[13] Cerf, N. J., Bourennane, M., Karlsson, A., and Gisin, N. (2002). Security of quantum key distribution using d-level systems. *Phys. Rev. Lett.*, 88:127902.

[14] Cloud, G. (2023). Delivering multi-core fiber technology in subsea cables. https://cloud.google.com/blog/products/infrastructure/delivering-multi-core-fiber-technology-in-subsea-cables. Accessed: 2025-03-09.

[15] Daemen, J. and Rijmen, V. (2001). Reijndael: The advanced encryption standard. *Dr. Dobb's Journal: Software Tools for the Professional Programmer*, 26(3):137–139.

[16] Ding, Y., Bacco, D., Dalgaard, K., Cai, X., Zhou, X., Rottwitt, K., and Oxenløwe, L. K. (2017). High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits. *npj Quantum Information*, 3(1).

[17] Dubrova, E., Ngo, K., Gärtner, J., and Wang, R. (2023). Breaking a fifth-order masked implementation of crystals-kyber by copy-paste. In *Proceedings of the 10th ACM Asia public-key cryptography workshop*, pages 10–20.

[18] Dynes, J., Kindness, S., Tam, S.-B., Plews, A., Sharpe, A., Lucamarini, M., Fröhlich, B., Yuan, Z., Penty, R., and Shields, A. (2016). Quantum key distribution over multicore fiber. *Optics express*, 24(8):8081–8087.

[19] Elkouss, D., Martínez Mateo, J., and Martin, V. (2010). Information reconciliation for quantum key distribution. *Quantum information computation*, 11.

[20] Fibercore, H. G. (2025). Sm-4c150080125001 multicore fiber. https://fibercore.humaneticsgroup.com/products/multicore-fiber/multicore-fiber/sm-4c150080125001. Accessed: 2025-02-20.

[21] Fink, D. (1997). A compendium of conjugate priors. Technical report.

[Flagship] Flagship, Q. T. Quantum key distribution (qkd). https://qt.eu/quantum-principles/communication/quantum-key-distribution-qkd. Accessed: 2025-03-09.

[23] Foro Constituyente UdeC (2024). Columna foro: La universidad de concepción frente al desafío del momento constituyente. https://foroconstituyente.udec.cl/columna-foro-la-universidad-de-concepcion-frente-al-desafio-del-momento-constituyente/. Accessed: 2025-02-28.

[24] Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H. (2002). Quantum cryptography. *Reviews of modern physics*, 74(1):145.

[25] Glauber, R. J. (1963). Coherent and incoherent states of the radiation field. *Physical Review*, 131(6):2766.

[26] Gómez, E., Gómez, S., Machuca, I., Cabello, A., Pádua, S., Walborn,

S., and Lima, G. (2021). Multidimensional entanglement generation with multicore optical fibers. *Phys. Rev. Appl.*, 15:034024.

[27] Gottesman, D., Lo, H.-K., Lutkenhaus, N., and Preskill, J. (2004). Security of quantum key distribution with imperfect devices. In *International Symposium on Information Theory, 2004. ISIT 2004. Proceedings.*, page 136. IEEE.

[28] Hasegawa, T., Tamura, Y., Sakuma, H., Kawaguchi, Y., Yamamoto, Y., and Koyano, Y. (2018). The first 0.14-db/km ultra-low loss optical fiber. *SEI Tech. Rev*, 86:18–22.

[29] Hedayat, A. and Wallis, W. D. (1978). Hadamard Matrices and Their Applications. *The Annals of Statistics*, 6(6):1184 – 1238.

[30] Hong, C.-K., Ou, Z.-Y., and Mandel, L. (1987). Measurement of subpicosecond time intervals between two photons by interference. *Physical review letters*, 59(18):2044.

[31] Honjo, T., Inoue, T., and Inoue, K. (2011). Influence of light source linewidth in differential-phase-shift quantum key distribution systems. *Optics Communications*, 284(24):5856–5859.

[32] ID Quantique (2017). ID210 Single-Photon Detector Brochure. https://dvd.ilphotonics.com/Id%20Quantique%20-%20fiber-coupled%20detectors%20-%20electronics%20-%20fiber-coupled%20lasers/Detectors/Infrared%20Single-Photon%20Detectors/ID210_Brochure.pdf. Accessed: 2025-03-04.

[33] Inamori, H., Lütkenhaus, N., and Mayers, D. (2007). Unconditional security of practical quantum key distribution. *The European Physical Journal D*, 41:599–627.

[34] Inoue, K., Waks, E., and Yamamoto, Y. (2002). Differential phase shift quantum key distribution. *Phys. Rev. Lett.*, 89:037902.

[35] IOEMA (2024). The ioema project: A new state-of-the-art data backbone. https://subtelforum.com/ioema-launches-high-capacity-data-backbone/. Accessed: 2025-03-09.

[36] Kahn, D. (1996). *The Codebreakers: The comprehensive history of*

secret communication from ancient times to the internet. Simon and Schuster.

[37] Lanyon, B. P., Barbieri, M., Almeida, M. P., Jennewein, T., Ralph, T. C., Resch, K. J., Pryde, G. J., O'brien, J. L., Gilchrist, A., and White, A. G. (2009). Simplifying quantum logic using higher-dimensional hilbert spaces. *Nature Physics*, 5(2):134–140.

[38] Lim, C. C. W., Curty, M., Walenta, N., Xu, F., and Zbinden, H. (2014). Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A*, 89:022307.

[39] Lloyd, S. (2008). Enhanced sensitivity of photodetection via quantum illumination. *Science*, 321(5895):1463–1465.

[40] Lo, H.-K., Chau, H. F., and Ardehali, M. (2005a). Efficient quantum key distribution scheme and proof of its unconditional security.

[41] Lo, H.-K., Ma, X., and Chen, K. (2005b). Decoy state quantum key distribution. *Physical review letters*, 94(23):230504.

[42] Lütkenhaus, N. (2000). Security against individual attacks for realistic quantum key distribution. *Physical Review A*, 61(5):052304.

[43] Lütkenhaus, N. and Jahma, M. (2002). Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *New Journal of Physics*, 4(1):44.

[44] Ma, X., Qi, B., Zhao, Y., and Lo, H.-K. (2005). Practical decoy state for quantum key distribution. *Physical Review A—Atomic, Molecular, and Optical Physics*, 72(1):012326.

[45] Martínez, D., Gómez, E. S., Cariñe, J., Pereira, L., Delgado, A., Walborn, S. P., Tavakoli, A., and Lima, G. (2023). Certification of a non-projective qudit measurement using multiport beamsplitters. *Nature Physics*, 19(2):190–195.

[46] Martínez, D., Pereira, L., Sawada, K., González, P., Cariñe, J., Muñoz, M., Delgado, A., Gómez, E., Walborn, S., and Lima, G. (2024). Efficient experimental qudit state estimation via point tomography. *arXiv preprint arXiv:2412.14915*.

[47] Morishima, T., Manabe, K., Toyokawa, S., Nakanishi, T., Sano, T., and Hayashi, T. (2020). Simple-structure lc-type multi-core fiber connector with low insertion loss. In *Optical Fiber Communication Conference*, pages Th3I–2. Optica Publishing Group.

[48] National Institute of Standards and Technology (2024). Nist releases first 3 finalized post-quantum encryption standards. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards. Accessed: 2025-02-20.

[49] Nielsen, M. A. and Chuang, I. L. (2010). *Quantum computation and quantum information*. Cambridge university press.

[50] NTT (2024). World's first space division multiplexing long-distance optical transmission experiment of up to 455 terabits per second in the terrestrial field environment. https://group.ntt/en/newsrelease/2024/12/09/241209a.html. Accessed: 2025-03-09.

[51] Optics, O. (2022). Multicore optical fiber. https://www.ofsoptics.com/multicore-optical-fiber/. Accessed: 2025-03-09.

[52] Park, J. L. (1970). The concept of transition in quantum mechanics. *Foundations of physics*, 1(1):23–33.

[53] Peng, C.-Z., Zhang, J., Yang, D., Gao, W.-B., Ma, H.-X., Yin, H., Zeng, H.-P., Yang, T., Wang, X.-B., and Pan, J.-W. (2007). Experimental long-distance decoy-state quantum key distribution based<? format?> on polarization encoding. *Physical review letters*, 98(1):010505.

[54] Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., et al. (2020). Advances in quantum cryptography. *Advances in optics and photonics*, 12(4):1012–1236.

[55] Raimond, J.-M. and Haroche, S. (2006). Exploring the quantum. *Oxford University Press*, 82(86):17.

[56] Ribezzo, D., Zahidy, M., Lemmi, G., Petitjean, A., De Lazzari, C.,

Vagniluca, I., Conca, E., Tosi, A., Occhipinti, T., Oxenløwe, L. K., Xuereb, A., Bacco, D., and Zavatta, A. (2023). Quantum key distribution over 100 km of underwater optical fiber assisted by a fast-gated single-photon detector. *Physical Review Applied*, 20(4).

[57] Richardson, D. J., Fini, J. M., and Nelson, L. E. (2013). Space-division multiplexing in optical fibres. *Nature photonics*, 7(5):354–362.

[58] Roetteler, M., Naehrig, M., Svore, K. M., and Lauter, K. (2017). Quantum resource estimates for computing elliptic curve discrete logarithms. In *Advances in Cryptology–ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II 23*, pages 241–270. Springer.

[59] Rojas-Rojas, S., Martínez, D., Sawada, K., Pereira, L., Walborn, S. P., Gómez, E. S., Bernardes, N. K., and Lima, G. (2024). Non-markovianity in high-dimensional open quantum systems using next-generation multicore optical fibers. *Quantum*, 8:1436.

[60] Rosenberg, D., Harrington, J. W., Rice, P. R., Hiskett, P. A., Peterson, C. G., Hughes, R. J., Lita, A. E., Nam, S. W., and Nordholt, J. E. (2007). Long-distance decoy-state quantum key distribution in optical fiber. *Physical review letters*, 98(1):010503.

[61] Rusca, D. and Gisin, N. (2024). Quantum cryptography: an overview of quantum key distribution. *arXiv preprint arXiv:2411.04044*.

[62] Sasaki, T., Yamamoto, Y., and Koashi, M. (2014). Practical quantum key distribution protocol without monitoring signal disturbance. *Nature*, 509(7501):475–478.

[63] Scarani, V., Acin, A., Ribordy, G., and Gisin, N. (2004). Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical review letters*, 92(5):057901.

[64] Schmitt-Manderbach, T., Weier, H., Fürst, M., Ursin, R., Tiefenbacher, F., Scheidl, T., Perdigues, J., Sodnik, Z., Kurtsiefer, C., Rarity, J. G., et al. (2007). Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Physical Review Letters*, 98(1):010504.

[65] Shannon, C. E. (1949). Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715.

[66] Sheridan, L. and Scarani, V. (2010). Security proof for quantum key distribution using qudit systems. *Physical Review A—Atomic, Molecular, and Optical Physics*, 82(3):030301.

[67] Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee.

[68] Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332.

[69] Shor, P. W. and Preskill, J. (2000). Simple proof of security of the bb84 quantum key distribution protocol. *Physical review letters*, 85(2):441.

[70] Standaert, F.-X. (2010). Introduction to side-channel attacks. *Secure integrated circuits and systems*, pages 27–42.

[71] Stucki, D., Barreiro, C., Fasel, S., Gautier, J.-D., Gay, O., Gisin, N., Thew, R., Thoma, Y., Trinkler, P., Vannel, F., et al. (2009). Continuous high speed coherent one-way quantum key distribution. *Optics express*, 17(16):13326–13334.

[72] Stucki, D., Brunner, N., Gisin, N., Scarani, V., and Zbinden, H. (2005). Fast and simple one-way quantum key distribution. *Applied Physics Letters*, 87(19):194108.

[73] Surján, P. R. (2012). *Second quantized approach to quantum chemistry: an elementary introduction*. Springer Science & Business Media.

[74] Szczykulska, M., Baumgratz, T., and Datta, A. (2016). Multi-parameter quantum metrology. *Advances in Physics: X*, 1(4):621–639.

[75] Taddei, M. M., Cariñe, J., Martínez, D., García, T., Guerrero, N., Abbott, A. A., Araújo, M., Branciard, C., Gómez, E. S., Walborn, S. P., et al. (2020). Experimental computational advantage from superposition of multiple temporal orders of quantum gates. *arXiv preprint arXiv:2002.07817*.

[76] Walenta, N., Burg, A., Caselunghe, D., Constantin, J., Gisin, N., Guinnard, O., Houlmann, R., Junod, P., Korzh, B., Kulesza, N., et al. (2014). A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing. *New Journal of Physics*, 16(1):013047.

[77] Weisstein, E. W. (2025). Gamma distribution. https://mathworld.wolfram.com/GammaDistribution.html.

[78] Wootters, W. K. and Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature*, 299(5886):802–803.

[79] Yates, R. D. and Goodman, D. J. (2014). *Probability and stochastic processes: a friendly introduction for electrical and computer engineers*. John Wiley & Sons.

[80] YOFC (2025). Multi-core fibre fan-in and fan-out module. https://en.yofc.com/view/2718.html. Accessed: 2025-02-20.

[81] Yuan, Z., Kardynal, B., Sharpe, A., and Shields, A. (2007). High speed single photon detection in the near infrared. *Applied Physics Letters*, 91(4).

[82] Yuan, Z., Plews, A., Takahashi, R., Doi, K., Tam, W., Sharpe, A., Dixon, A., Lavelle, E., Dynes, J., Murakami, A., et al. (2018). 10-mb/s quantum key distribution. *Journal of Lightwave Technology*, 36(16):3427–3433.

[83] Zhang, Y., Li, Z., Chen, Z., Weedbrook, C., Zhao, Y., Wang, X., Huang, Y., Xu, C., Zhang, X., Wang, Z., Li, M., Zhang, X., Zheng, Z., Chu, B., Gao, X., Meng, N., Cai, W., Wang, Z., Wang, G., Yu, S., and Guo, H. (2019). Continuous-variable qkd over 50 km commercial fiber. *Quantum Science and Technology*, 4(3):035006.

[84] Zhang, Z., Zhao, Q., Razavi, M., and Ma, X. (2017). Improved key-rate bounds for practical decoy-state quantum-key-distribution systems. *Physical Review A*, 95(1):012333.

APPENDIX

A Published Paper: Non-Markovianity in High-Dimensional Open Quantum Systems using Next-generation Multicore Optical Fibers

In this section we reproduce, in full, an article published by us in 2024 [59]. In this article Alice is connected directly to Bob with no MCF in between. Alice's phase modulators are then used to simulate certain types of non-Markovian noise.

Non-Markovianity in High-Dimensional Open Quantum Systems using Next-generation Multicore Optical Fibers

Santiago Rojas-Rojas [1,2], Daniel Martínez [1,2,3,4], Kei Sawada [1,2], Luciano Pereira [5], Stephen P. Walborn [1,2], Esteban S. Gómez [1,2], Nadja K. Bernardes [6], and Gustavo Lima[1,2]

[1]Departamento de Física, Universidad de Concepción, casilla 160-C, Concepción, Chile
[2]Millennium Institute for Research in Optics, Universidad de Concepción, casilla 160-C, Concepción, Chile
[3]University of Vienna, Faculty of Physics, Vienna Center for Quantum Science and Technology (VCQ), 1090 Vienna, Austria
[4]Christian Doppler Laboratory for Photonic Quantum Computer, Faculty of Physics, University of Vienna, 1090 Vienna, Austria
[5]Instituto de Física Fundamental IFF-CSIC, Calle Serrano 113b, Madrid 28006, España
[6]Departamento de Física, Centro de Ciências Exatas e da Natureza, Universidade Federal de Pernambuco, 50670-901 Recife-PE, Brazil

With the advent of quantum technology, the interest in communication tasks assisted by quantum systems has increased both in academia and industry. Nonetheless, the transmission of a quantum state in real-world scenarios is bounded by environmental noise, so that the quantum channel is an open quantum system. In this work, we study a high-dimensional open quantum system in a multicore optical fiber by characterizing the environmental interaction as quantum operations corresponding to probabilistic phase-flips. The experimental platform is currently state-of-the-art for quantum information processing with multicore fibers. At a given evolution stage we observe a non-Markovian behaviour of the system, which is demonstrated through a proof-of-principle implementation of the Quantum Vault protocol. A better understanding of phase-noise in multicore fibers will improve several real-world communication protocols, since they are a prime candidate to be adopted in future telecom networks.

1 Introduction

Currently, optical fiber-based communication is the fastest method for information transmission [1], mainly due to the multiple alternatives it offers for multiplexing techniques [2, 3]. One new promising method for increasing fiber information capacity is the space-division multiplexing technique based on Multicore Fibers (MCFs). In this case, more information is sent through the fiber by exploiting the extra cores contained in its cladding [4]. MCFs have allowed transmission rates up to 305 Tb/s through a 19-core MCF [5], setting a new benchmark for ultrahigh transmission capabilities that largely surpass conventional single-mode fibers [6]. Moreover, it has been recently demonstrated that MCFs are compatible with quantum information processing (QI). For instance, high-dimensional quantum cryptographic protocols have been performed using 4-core fibers. In this case, high-dimensional quantum states (hereafter qudits) are encoded by exploiting the available core modes for single photon propagation in the MCF [7, 8]. This encoding strategy has been further extended into other QI protocols [9–13], and to build high-dimensional entangled photons sources [14–16].

In real large-scale networks, optical fibers are exposed to perturbations induced by environmental noise. As a result of these perturbations, information loss could be introduced according to the Markov hypothesis behind noise processes, spoiling the information transmission [17]. The Markovian nature of noise has significant consequences for quantum communication tasks and can be witnessed by a monotonic decay of channel capacities along the propagation [18]. At the same time, the interest in quantum dynamics deviating from the Markov hypothesis, namely non-

Santiago Rojas-Rojas: santirojas@udec.cl

Markovianity (NM), has increased in recent years due to its theoretical relevance and possible application in the protection and processing of quantum information [19–23]. The behavior of non-Markovian processes has been observed in photonic experimental simulations of environmental effects through different schemes [24–35]. To date, the use of NM as a resource for QI has been mainly focused on entanglement-based protocols [36, 37], while a formal resource theory for NM is still in early development [38–40]. Thus, a relevant goal to achieve is the experimental observation of NM in a simple scenario without considering entanglement, envisaging its application for QI tasks in the prepare-and-measure scenario. For instance, measuring non-Markovian effects through an adequately defined quantum channel capacity allows linking NM with the efficiency of a specific QI protocol [18, 41]. Of particular interest is Ref. [42] that has introduced the Quantum Vault (QV), a protocol for storing and retrieving information encoded in a quantum system subject to non-Markovian evolution.

In this work, we introduce a new model to characterize the phase-noise of multicore optical fibers, which is arguably the main effect that leads to the degradation of their information capacity. In our model, the environmental interaction is treated as quantum operations corresponding to probabilistic phase-flips acting on path qudits, which are encoded in terms of the core modes available for photon propagation. The types of phase flips considered in the model can readily be changed moving from simplified scenarios to unrestricted ones. As an initial investigation with this model, we focus on the specific conditions under which the phase-noise will lead to a NM map implemented in the path qudits. The dynamics are experimentally realized by controlling the occurrence probability of the desired error operations. The setup adopted is based on a platform recently introduced to control qudit states propagating over MCFs [10]. We observe a non-monotonic behavior of three different capacities, allowing a proof-of-principle realization of a QV [43–45]. As discussed above, the observation of NM dynamics in a prepare and measure setup configuration is per se interesting, since it may lead to the development of new QI protocols related to data hiding. Nonetheless, we highlight that our model is far more general, and has been developed with the intent of modeling the imperfections to be observed in installed cables of multicore fibers in future high-capacity telecom networks.

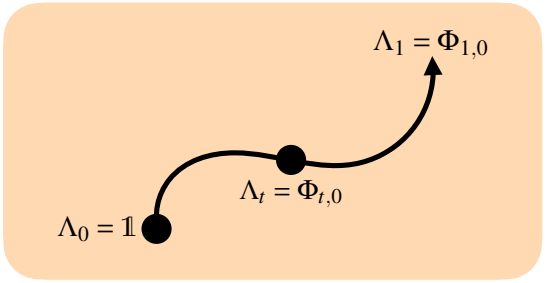


Figure 1: A quantum map Λ_t can be defined as a curve in the space of quantum channels. We use $t = 1 - p_0$ as the dynamical variable, where p_0 is the no-change probability. Assuming this probability to be null at the end of the evolution, the ending point corresponds to $t = 1$.

2 Noisy quantum maps in MCFs

A general quantum process is defined by a family of one parameter dynamical maps $\{\Phi_{t,0}\}$, where $\Phi_{t,0}$ is a completely positive and trace preserving (CPTP) map for any $t > 0$ [18, 46], taking an input density operator ρ_0 into an output density operator ρ_t. As depicted in Fig. 1, a quantum process can be described by a continuous evolution curve Λ_t in the space of CPTP maps, such that $\Lambda_0 = \mathbb{1}$. An evolution is called CP-divisible if $\Phi_{t,0} = \Phi_{t,s}\Phi_{s,0}$, where $\Phi_{t,s}$ is completely positive (CP) for all stages s such that $0 \leq s \leq t$. All processes given by CP-divisible maps are called Markovian evolutions [21]. Otherwise, they are called non-Markovian.

In the following, we consider a noisy quantum process where a quantum system in an unknown state may be affected by a set of unitary transformations U_k operating with their respective probability p_k. The formalism of quantum processes allows us to define such a dynamical map following an intuitive posit: when the system is just starting to evolve from its initial state ρ, it does not undergo any change yet, so the probability p_0 of it remaining unchanged (or being transformed only by $U_0 = \mathbb{1}$) must be equal to one, with all the remaining probabilities $p_{k\neq 0}$ being null; as it evolves, the no-change

probability p_0 decreases while the remaining probabilities increase. (A similar approach has been used for the experimental simulation of environmental effects on single qubits [29].) This way, we associate the dynamical variable t with a decay of p_0. Since all the relevant behavior for our study is observed for a finite value of p_0, knowing the particular dependence of t on it is not crucial. Then, we can take $t = 1 - p_0$ as the dynamical parameter to define the noisy process, which is now enclosed by the curve in $0 \leq t \leq 1$ or $1 \geq p_0 \geq 0$.

The explicit definition of our map makes use of the *operator-sum* representation for a quantum channel $\Phi(\rho) = \rho'$ in the framework of quantum operations, where all the environmental effects are captured by a complete set of *Kraus operators* E_k acting on the system's Hilbert space as $\rho' = \Phi(\rho) = \sum_k E_k \rho E_k^\dagger$. The noisy process Λ_t under our consideration is composed of a family of channels whose Kraus operators $E_i = \sqrt{p_i} U_i$ describe the occurrence of a unitary error operation U_i [see the examples below in (2)] affecting the system with probability p_i, all the p_i being defined in function of the no-change probability p_0. Let $|\psi\rangle$ be the state of a single photon propagating through a N-core optical fiber:

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{\ell=1}^{N} e^{i\phi_\ell} |\ell\rangle \ , \tag{1}$$

where $|\ell\rangle$ denotes a one-photon state in the core ℓ. We will consider a set of error operations U_i that permute the phase values ϕ_ℓ of the state in Eq. (1). Each permutation on its own is a noiseless operation, so the presence of noise is due to the probabilistic combination of them and somewhat extends the concept of bit-flip or phase-flip channels found in open qubit systems to higher dimensions. We can address different scenarios by allowing permutations only between cores on certain subsets (this has some relation to the prescription given in [47, 48] to implement non-Markovian phase patterns). Let s be the number of cores in these subsets: $s = 1$ prevents reordering, so the only possible unitary transformation is the identity, leading to trivial Markovian dynamics. The $s = 2$ case (Fig. 2)

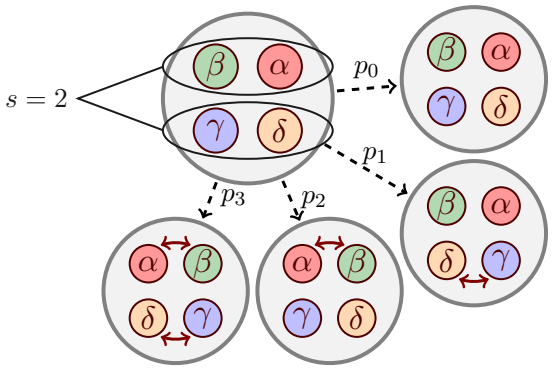


Figure 2: The four possible operations when $N = 4$ and $s = 2$, with their respective probabilities p_i. Greek symbols represent the phases of the logical state at each core.

involves just four possible operations, namely,

$$U_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \ U_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \tag{2}$$
$$U_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \ U_3 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

while $s = 3$ and $s = 4$ enable 6 and 24 unitary transformations, respectively, corresponding to the number of available permutations. It is worth remarking that instead of the most common method used in an experimental simulation of non-Markovian processes — that is, to consider and manipulate the state of the environment explicitly — our approach reflects the environmental influence by the variation on the specific probability of an error (permutation) occurring, similar to the scheme used in Ref. [30] to implement a dephasing channel or the simulation of classical non-Markovianity in [34]. In this way, we intend to make our experimental simulation consistent with the standard premise that only the state of the system is accessible to the experimenter, so it can be used as a building block to describe a general noise process for qudits, just like in qubit systems the bit-flip and phase-flip errors are components of the general depolarizing channel. The inaccessibility of the environment is also relevant for using our system as a secure channel.

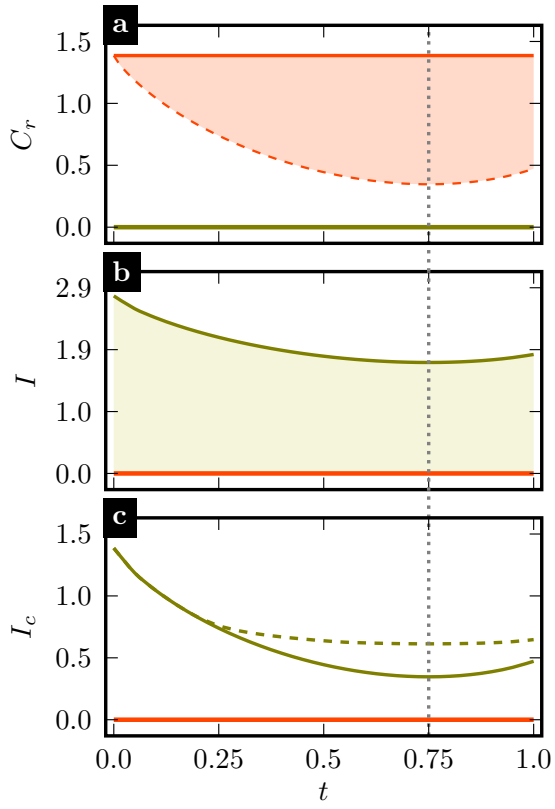


Figure 3: Evolution of coherence and quantum mutual information under maps Λ_{p_0} for $s = 2$ and when permutations are equally probable (See Fig. 2). (a) Relative entropy of coherence as a function of t from maximally coherent initial states. If the relative phases between the terms of the state are null, its REC is constant, as depicted by the red line. The other cases are contained in the orange region. (b) Quantum mutual information at each stage of the map Λ_t. The beige region contains the results obtained from 10^6 normally-distributed mixed states. Green solid curves correspond to a chaotic input state $\mathbb{1}/4$. (c) Evolution of coherent information. In this case, we show the maximum at each point obtained from a normal distribution of 10^6 initial mixed states (dashed line). Green solid curves correspond to a chaotic input state. The vertical dashed lines indicate where the minimum is reached.

3 Non-Markovian effects in quantum information capacities

In order to assess the effect — and usefulness — of NM in quantum information and quantum communication protocols, different NM measures have been proposed, which are based on the monotonic decay of certain quantifiers under the action of CPTP maps. An increase or revival of these quantities along evolution indicates a backflow of information from the environment to the system [20, 21]. That is, when these quantities show an increase or resurgence during evolution, it indicates a transfer of information from the environment back to the system, serving as evidence/witness of NM's evolution.

The first information resource we can consider is the *quantum coherence*. If a system evolves under a CPTP map, such as Λ_t, its coherence cannot increase. Conversely, coherence is expected to decay monotonically under a Markovian noisy process, so a suitable NM witness is given by an increase in the *relative entropy of coherence* (REC) [49, 41], which has a closed form for a N-dimensional quantum state ρ given by:

$$C_r = S(\rho_{\text{diag}}) - S(\rho)\,. \tag{3}$$

Here, ρ_{diag} is the diagonal part of the density matrix ρ, and S denotes the von-Neumann entropy [50]. This relation with the entropic characteristics of the system poses the maximum REC as a valid measure of the channel capacity, providing an interpretation of coherence in terms of the average amount of information conveyed by a state. We evaluate its behavior under our map Λ_t, taking as initial states the set of maximally coherent pure states with $C_r = \log 4$. The orange region depicts the respective evolution of C_r in Fig. 3 (a) for $s = 2$ when the error operations are equally probable, i.e., $p_{i\neq 0} = (1 - p_0)/3$. We observe how C_r decays to a minimum at a certain t corresponding to a finite no-change probability p_0, after which it increases. The minimum is reached when all the permutations are equally probable, i.e., when $p_i = p_{\min}$ for all i. The revival of REC in the regime $1 - p_{\min} < t < 1$ (or equivalently $p_0 < p_{\min}$) breaks the monotonic decrease imposed by the Markov approximation.

Diagonal density matrices correspond to incoherent states giving a null value of distance-based measures of coherence such as REC [green line in Fig. 3 (a)]. However, these states have maximal information content that can be transmitted through a quantum channel, which can be measured by proper capacities capturing the *non-unital part* of the dynamics [21]. In analogy to the classical Shannon capacity, different quantities are used to estimate a bound for the average amount of transmitted information, depending on the particular protocol. First, the *quantum mutual*

information,

$$I(\rho,\Phi) = S(\rho) + S(\Phi[\rho]) - S(\rho,\Phi)\,, \qquad (4)$$

limits the amount of classical information that can be transmitted through the channel Φ. In this definition, the last term corresponds to the *entropy exchange* $S(\rho,\Phi)$, which quantifies the entropy change with the environment [18, 51]. It is also used to define the *coherent information* [52]

$$I_c(\rho,\Phi) = S(\Phi[\rho]) - S(\rho,\Phi)\,. \qquad (5)$$

This quantity is important for several reasons, which are discussed in more detail in the supplementary material. Its fundamental definition considers the entanglement between the system and an *ancilla*, this being the reason why it is regarded as a proper bound of the nonclassical information conveyed by the quantum carrier [53].

Quantum mutual information and coherent information cannot be increased by any post-processing of the channel output. This property, the *data processing inequality* [54], is related to the monotonic decay of both capacities under a Markov noisy process. A break of this behavior is a signature of NM evolution [18]. In Fig. 3, we present the evolution of the quantum mutual information (b) and the coherent information (c) under Λ_t for different initial states. Dark green curves correspond to the evolution of the capacities for a mixed input state $\rho = \mathbb{1}/d$. Noticeably, both capacities I and I_c attest to the non-Markovian nature of the map: for mixed states, a minimum is again reached at $p_0 = p_{\min}$. According to its definition, the decrease of I (of I_c) up to this stage of the evolution indicates a loss of classical (quantum) correlations between the input and the output, with a consequent variation of entropy on the environment, or equivalently, a leak of information from the system to it. In the region $1 - p_{\min} < t < 1$, both capacities rise again, indicating an information back-flow from the environment to the system. Note that since all the maximally coherent states of Fig. 3 (a) are pure, their von Neumann entropy is null, so the related quantum mutual information is also null [red lines in Figs. 3 (b,c)].

4 Non-Markovian dynamics in MCF

4.1 The quantum vault protocol

As far as they account for the maximal average amount of information that can be transmitted, the channel capacities introduced in the previous section identify resources that can be used to store and retrieve information by state preparation and measurement of a quantum state. This is the concept of the quantum vault, originally introduced in Ref. [42]. Consider that Alice wants to store some information by encoding it in a qudit. The system evolves by the map Λ_t, with the resource at each stage being quantified by some channel capacity $K(t)$. After the process is finished, i.e., for $t_f = 1$ ($p_0 = 0$), Alice tries to recover her information. The more information that is contained in the final state, the more successful the retrieval is. Suppose that at some stage of the evolution in the interval $0 < t < 1$, an eavesdropper Eve attempts to measure the state of the system and thus steal Alice's information. If Eve cannot retrieve as much information as Alice, then the system constitutes a quantum vault [42]. The noisy process Λ_t has a key feature that enables the implementation of the quantum vault, namely, the non-monotonic behavior. There is a finite interval where $K(t) < K(t_f)$, and less information can be retrieved. The revival time Δt, where the capacities increase at the end of the evolution, can then be used to quantify the suitability of a given system to serve as a QV.

In a general N-core fiber, if m is the integer quotient of N divided by the size of the subsets s, there are $(s!)^m\,(N-ms)!$ possible permutations. Since we consider $t_f = 1$, the uniform probability $p_{\min}$ is equal to Δt and takes the value

$$\Delta t = p_{\min} = \frac{1}{(s!)^m\,(N-ms)!}\,. \qquad (6)$$

If we consider the error operations to occur with the same probability, i.e. $p_{i\neq 0} = (1-p_0)/3$ in a 4-core fiber with $s = 2$, we get $\Delta t = 0.25$ (See Fig. 3). However, from Eq. (6), it is clear that the value of the revival time Δt is inversely proportional to the number of available permutations affecting the evolution. Thus, maximal information recovery in the QV protocol can already be obtained while considering a simplified scenario in the $s = 2$ case, where phase

permutations can only occur simultaneously on both subsets of cores, i.e., $p_1 = p_2 = 0$ and $p_3 = 1 - p_0$. In this case, the revival time is $\Delta t = 0.5$.

4.2 Experimental Setup

In order to demonstrate a new platform to study the dynamics of high-dimensional open quantum systems, we exploit the use of a MCF-based 4-arm Mach-Zehnder interferometer to prepare four-dimensional ($d = 4$) qudit states, and also to statistically apply a set of unitary operations U_i to them. By doing this, we simulate the state transition maps. The experiment consists of three main parts: state preparation, map implementation, and quantum state tomography characterization, and is presented in Fig. 4.

Qudit Source. A CW-1546 nm laser attenuated by neutral filters and a fiber intensity modulator controlled by a Field Programmable Gate Array (FPGA1) prepares light pulses with a repetition rate of 2 MHz, which are propagated by telecom SMF-28 fibers. The combination of these three devices allows the generation of weak coherent pulses with an average photon number of $\mu = 0.15$, which provides a good approximation to a single photon source, since 95.7% of the non-vacuum pulses are single photons. Next, a demultiplexer (DMUX) device is used to connect the initial SMF into a single core of a four-core MCF, while the other three cores remain unconnected. A backbone device in the setup is the MCF Beam Splitter (MCF-BS), which enables the superposition state on the propagation paths of the MCF[10, 12]. An MCF-BS is fabricated by heating and stretching a section of the MCF, creating a tapered subsection of the fiber. This geometric deformation of the MCF structure changes the distance between the cores, allowing crosstalk between them. The MCF-BS was recently characterized by Cariñe et al. [10], who proved that the output distribution corresponds to a $d = 4$ Haddamard matrix H_4, allowing the generation of superposition states. Thus, the qudit state after MCF-BS is $|\psi_0\rangle = (1/2)\sum_{\ell=1}^{4} e^{i\phi_\ell}|\ell\rangle$, where ϕ_k are individual phase drifts that will be addressed in the next stage.

Map Implementation. To extinguish parasitic phase drifts in state preparation and to apply the probabilistic dynamical map, we include a phase stabilization system in the setup. It is composed of three $LiNbO_3$ phase modulators (PMs) in a feedback-loop connected with the avalanche photo detectors (APDs). The control system works as follows: Initially, there is a 100 ms stabilization interval, where FPGA1 implements a stabilization procedure [10] to compensate for phase drifts between cores and generate the desired initial state. This is done by optimizing the observed probability distribution in the APDs, such that it is very close to the distribution expected for the state that one wants to generate. Typical fidelities observed in this stage are higher than 99%, due to almost perfect mode matching for the different core modes in the final beam-splitter.

Once the target output probability is reached, the dynamic map Λ_t is implemented for the next 100 ms time interval. This is done by randomly applying the unitaries U_0 and U_3 (see Fig. 2), for each of the 200.000 pulses generated, with probabilities p_0 and $1 - p_0$, respectively. In this way, the observed statistics, integrated over the 100 ms time interval, are associated with a mixed state that emerges after the evolution through a map Λ_t, with $t = p_3 = 1 - p_0$.

Characterization. A quantum state tomography with five mutually unbiased bases (MUBs) in $d = 4$ is used to estimate the final qudit density matrix [55–61], allowing the calculation of the required channel capacity. The measurement projection is implemented using a second FPGA2 that controls a second set of phase-modulators and with the final 4×4 MCF beam-splitter. The states associated with the four outcomes of this last beam-splitter are given by

$$
\begin{aligned}
|\psi_0\rangle &= \frac{1}{2}(e^{i\phi_0^B}|0\rangle + e^{i\phi_1^B}|1\rangle + e^{i\phi_2^B}|2\rangle + e^{i\phi_3^B}|3\rangle),\\
|\psi_1\rangle &= \frac{1}{2}(e^{i\phi_0^B}|0\rangle + e^{i\phi_1^B}|1\rangle - e^{i\phi_2^B}|2\rangle - e^{i\phi_3^B}|3\rangle),\\
|\psi_2\rangle &= \frac{1}{2}(e^{i\phi_0^B}|0\rangle - e^{i\phi_1^B}|1\rangle + e^{i\phi_2^B}|2\rangle - e^{i\phi_3^B}|3\rangle),\\
|\psi_3\rangle &= \frac{1}{2}(e^{i\phi_0^B}|0\rangle - e^{i\phi_1^B}|1\rangle - e^{i\phi_2^B}|2\rangle + e^{i\phi_3^B}|3\rangle), \quad (7)
\end{aligned}
$$

where ϕ_k^B is the phase applied by the second modulator in the core mode k. The projection is concluded connecting commercial InGaAs single-photon detection modules to each output mode, working in gated mode and configured with 10% overall detection efficiency. Over the 100 ms measurement interval, FPGA2 imprints

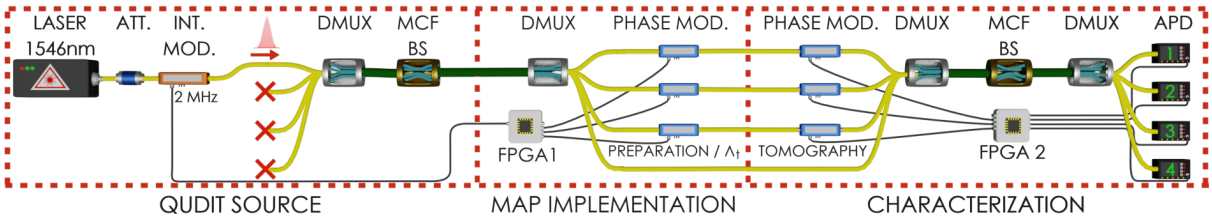


Figure 4: Four-arm Mach Zehnder interferometer based on MCF to simulate non-markovian dynamics. A CW-1546 nm laser, neutral attenuators, and an intensity modulator generate a weak coherent state with a mean photon number of $\mu = 0.15$ at a repetition rate of 2 MHz. The single photon state is transmitted through an MCF DMUX and an MCF BS, generating a 4-dimensional state encoded on the 4 possible core modes inside the MCF. An MCF DMUX is used to spatially separate the paths such that one can address the relative phases via PMs. During a 100 ms time interval, an FPGA-based active control system adjusts the voltages on the PMs to generate the state $|e_i\rangle$. Immediately thereafter, in the next 100 ms time interval, FPGA1 uses the PMs to randomly implement i) the identity or ii) the phase-flips associated to the transition 3 in Fig. 2, with probability $p_3 = 1 - p_0$. In the characterization stage, a second FPGA performs measurements over 5 MUBs to reconstruct the resulting density matrix. This is done by closing the interferometer with a MCF BS and collecting the single photon counts with four APDs.

the phases that correspond to the 16 different states of the four MUBS and records the corresponding statistics. The fifth MUB (logical basis) was measured before each round of the experiment. The results were used to compute the experimental density matrix ρ_{exp} using a maximum likelihood estimation routine [62], and then the different channel capacities.

4.3 Proof-of-principle realization of the QV protocol

The fact that the randomly applied unitaries are actually performed by the user allows the NM to be exploited in a controlled way. Let us illustrate this by outlining how the QV procedure applied to our MCF setup can be used to hide information efficiently. Suppose the photons are sent through a long MCF fiber that serves as a quantum memory. Let us apply phases using the relevant probability distribution corresponding to p_{min}. Then, the information that an eavesdropper can recover is minimal. Using a classical register, the user can make a record of the particular unitary U_i that was applied to each light pulse sent through the fiber. When the photons exit the fiber, if one has access to the classical register, one can look up which unitary was applied to each photon and apply a second unitary chosen so that the complete evolution corresponds to a non-Markovian channel with $t = 1$, where information recovery is maximum. An eavesdropper who does not have access to the classical register does not know which unitaries have been applied to which photons and thus cannot generate a non-Markovian channel. In this way, the information hidden in the vault can only be recovered by users with access to the classical memory register.

Consider an arbitrary orthonormal base defined by the states:

$$|e_1\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ i \\ i \\ -1 \end{pmatrix}, \quad |e_2\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ i \\ -i \\ 1 \end{pmatrix}, \quad |e_3\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ -i \\ -i \\ -1 \end{pmatrix}, \quad |e_4\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ -i \\ i \\ 1 \end{pmatrix}, \tag{8}$$

which are all equally weighted superpostions of the states $|\ell\rangle$ ($\ell = 0, 1, 2, 3$) corresponding to a single photon propagating in the ℓ-th core. To simulate different channel dynamics in our setup, the evolution of the input state $|e_2\rangle$ was studied. For each measurement interval of 100 ms, we randomly applied U_0 and U_3 considering different values for the probabilities p_0 and p_3. The red dots in Fig. 5 correspond to the evolution of the relative entropy of coherence C_r at specific stages in the simplified case ($p_3 = 1 - p_0$ and $p_1 = p_2 = 0$). This scenario allows C_r to rise back to its initial value at the end of the evolution, so the information backflow is complete. The simulation consists of summing up, for a given stage, the statistics obtained in all previous ones. Thus, simulating the photon state evolution through different channel dynamics, sequentially. The experimental results follow the theoretical prediction very closely,

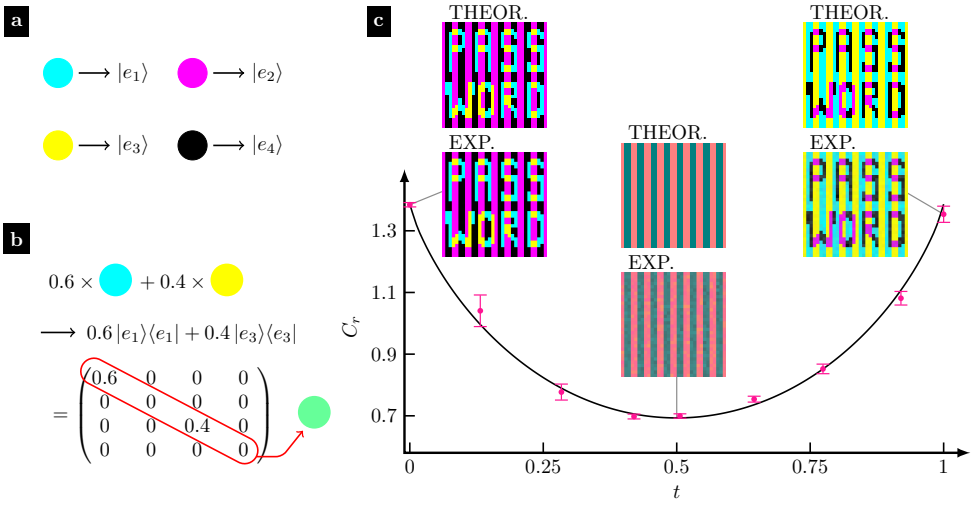


Figure 5: Proof-of-principle implementation of the quantum vault protocol to store an image using the noisy map Λ_t with $p_1 = p_2 = 0$. (a) Each qudit in the 4-dimensional canonical basis is associated with a specific color of the cyan-magenta-yellow-black (CMYK) model. (b) Mapping the CMYK color model into the basis allows a direct equivalence between color mixtures and mixed states: the diagonal of the density matrix in this basis is the CMYK code of the respective color. (c) At the input stage, Alice stores a message as an image whose pixels have one of the base colors. As the system evolves, the distinguishability between different state pairs in the basis decreases, which is reflected by a decrease in the REC. At $t = 1 - p_{\min}$, the capacity is minimal, rendering the message of the image unreadable. Non-Markovian dynamics in the final stage of the evolution leads to an increase in distinguishability, allowing Alice to retrieve her information even if the final state of each pixel is different from its initial state (colors are swapped in the retrieved image). In the insets, the top and bottom images correspond to the predicted and measured images. (Please see Fig. 6 where we present different cases in the supplementary material)

serving as a demonstration that different channel dynamics (Markovian and Non-markovian) can be simulated in a very controlled way in our system. To compute the error bars for the experimental data set, we performed a Monte Carlo routine by varying a Poisson distribution centered on the experimental counts and computed 1000 simulated density matrices. Error bars correspond to one standard deviation of the ensemble.

Now, let us show how a classical message is affected by such different types of dynamics. Consider an image composed of 1024 pixels whose color is defined in the four-color model CMYK (cyan, magenta, yellow, black). This pattern of colors can be encoded directly in the quantum state of the photons sent through our setup. As depicted in Fig. 5b, associating the basis states above with the CMYK code, provides a straightforward visual representation of mixed states as color mixtures. The user stores a four-color image whose pixels correspond exactly to one of the four CMYK colors, as shown in the top left inset of Fig. 5c. This is done by preparing a set of 1024 qudits, whose states are defined according to the CYMK color code. As the evolution proceeds, each of these pixel-states is independently affected by the noisy map Λ_t, so they turn into a mixed state ρ_t. In Fig. 5c, we plot the respective images retrieved. The output image was recovered by measuring in the encoding basis (8). The full backflow of the information encoded is reflected by the last image, where all pixels are in a pure color of the CMYK code, just like the initial image. The minimum of the capacity C_r is reached with $p_3 = p_0 = 1/2$ ($t = 0.5$), when all the pixel-states at this point are in one of two mixtures, rendering the message in the image unreadable. The average fidelity of the reconstructed qudits is 98.5%, so the difference between the experimental and theoretical images is almost negligible.

5 Conclusions

Applying quantum technologies in practical scenarios requires the study of decoherence, which is intrinsically related to environmental noise, that can outweigh the advantages that quantum systems could provide. In this

context, studying open quantum systems and non-Markovianity is a relevant topic, as it could provide bright insights for fault-tolerant quantum communication tasks, real-world system evolution, or even practical quantum memories [63, 64].

We have shown that multicore optical fibers provide a suitable platform to implement NM maps in higher dimensions through the probabilistic application of unitary operations in each fiber core optical mode. We used such technique in a proof-of-principle experiment to show that under a restricted scenario for phase flips, if the multicore fiber is used as a quantum memory, NM maps may lead the system evolution to a regime where information backflow from the environment to the system is observed. Thus, enabling the use of the system as a quantum vault where information is harder to retrieve along the evolution than at the end of it.

The set of errors used in our study serves as a reliable proving ground that can be extended (with $s > 2$) to include more noisy operations affecting open systems in actual communication networks implemented over installed multicore optical fibers. A further study of transition map models in multicore fibers could be useful for both classical and quantum communication tasks since a deep understanding of the noise contribution could lead to the implementation of noise passive filters, thus reducing the complexity and cost of communication infrastructure networks.

Acknowledgments

This work was supported by Fondo Nacional de Desarrollo Científico y Tecnológico (ANID) (Grants No. 3200779, 1200266, 1231940, 1200859, 1240746) and ANID – Millennium Science Initiative Program – ICN17_012. K.S. acknowledges financial support from project UCO 1866. LP was supported by ANID-PFCHA/DOCTORADO-BECAS-CHILE/2019-772200275, the CSIC Interdisciplinary Thematic Platform (PTI+) on Quantum Technologies (PTI-QTEP+), and the Proyecto Sinérgico CAM 2020 Y2020/TCS-6545 (NanoQuCo-CM). N.K.B. acknowledges financial support from CAPES, CNPq Brazil (Universal Grant No. 406499/2021-7), and FAPESP (Grant 2021/06035-0). N.K.B. is part of the Brazilian National Institute for Quantum Information (INCT Grant 465469/2014-0).

References

[1] Robert Maher, Alex Alvarado, Domaniç Lavery, and Polina Bayvel. "Increasing the information rates of optical communications via coded modulation: a study of transceiver performance". Sci. Rep. **6**, 21278 (2016).

[2] C.A. Brackett. "Dense wavelength division multiplexing networks: principles and applications". IEEE Journal on Selected Areas in Communications **8**, 948–964 (1990).

[3] D. J. Richardson, J. M. Fini, and L. E. Nelson. "Space-division multiplexing in optical fibres". Nature Photon. **7**, 354–362 (2013).

[4] Tetsuya Hayashi, Toshiki Taru, Osamu Shimakawa, Takashi Sasaki, and Eisuke Sasaoka. "Design and fabrication of ultra-low crosstalk and low-loss multi-core fiber". Opt. Express **19**, 16576–16592 (2011).

[5] Jun Sakaguchi, Benjamin J. Puttnam, Werner Klaus, Yoshinari Awaji, Naoya Wada, Atsushi Kanno, Tetsuya Kawanishi, Katsunori Imamura, Harumi Inaba, Kazunori Mukasa, Ryuichi Sugizaki, Tetsuya Kobayashi, and Masayuki Watanabe. "19-core fiber transmission of 19×100×172-Gb/s SDM-WDM-PDM-QPSK signals at 305Tb/s". In National Fiber Optic Engineers Conference. Page PDP5C.1. Optica Publishing Group (2012).

[6] Werner Klaus, Jun Sakaguchi, Benjamin J. Puttnam, Yoshinari Awaji, Naoya Wada, Tetsuya Kobayashi, and Masayuki Watanabe. "Free-space coupling optics for multicore fibers". IEEE Photonics Technology Letters **24**, 1902–1905 (2012).

[7] G. Cañas, N. Vera, J. Cariñe, P. González, J. Cardenas, P. W. R. Connolly, A. Przysiezna, E. S. Gómez, M. Figueroa, G. Vallone, P. Villoresi, T. Ferreira da Silva, G. B. Xavier, and G. Lima. "High-dimensional decoy-state quantum key distribution over multicore telecommunication fibers". Phys. Rev. A **96**, 022317 (2017).

[8] J. F. Dynes, S. J. Kindness, S. W.-B. Tam, A. Plews, A. W. Sharpe, M. Lucamarini,

B. Fröhlich, Z. L. Yuan, R. V. Penty, and A. J. Shields. "Quantum key distribution over multicore fiber". Opt. Express **24**, 8081–8087 (2016).

[9] Guilherme B. Xavier and Gustavo Lima. "Quantum information processing with space-division multiplexing optical fibres". Commun. Phys. **3**, 9 (2020).

[10] J. Cariñe, G. Cañas, P. Skrzypczyk, I. Šupić, N. Guerrero, T. Garcia, L. Pereira, M. A. S. Prosser, G. B. Xavier, A. Delgado, S. P. Walborn, D. Cavalcanti, and G. Lima. "Multi-core fiber integrated multi-port beam splitters for quantum information processing". Optica **7**, 542–550 (2020).

[11] J. Cariñe, M. N. Asan-Srain, G. Lima, and S. P. Walborn. "Maximizing quantum discord from interference in multi-port fiber beamsplitters". npj Quantum Information **7**, 172 (2021).

[12] Márcio M. Taddei, Jaime Cariñe, Daniel Martínez, Tania García, Nayda Guerrero, Alastair A. Abbott, Mateus Araújo, Cyril Branciard, Esteban S. Gómez, Stephen P. Walborn, Leandro Aolita, and Gustavo Lima. "Computational advantage from the quantum superposition of multiple temporal orders of photonic gates". PRX Quantum **2**, 010320 (2021).

[13] Daniel Martínez, Esteban S. Gómez, Jaime Cariñe, Luciano Pereira, Aldo Delgado, Stephen P. Walborn, Armin Tavakoli, and Gustavo Lima. "Certification of a non-projective qudit measurement using multiport beamsplitters". Nat. Phys. (2022).

[14] Hee Jung Lee, Sang-Kyung Choi, and Hee Su Park. "Experimental demonstration of four-dimensional photonic spatial entanglement between multi-core optical fibres". Sci. Rep. **7**, 4302 (2017).

[15] Hee Jung Lee and Hee Su Park. "Generation and measurement of arbitrary four-dimensional spatial entanglement between photons in multicore fibers". Photon. Res. **7**, 19–27 (2019).

[16] Esteban S. Gómez, S. Gómez, I. Machuca, A. Cabello, S. Pádua, S.P. Walborn, and G. Lima. "Multidimensional entanglement generation with multicore optical fibers". Phys. Rev. Appl. **15**, 034024 (2021).

[17] Michael A. Nielsen and Isaac L. Chuang. "Quantum computation and quantum information". Cambridge University Press. Cambridge; New York (2010). 10th anniversary ed edition.

[18] B. Bylicka, D. Chruściński, and S. Maniscalco. "Non-markovianity and reservoir memory of quantum channels: a quantum information theory perspective". Sci. Rep. **4**, 5720 (2014).

[19] M. M. Wolf, J. Eisert, T. S. Cubitt, and J. I. Cirac. "Assessing non-markovian quantum dynamics". Phys. Rev. Lett. **101**, 150402 (2008).

[20] Heinz-Peter Breuer, Elsi-Mari Laine, and Jyrki Piilo. "Measure for the degree of non-markovian behavior of quantum processes in open systems". Phys. Rev. Lett. **103**, 210401 (2009).

[21] Ángel Rivas, Susana F Huelga, and Martin B Plenio. "Quantum non-markovianity: characterization, quantification and detection". Rep. Prog. Phys. **77**, 094001 (2014).

[22] Ruggero Vasile, Sabrina Maniscalco, Matteo G. A. Paris, Heinz-Peter Breuer, and Jyrki Piilo. "Quantifying non-markovianity of continuous-variable gaussian dynamical maps". Phys. Rev. A **84**, 052118 (2011).

[23] Jun-Hong An and Wei-Min Zhang. "Non-markovian entanglement dynamics of noisy continuous-variable quantum channels". Phys. Rev. A **76**, 042127 (2007).

[24] F. F. Fanchini, G. Karpat, B. Çakmak, L. K. Castelano, G. H. Aguilar, O. Jiménez Farías, S. P. Walborn, P. H. Souto Ribeiro, and M. C. de Oliveira. "Non-markovianity through accessible information". Phys. Rev. Lett. **112**, 210402 (2014).

[25] S. Haseli, G. Karpat, S. Salimi, A. S. Khorashad, F. F. Fanchini, B. Çakmak, G. H. Aguilar, S. P. Walborn, and P. H. Souto Ribeiro. "Non-markovianity through flow of information between a system and an environment". Phys. Rev. A **90**, 052118 (2014).

[26] Jiasen Jin, Vittorio Giovannetti, Rosario Fazio, Fabio Sciarrino, Paolo Mataloni, Andrea Crespi, and Roberto Osellame. "All-optical non-markovian stroboscopic quantum simulator". Phys. Rev. A **91**, 012122 (2015).

[27] Nadja K. Bernardes, Alvaro Cuevas, Adeline Orieux, C. H. Monken, Paolo Mataloni, Fabio Sciarrino, and Marcelo F. Santos. "Experimental observation of weak non-Markovianity". Sci. Rep. **5**, 17520 (2015).

[28] Álvaro Cuevas, Andrea Geraldi, Carlo Liorni, Luís Diego Bonavena, Antonella De Pasquale, Fabio Sciarrino, Vittorio Giovannetti, and Paolo Mataloni. "All-optical implementation of collision-based evolutions of open quantum systems". Sci. Rep. **9**, 3205 (2019).

[29] A. Salles, F. de Melo, M. P. Almeida, M. Hor-Meyll, S. P. Walborn, P. H. Souto Ribeiro, and L. Davidovich. "Experimental investigation of the dynamics of entanglement: Sudden death, complementarity, and continuous monitoring of the environment". Phys. Rev. A **78**, 022322 (2008).

[30] B. Marques, A. A. Matoso, W. M. Pimenta, A. J. Gutiérrez-Esparza, M. F. Santos, and S. Pádua. "Experimental simulation of decoherence in photonics qudits". Sci. Rep. **5**, 16049 (2015).

[31] G. H. Aguilar, A. Valdés-Hernández, L. Davidovich, S. P. Walborn, and P. H. Souto Ribeiro. "Experimental entanglement redistribution under decoherence channels". Phys. Rev. Lett. **113**, 240501 (2014).

[32] M. Ringbauer, C. J. Wood, K. Modi, A. Gilchrist, A. G. White, and A. Fedrizzi. "Characterizing quantum dynamics with initial system-environment correlations". Phys. Rev. Lett. **114**, 090402 (2015).

[33] Daniel F. Urrego, Jefferson Flórez, Ji ří Svozilík, Mayerlin Nuñez, and Alejandra Valencia. "Controlling non-markovian dynamics using a light-based structured environment". Phys. Rev. A **98**, 053862 (2018).

[34] Adeline Orieux, Antonio D'Arrigo, Giacomo Ferranti, Rosario Lo Franco, Giuliano Benenti, Elisabetta Paladino, Giuseppe Falci, Fabio Sciarrino, and Paolo Mataloni. "Experimental on-demand recovery of entanglement by local operations within non-Markovian dynamics". Sci. Rep. **5**, 8575 (2015).

[35] Thais de Lima Silva, Stephen P. Walborn, Marcelo F. Santos, Gabriel H. Aguilar, and Adrián A. Budini. "Detection of quantum non-markovianity close to the born-markov approximation". Phys. Rev. A **101**, 042120 (2020).

[36] Susana F. Huelga, Ángel Rivas, and Martin B. Plenio. "Non-markovianity-assisted steady state entanglement". Phys. Rev. Lett. **108**, 160402 (2012).

[37] Nicolás Mirkin, Pablo Poggi, and Diego Wisniacki. "Entangling protocols due to non-markovian dynamics". Phys. Rev. A **99**, 020301 (2019).

[38] Namit Anand and Todd A. Brun. "Quantifying non-markovianity: a quantum resource-theoretic approach" (2019). arXiv:1903.03880.

[39] Graeme D. Berk, Andrew J. P. Garner, Benjamin Yadin, Kavan Modi, and Felix A. Pollock. "Resource theories of multi-time processes: A window into quantum non-Markovianity". Quantum **5**, 435 (2021).

[40] Samyadeb Bhattacharya, Bihalan Bhattacharya, and A S Majumdar. "Convex resource theory of non-markovianity". Journal of Physics A: Mathematical and Theoretical **54**, 035302 (2020).

[41] Zhi He, Hao-Sheng Zeng, Yan Li, Qiong Wang, and Chunmei Yao. "Non-markovianity measure based on the relative entropy of coherence in an extended space". Phys. Rev. A **96**, 022106 (2017).

[42] Carlos Pineda, Thomas Gorin, David Davalos, Diego A. Wisniacki, and Ignacio García-Mata. "Measuring and using non-markovianity". Phys. Rev. A **93**, 022117 (2016).

[43] D.P. DiVincenzo, D.W. Leung, and B.M. Terhal. "Quantum data hiding". IEEE Transactions on Information Theory **48**, 580–598 (2002).

[44] A. Tapp, A. Ambainis, R. de Wolf, and M. Mosca. "Private quantum channels". In 2013 IEEE 54th Annual Symposium on Foundations of Computer Science. Page 547. Los Alamitos, CA, USA (2000). IEEE Computer Society.

[45] C. Lupo, M. M. Wilde, and S. Lloyd. "Quantum data hiding in the presence of noise". IEEE Trans. Inf. Theory **62**, 3745 (2016).

[46] H.P. Breuer and F. Petruccione. "The

Theory of Open Quantum Systems". Oxford University Press. (2007).

[47] Robert Fischer, Itamar Vidal, Doron Gilboa, Ricardo R. B. Correia, Ana C. Ribeiro-Teixeira, Sandra D. Prado, Jandir Hickman, and Yaron Silberberg. "Light with tunable non-markovian phase imprint". Phys. Rev. Lett. **115**, 073901 (2015).

[48] Toni Eichelkraut and Alexander Szameit. "Random sudoku light". Nature **526**, 643–644 (2015).

[49] Kang-Da Wu, Zhibo Hou, Guo-Yong Xiang, Chuan-Feng Li, Guang-Can Guo, Daoyi Dong, and Franco Nori. "Detecting non-Markovianity via quantified coherence: theory and experiments". npj Quantum Inf. **6**, 55 (2020).

[50] John Von Neumann. "Mathematical Foundations of Quantum Mechanics; New Edition". Princeton University Press. Princeton (2018).

[51] A S Holevo and V Giovannetti. "Quantum channels and their entropic characteristics". Rep. Prog. Phys. **75**, 046001 (2012).

[52] Benjamin Schumacher and M. A. Nielsen. "Quantum data processing and error correction". Phys. Rev. A **54**, 2629–2635 (1996).

[53] Seth Lloyd. "Capacity of the noisy quantum channel". Phys. Rev. A **55**, 1613–1622 (1997).

[54] Dan C. Marinescu and Gabriela M. Marinescu. "Classical and Quantum Information". Academic Press. Burlington, MA (2012).

[55] Julian Schwinger. "Unitary operator bases". Proc. Natl. Acad. Sci. U.S.A. **46**, 570–579 (1960).

[56] I D Ivonovic. "Geometrical description of quantal state determination". J. Phys. A **14**, 3241–3245 (1981).

[57] William K Wootters and Brian D Fields. "Optimal state-determination by mutually unbiased measurements". Ann. Phys. **191**, 363–381 (1989).

[58] A. B. Klimov, C. Muñoz, A. Fernández, and C. Saavedra. "Optimal quantum-state reconstruction for cold trapped ions". Phys. Rev. A **77**, 060303 (2008).

[59] S N Filippov and V I Man'ko. "Mutually unbiased bases: tomography of spin states and the star-product scheme". Phys. Scr. **T143**, 014010 (2011).

[60] R. B. A. Adamson and A. M. Steinberg. "Improving quantum state estimation with mutually unbiased bases". Phys. Rev. Lett. **105**, 030406 (2010).

[61] G. Lima, L. Neves, R. Guzmán, E. S. Gómez, W. A. T. Nogueira, A. Delgado, A. Vargas, and C. Saavedra. "Experimental quantum tomography of photonic qudits via mutually unbiased basis". Opt. Express **19**, 3542–3552 (2011).

[62] Jiangwei Shang, Zhengyun Zhang, and Hui Khoon Ng. "Superfast maximum-likelihood reconstruction for quantum tomography". Phys. Rev. A **95**, 062336 (2017).

[63] Shrikant U. and Mandayam P. "Quantum non-markovianity: Overview and recent developments". Front. Quantum. Sci. Technol. **2**, 1134583 (2023).

[64] Francesco Buscemi, Rajeev Gangwar, Kaumudibikash Goswami, Himanshu Badhani, Tanmoy Pandit, Brij Mohan, Siddhartha Das, and Manabendra Nath Bera. "Information revival without backflow: non-causal explanations of non-Markovianity" (2024). arXiv:2405.05326.

[65] Howard Barnum, M. A. Nielsen, and Benjamin Schumacher. "Information transmission through a noisy quantum channel". Phys. Rev. A **57**, 4153–4175 (1998).

Supplementary material

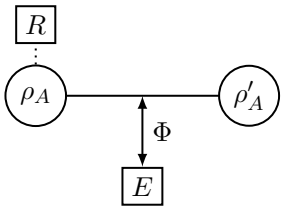
Coherent information and channel privacy

We will now discuss in more detail the original definition of coherent information and its relation to the privacy of a quantum channel. Consider that in addition to the original system A, we have a replica of it (either physical or just a mathematical device) that serves as a reference or ancilla system R. Consider a quantum channel Φ which acts only in the system A and describes its interaction with the environment E. This channel transforms the initial state ρ_A of A into a final state ρ'_A. Generally, ρ is a mixed state but can be purified in the bipartite Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_R$. The purification of ρ is given by

the entangled state $|\Psi_{AR}\rangle$. We can express the evolution of the extended system AR by means of the superoperator $\Phi \otimes \mathbb{1}_R$ to obtain

$$\rho'_{AR} = \{\Phi \otimes \mathbb{1}_R\} \left(|\Psi_{AR}\rangle \langle \Psi_{AR}| \right). \tag{9}$$

This translates into the following scheme:



Now, consider the entropy $S(\rho'_{AR})$ of the bipartite system composed of the output and the ancilla. Since this subsystem is not affected by the evolution, $S(\rho'_{AR})$ can still be considered as an intrinsic property of the system A, depending only on its initial state ρ_A and the channel Φ [52]. Still, if the environment is initially in a pure state, we can identify $S(\rho'_{AR})$ with its entropy after evolution. The previous statements allow us to define the entropy exchange,

$$S(\rho_A, \phi) = S(\rho'_{AR}) = S(\rho'_E), \tag{10}$$

as the amount of information exchanged between A and the environment. The last identity comes from the fact that the tripartite state in the extended system ARE remains pure along the evolution. Upon the entropy exchange, we define the two intrinsic quantities introduced in Sec. 3, namely, the quantum mutual information and the coherent quantum information. This last quantity, given by

$$I_c(\rho_A, \Phi) = S(\Phi[\rho_A]) - S(\rho_A, \phi), \tag{11}$$

measures the degree of quantum correlation retained by R and A during the evolution, so it is considered as a proper measure of the nonclassicality of the final state ρ'_{AR}. The previous definitions provide a formal connection between our map and the task of *quantum data hiding* [43, 44]. In this context, removing correlations between A and R allows to hide quantum information by transferring them to the environment (cf. [64]). This is quantified by the entropy exchange and the associated reduction of the coherent information.

Consider the evolution of the coherent information I_c under the map Λ_t, shown in Fig. 3 (e,f). This is obtained by taking the chaotic initial state $\rho_A = \mathbb{1}/4$, whose purification is given by a maximally entangled state. As t increases, the corresponding quantum channel Φ_{p_0} reduces its coherent information due to the entropy exchange: the information is hidden in the environment. This highlights the key role of the inaccessible environment in our model for implementing the quantum vault. As the system interacts with the environment, neither Alice nor Eve can obtain the information stored in its initial state.

Conveniently enough, further evolution of the system in the non-Markovian regime allows for partial o complete information recovery. In the optimal case [Fig 3 (a)] the information is fully restored, so the coherent information reaches its maximal value at the output:

$$I_c(\rho'_A) = I_c(\rho_A) = s(\rho_A). \tag{12}$$

This way, it is shown that in the optimal scenario, Λ_t allows for a quantum private channel in the limit $p_0 \longrightarrow 0$, after performing quantum data hiding during the evolution, maximally at $p_0 = p_{\min}$. The previous results can be expressed by means of another information quantity obtained from a different partition of the extended system ARE, namely, the *loss* given by

$$\begin{aligned} L(\rho, \Phi) &= S(\rho_R) + S(\rho'_E) - S(\rho'_{RE}) \\ &= S(\rho_A) + S(\rho, \Phi) - S(\rho'_A). \end{aligned} \tag{13}$$

Notice that it corresponds to the quantum mutual information between the input and the environment. The loss is non-negative, and it is null only if the state ρ'_{RE} is separable, i.e. in the absence of correlations between the R and E, meaning that no information has leaked into the environment. Indeed, it has been shown that $L(\rho, \Phi) = 0$ is equivalent to Eq. (12), allowing for a completely private channel [51, 65]. This is attained in our optimal case, where all the information has flown back from the environment to the system at the end of the evolution.

QV protocol in different scenarios

The implementation of the QV in Sec. 4.1 considers the optimal scenario in the $s = 2$ case, where phase permutations can only occur simultaneously on both subsets of cores ($p_1 = p_2 = 0$ and $p_3 = 1 - po$). With this restriction,

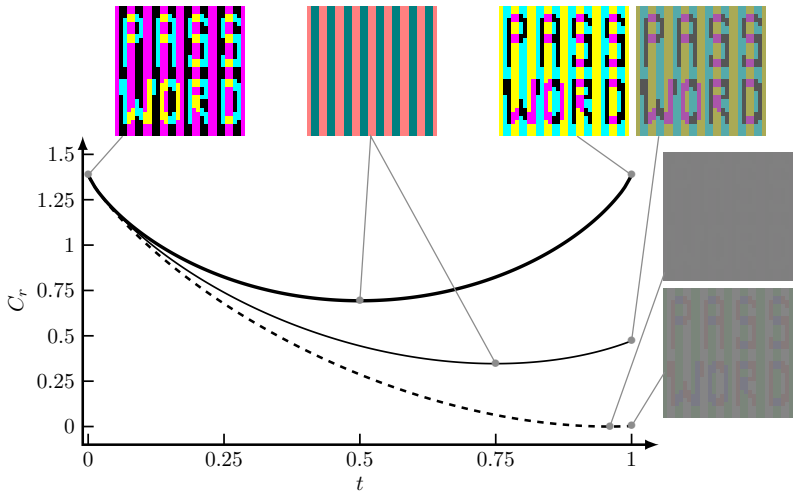


Figure 6: Implementation of the quantum vault protocol to store an image, using the noisy map Λ_t in three different scenarios. Each qudit in the 4-dimensional canonical basis is associated with a specific color of the cyan-magenta-yellow-black (CMYK) model. At the input stage, Alice stores a message as an image whose pixels have one of the base colors. As the system evolves, distinguishability between different pairs of states in the basis is reduced, which is reflected by a decrease in the quantum mutual information (which quantifies the capacity of a quantum channel to convey a classical message). At $t = 1-p_{\min}$, the capacity is minimal, rendering the message of the image unreadable. Non-Markovian dynamics in the final stage of the evolution lead to an increase in the quantum mutual information with the respective revival of distinguishability, allowing Alice to retrieve her information. In the simplified scenario where $p_1 = p_2 = 0$ (thick line), a full recovery is possible, even if the final state of each pixel is different from their initial state (colors are swapped in the retrieved image). In the uniform scenario $p_1 = p_2 = p_3 = (1 - p_0)/3$ (thin line), there is a partial revival of distinguishability, allowing one to read the message. Finally, the unrestricted scenario with $s = 4$ (dashed line), where permutations between all the cores can occur, enables complete encryption of the image at the minimum, at the expense of a low recovery in the output.

the relative entropy of coherence increases back to its initial value, allowing a complete information backflow at the end of the evolution. In Fig. 6, we compare how the QV performs in this optimal case and more unrestricted scenarios. The information backflow in the former case is reflected by the output image, all of whose pixels are in a pure color of the CMYK base, just like the image initially stored by Alice. In the uniform case $p_{i\neq 0} = (1-p_0)/3$ (thin filled curve) evolution until $p_0 = 1/4$ put the pixels in the same two mixtures as before. However, their state is not pure at the end of the evolution so Alice can recover the information only partially. Finally, the more realistic case $s = 4$, where permutations can occur between all the four cores (dashed curve), enables full encryption of Alice's message, with all the base states evolving to the same mixed state, or equivalently, all the pixels in the image becoming gray. This comes at the cost of a very poor recovery at the end of the evolution, reflected by a barely readable message in the output image. This is related to the fact that the value of $p_{\min}$ in (6) is inversely proportional to the number of available permutations affecting the evolution.

B Submitted Paper: Efficient Experimental Qudit State Estimation via Point Tomography

In this section we reproduce, in full, an article submitted by us to the journal Physical Review Letters in 2024 [46]. As in the previous section, this article is based on the same experimental setup with Alice connected directly to Bob. However, in this case Bob's 4C-MBS is swapped out for a 7C-MBS (seven-core multicore beam splitter), with one detector at each of its seven outputs, in order to implement a POVM on a four-dimensional state.

Efficient Experimental Qudit State Estimation via Point Tomography

D. Martínez,[1,2] L. Pereira,[3] K. Sawada,[1] P. González,[1] J. Cariñe,[4]
M. Muñoz,[5] A. Delgado,[1] E. S. Gómez,[1] S. P. Walborn,[1] and G. Lima[1]

[1]*Departamento de Física and Millennium Institute for Research in Optics, Universidad de Concepción, 160-C Concepción, Chile*
[2]*Vienna Center for Quantum Science and Technology (VCQ) and Christian Doppler Laboratory for Photonic Quantum Computer, Faculty of Physics, University of Vienna, 1090 Vienna, Austria*
[3]*Instituto de Física Fundamental IFF-CSIC, Calle Serrano 113b, Madrid 28006, España*
[4]*Departamento de Ingeniería Eléctrica, Universidad Católica de la Santísima Concepción, Concepción, Chile*
[5]*Departamento de Ingeniería Matemática and Centro de Investigación en Ingeniería Matemática (CI^{2}MA), Universidad de Concepción, 160-C Concepción, Chile*

(Dated: November 30, 2024)

Point tomography is a new approach to the problem of state estimation, which is arguably the most efficient and simple method for modern high-precision quantum information experiments. In this scenario, the experimenter knows the target state that their device should prepare, except that intrinsic systematic errors will create small discrepancies in the state actually produced. By introducing a new kind of informationally complete measurement, dubbed Fisher-symmetric measurements, point tomography determines deviations from the expected state with optimal efficiency. In this method, the number of outcomes of a measurement saturating the Gill-Massar limit for the reconstruction of d-dimensional quantum states can be reduced from $\sim 4d-3$ to only $2d-1$ outcomes. Thus, providing better scalability as the dimension increases. Here we demonstrate the experimental viability of point tomography. Using a modern photonic platform constructed with state-of-the-art multicore optical fiber technology, we generate 4-dimensional quantum states and implement seven-outcome Fisher-symmetric measurements efficiently. Our experimental results exhibit the main feature of point tomography, namely a precision close to the Gill-Massar limit with a single few-outcome measurement. Specifically, we achieved a precision of $3.8/N$ while the Gill-Massar limit for $d=4$ is $3/N$ (N being the ensemble size).

Introduction– High-dimensional quantum states (qudits) exhibit important advantages over bi-dimensional systems for quantum information processing. For instance, qudits can increase sensitivity in quantum metrology [1–3] and efficiency in quantum computing [4–8]. Nonetheless, the benefits of adopting qudit states may be overshadowed by the difficulty in estimating them accurately, impairing our capability to generate, control, and transmit them. This has led to the design of various estimation methods aimed at achieving high estimation precision or reducing the resources required by the estimation process. Modern adaptive quantum tomography methods, for example, rely on interactive algorithms to reach the Gill-Massar limit [9] for some particular quantum states [10–14]. Unfortunately, in general, their efficiencies quickly degrade or the protocol become too complex to implement as the dimension of the system increases [15].

Single-setting tomographic methods provide an alternative to adaptive methods [16]. In this approach, a single positive-operator-valued measure (POVM) is used for the state reconstruction. If the recorded statistics of the outcomes of the POVM are sufficient to reconstruct the quantum state, the POVM is said to be informationally complete. The POVM is also said to be globally informationally complete if it can be used to reconstruct any unknown quantum state, in which case the POVM must have at least d^2 elements [16, 22] for a d-dimensional system. There have been several theoretical and experimental studies adopting globally informationally complete POVMs [17–21]. Nevertheless, since the scalability of the number of outcomes is demanding, many of the experimental demonstrations actually do not fully implement the required generalized measurement. Instead, they rely on measuring the statistics of each outcome independently and, therefore, the simplicity provided by single-setting tomography is replaced by d^2 different measurements.

A modern take on POVM-based state reconstruction is provided by point tomography [22, 23], which finds practical relevance for modern quantum platforms that can achieve high-precision in quantum information tasks. Point tomography departs from previous methods by relying not on globally- but instead on locally-complete POVMs. The new kind of measurement used, namely Fisher-symmetric measurements, are chosen such that the Fisher information is distributed uniformly among a set of parameters that uniquely identify quantum states in the neighborhood of an arbitrary target state. Thus, point tomography neatly applies to the situation where the experimentalist has a well-characterized preparation device that emits a state with only small systemic deviations from the target state. Choosing the proper POVM, the method can saturate the Gill-Massar limit. Besides high-precision, point tomography has another huge practical advantage. By resorting only to locally complete POVMs, the number of POVM outcomes can be drastically reduced, giving much better scalability when applied to higher dimensions. In the case of pure quantum states, the number of outcomes can be reduced from $\sim 4d-3$ to only $2d-1$ [22, 23].

Here, we use state-of-the-art multicore optical fiber technology to demonstrate for the first time the experimental viability of this point tomography method. With this new

photonic platform, we are able to generate path-encoded four-dimensional quantum states with a high degree of precision [24], and implement high-fidelity genuine seven-outcome POVMs [25]. Our experimental results exhibit the main feature of point tomography, namely a precision close to the Gill-Massar limit with a single few-outcome Fisher-symmetric measurement. A fit of the experimental data provides an estimation accuracy of $3.8/N$ while the Gill-Massar limit for $d = 4$ is $3/N$ (N being the ensemble size). This result is even valid for an ensemble as small as $N = 50$. Furthermore, we also experimentally test the method for states in a broader neighborhood. In this case the estimation precision decreases, as expected, but we see that for small ensembles it is still possible to achieve a precision comparable to the Gill-Massar limit. Our results help pave the way for a broader adoption of point tomography, which resonates well with all modern quantum platforms being developed for high-precision quantum information processing [26, 27].

Method– As discussed above, a priori information is used in the construction of Fisher-symmetric measurements. That is, the state $|\psi\rangle$ to be estimated must be in the neighborhood of a given arbitrary fiducial state $|0\rangle$

$$|\psi\rangle = \frac{1}{A}\left(|0\rangle + \sqrt{\theta}\sum_{j=1}^{3}|j\rangle\right), \tag{1}$$

where A is a normalization constant, $\{|j\rangle\}$ with $j = 1,\ldots,d-1$ is an orthornormal basis, and the coefficient θ is infinitesimal $|\theta|^2 \lll 1$. The quality of the characterization depends on how small this parameter is. Then, the aim of point tomography is to estimate $|\psi\rangle$ with the ultimate precision provided by the Gill-Massar bound, while also maintaining the classical fisher information matrix uniformly distributed over the target state $|0\rangle$. As has been demonstrated in Ref. [22], all rank-1 POVMs $|\phi^\eta\rangle\langle\phi^\eta|$ ($\eta = 1,\ldots,2d-1$), with $|\phi^\eta\rangle = \sum_{j=0}^{d-1} a_j^\eta |j\rangle$ and a_0^η real, define a Fisher-symmetric measurement if the matrix C, with elements $C_{j,k} = \sum_{\eta=1}^{2d-1} a_j^\eta a_k^\eta$ ($j,k = 1,\ldots,d-1$), has null norm.

Recently, a method to implement POVMs in a d-dimensional Hilbert space using $D \times D$ modern multiport beam splitters (MBS) was presented [25]. For a photonic qudit, encoded in terms of d spatial optical modes, a rank-1 POVM is realized by connecting these modes to d of the D inputs of the MBS ($D > d$). Thus, by connecting different sets of inputs, there are $D!/[d!(D-d)!]$ different classes of possible POVMs that can be implemented. Exploiting the fact that relative phases can be imprinted between the optical modes before the MBS, the rank-1 POVM elements are proportional to the states

$$|\eta_j\rangle = \Phi^\dagger_{k_1\cdots k_d} M_{k_1\cdots k_d}|j\rangle, \tag{2}$$

where $k_1\cdots k_d$ defines the connected input modes of the MBS, $\Phi_{k_1\cdots k_d}$ is a diagonal matrix defining the phases applied before the MBS, and $M_{k_1\cdots k_d}$ is a $D \times d$ matrix, which is the part of the MBS $D \times D$ unitary matrix acting on the modes $k_1\cdots k_d$ [25].

In this work, we are interested on implementing a fisher symmetric 7-outcome measurement onto a 4-dimensional fiducial state using the technique of Ref. [25]. In this case, there are 35 different types of POVMs defined by Eq. (2) that could possibly be used in point tomography. For our particular implementation, these measurements are given explicitly in the supplemental material [28]. In order to select the best POVM candidate, we minimize the 2-norm of the matrix C for each family of feasible POVMs. We find that even though we cannot implement a Fisher symmetric measurement exactly, there is a configuration close to a perfect one, where the corresponding matrix C has norm $||C|| \approx 0.63$ [28].

Experiment– Our experimental setup is depicted in Fig. 1. It has two main stages dedicated for state preparation and POVM implementation. The experiment relies on modern multi-core optical fiber (MCF) technologies, which have been developed to meet the increasing demand for bandwidth in optical communication networks [29]. In MCFs, light is transmitted through multiple single-mode cores that are contained within a common cladding. Since the crosstalk between them is depreciable, such core modes can be used to encode d-dimensional photonic quantum systems. Because the cores are within the same cladding, the platform is inherent robust against thermal and mechanical perturbations to the quantum system, as they act like global effects. In a series of independent studies (See Ref. [30] for a comprehensive review), such platform has been shown to achieve high-precision in many different quantum information tasks, ranging from high-dimensional quantum communication [31–34], entanglement generation [35–38], to more efficient quantum computing approaches [8].

The purpose of the preparation stage is to generate 4-dimensional quantum states. This is accomplished by using the path-encoding strategy for a single photon propagating over a 4-core fiber [24]. The basis states $|i\rangle$, with $i = 0,1,2,3$, denote the state of a photon transmitted by the i-th core of the MCF. In our setup, a semiconductor telecom CW-laser operating at 1546 nm, followed by an attenuator (Att), and an external fiber-pigtailed intensity modulator (IM), are used to generate weak coherent states comprised of 5 ns-long pulses at a rate of 2 MHz. The IM is controlled by a field programmable gate array unit (FPGA). The mean photon number per pulse generated is adjusted to $\mu = 0.10$. In this case, the contribution of multi-photon events to the recorded statistics is only 4.7% and is, therefore, negligible. The generated single-photon is first sent over a single-core fiber of a DMUX, which is a device composed of N single-core fibers connected to a single N-core fiber, where each single-core fiber is mapped to one of the cores of the MCF. The single-photon is then transmitted to one of the cores of the 4C-MCF at the end of the DMUX.

This first DMUX is connected to a 4×4 MBS (4C-MBS in Fig. 1). The 4×4 MBSs are manufactured by locally heating a small transverse region of a homogeneous 4-core fiber and applying a controlled longitudinal stretching tension. This leads to a tapered fiber where, due to evanescent coupling,

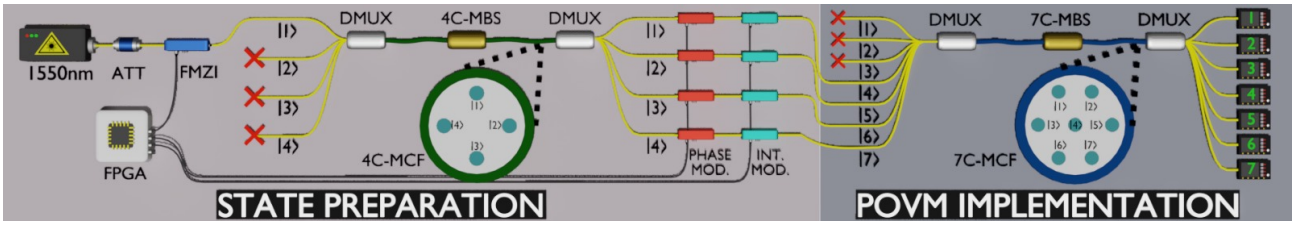


FIG. 1. Experimental setup. In the preparation stage, single photon states are generated with a CW-laser, an attenuator (Att), and an Mach-Zehnder based intensity modulator (FMZI). The light is distributed from one of the fiber cores to all four of them by a 4C-MBS (4-core multicore beam splitter). The cores are separated into fibers and the intensity and phase of each one are modulated by phase modulators (PMs) and variable intensity modulators (IM) to prepare four-dimensional single-photon states. In the measurement stage, the four fibers are fed into a 7C-MBS (7-core multicore beam splitter) and each of the seven outputs is sent to a single-photon detector (D1 through D7). Since the number of outcomes from the 7C-MBS is greater than 4, the corresponding measurement is a POVM. See the main text for details.

photons will jump from one core to the others [24]. The 4C-MBS has a mean fidelity of $F = 0.995 \pm 0.003$ [24] with respect to the unitary matrix

$$U_4 = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, \tag{3}$$

while achieving an almost ideal split ratio of 25% (0.248 ± 0.01 [24]). Thus, after the propagation through the MBS, the photon is found in a equally weighted coherent superposition of the $|i\rangle$ basis states. Next, the 4×4 MBS is connected to another DMUX in reverse. Each of the 4 single-core fibers coming from this DMUX is supplemented with phase and intensity modulators (PMs and IMs, respectively) to control state parameters. While the IM voltages can be set manually, the PM voltages must be constantly adjusted as the optical paths on the single-mode fibers slowly drift. This is accomplished by having FPGA controlling the PMs with a feed-back algorithm based on counts recorded by the single-photon detectors. At this stage of the setup, single-photon states $|\chi\rangle = \sum_{i=0}^{3} \alpha_j e^{i\phi_i}|i\rangle$ can be generated, thus defining the preparation stage for four-dimensional path-encoded states.

The single photons are then sent to the measurement stage through 4 single-core fibers connected to the third and different DMUX, which now maps 7 single-core fibers into a single 7-core fiber. Four of the DMUX's inputs are connected to these fibers, while the others three are not connected to any light source. The DMUX's output is connected to a 7×7 MBS (7C-MBS in Fig. 1)) that is followed by another DMUX, which is identical to the third DMUX but in reverse. Finally, the light coming out of each of the 7 single-core fibers is detected with InGaAs single-photon detection modules (D1 through D7). The FPGA records the counts of all detectors. This combination of DMUXs, MBS, and detectors defines the measurement stage, which realizes a POVM with 7 elements acting on the 4-dimensional state $|\chi\rangle$. The elements of the POVM are dependent on which of the input fibers are used, as well as the 7×7 matrix describing the MBS. The process tomography of the 7×7 MBS used in our experiment was presented in Ref. [24] and its matrix is given explicitly in the supplemental material [28]. The chosen POVM, to study experimentally the method of point tomography, is obtained when the 4 outputs of the preparation stage are connected to the inputs $i = 4,5,6$ and 7 of the measurement stage [28].

Results– We experimentally study the estimation accuracy achievable by the method of point tomography while considering three different states $|\psi_i\rangle$ (see Eq. (1)), with $\theta_1 = 10^{-2}$, $\theta_2 = 10^{-1}$, and $\theta_3 = 2\times10^{-1}$. As θ_i increases, the states $|\psi_i\rangle$ move away from the fiducial state $|0\rangle$ and the efficiency of the estimation process is expected to decrease.

The statistics generated by the measurement, for each state and for each ensemble size, is post-processed by the maximum likelihood estimation technique [39], which delivers the final estimate $|\tilde{\psi}_i\rangle$ of $|\psi_i\rangle$ and the corresponding infidelity $I_F = 1 - F(|\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|, \rho_i)$, where $F(:)$ is the fidelity between quantum states. The error of the infidelity value experimentally recorded is calculated using the bootstrapping technique. To model the experimental results, we assume the traditional white noise model affecting the preparation and measurement stages. This leads to the consideration of a highly pure albeit mixed state of the form $\rho_i = \lambda|\psi_i\rangle\langle\psi_i| + (\lambda-1)I/d$ (with $\lambda = 0.987$) to proper describe our experiment. We also account for systematic errors in our error model.

The experimental results are presented in Fig. 2a, Fig. 2b, and Fig. 2c for states $|\psi_1\rangle, |\psi_2\rangle$, and $|\psi_3\rangle$, respectively, which show the infidelity as a function of the ensemble size N (both axes in logarithmic scale). The filled circles indicate the experimentally obtained infidelity values, while vertical bars indicate the highest and lowest infidelity values obtained using the bootstrapping technique. The black solid line corresponds to the Gill-Massar limit for the infidelity given by $3/N$, and the red solid line is the best achievable infidelity for our setup considering the white noise error model. The shaded area shows the interquartile range generated by our error model.

Figure 2a shows the case where we estimate state $|\psi_1\rangle$, which has the largest fidelity with respect to the fiducial state $|0\rangle$. The infidelity exhibits values very close to both the Gill-Massar bound and those of the white noise model in the inspected interval of ensemble size. This shows that the

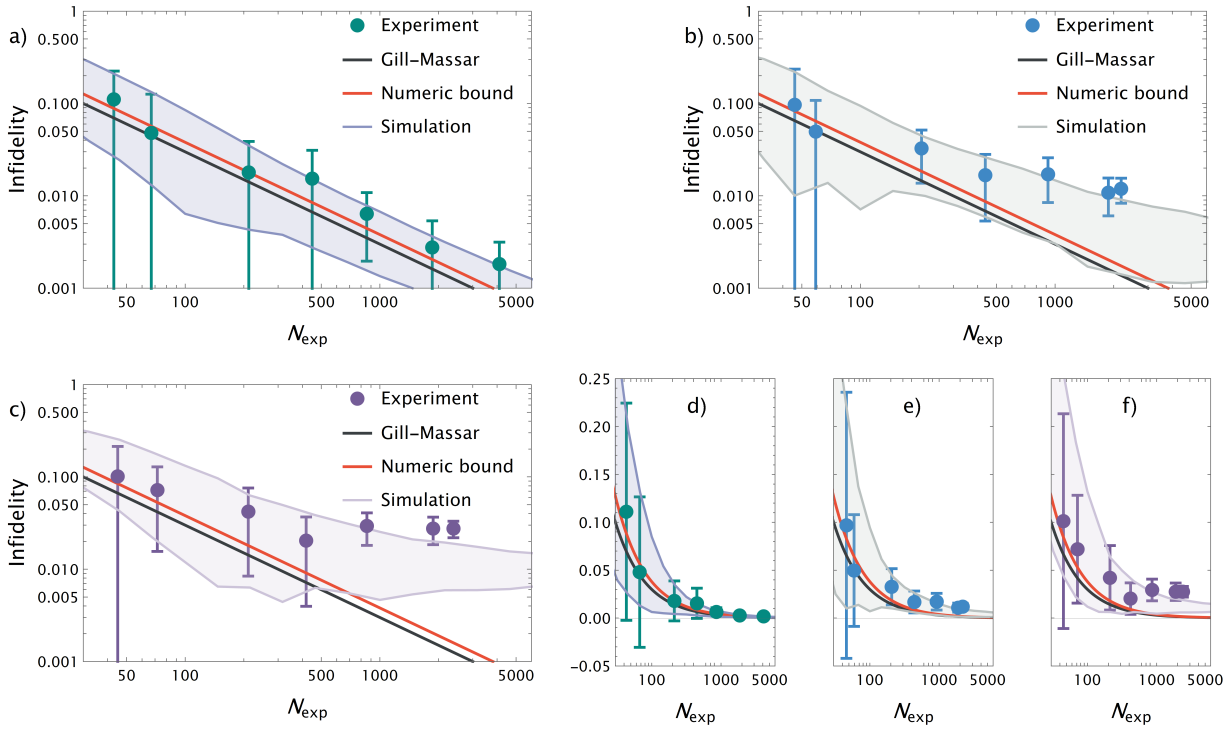


FIG. 2. Experimental results. Insets a), b), and c) are log-log plots for states $|\psi_1\rangle, |\psi_2\rangle$, and $|\psi_3\rangle$ respectively, showing the infidelity as a function of sample size. The filled circles indicate the experimentally obtained infidelity values, while error bars indicate the highest and lowest infidelity values obtained using the bootstrapping technique. The black solid line corresponds to the Gill-Massar limit for the infidelity given by $3/N$, and the red solid line is the best achievable infidelity for our setup considering a white noise error model. The shaded area shows the interquartile range generated by our error model. Insets d), e), and f) show the same data as a), b), and c), respectively, using a linear-log scale in order to show the typical reduction of the errors due to the increase in sample size.

implemented POVM is able to estimate the state $|\psi_1\rangle$ with high precision following a trend similar to the Gill-Massar limit. Specifically, a fit of the experimental results related with state $|\psi_1\rangle$ leads to a infidelity behaviour that decreases as a function of the ensemble size N according to $3.8/N$, which is quite close to the theoretical Gill-Massar limit given by $3/N$. Even the highest infidelity values for smaller ensembles do not differ significantly from this bound. Figures 2b and 2c show results for larger imposed systemic error. In these two cases and for small ensemble sizes, the experimental setup provides infidelity values still close to the Gill-Massar limit, and these even show a similar linear trend. As the size of the ensemble increases, the infidelity values are higher than in the case of state $|\psi_1\rangle$, and clearly differ from the lower Gill-Massar bound. Moreover, for the largest ensemble sizes, the infidelity values start to plateau. This is an experimental indication of the limits of the neighborhood that may be accurately considered in point tomography, as well as, an indication that systematic errors dominate over the effects of finite statistics for distant states. Lastly, note that the infidelities for the estimation of $|\psi_2\rangle$ and $|\psi_3\rangle$ follow the general behavior of the white noise model (grey shaded region). Figures 2d, 2e and 2f are used only to show the error bars out of the logarithmic scale for each case considered, where one can see the typical reduction of the errors due to the increase in sample size.

Conclusion– We have successfully demonstrated the viability of point tomography, a state estimation technique that has practical relevance for modern high-precision quantum information processing. Specifically, assuming that an arbitrary target state can be prepared with high-accuracy by the experimentalist, the method offers a estimation efficiency that saturates the Gill-Massar limit, while requiring the implementation of a simpler POVM whose number of outcomes can be greatly reduced from the traditional value of $\sim 4d-3$ to only $2d-1$, making POVM-based tomography for higher-dimensions ($d \geq 2$) much more viable. In our work, we use state-of-the-art multicore optical fiber technology to efficiently generate four-dimensional quantum states and to implement a high-fidelity Fisher-symmetric measurement in the form of a seven-outcome generalized measurement. Our experimental investigation clearly demonstrates the viability of point tomography under real world conditions, as we studied the method in different scenarios. In the high-precision regime, we observe a precision trend close to the Gill-Massar limit even though the POVM performed is not exactly a Fisher symmetric measurement. In lower-precision regimes, we show that the method can still be relevant. For small ensemble sizes where statistical errors dominate, the

average infidelities are still close to the Gill-Massar bound and show a linear decrease in the log-log plot as the ensemble size increases. The robustness of the method demonstrated in our experimental results, paves the way for a broader adoption of point tomography in all modern quantum platforms developed for high-precision quantum information.

This work was supported by Fondo Nacional de Desarrollo Científico y Tecnológico (FONDECYT) Grants No. 1200859, 1240746, and 123194, and by ANID – Millennium Science Initiative Program – ICN17_012. LP was supported by ANID-PFCHA/DOCTORADO-BECAS-CHILE/2019-772200275, the CSIC Interdisciplinary Thematic Platform (PTI+) on Quantum Technologies (PTI-QTEP+), the CAM/FEDER Project No. S2018/TCS-4342 (QUITEMAD-CM), and the Proyecto Sinérgico CAM 2020 Y2020/TCS-6545 (NanoQuCo-CM). KS was supported by the UCO 1866 project of the University of Concepción. MM was supported by ANID-PFCHA/DOCTORADO-NACIONAL/2019-21190958.

[1] S. Lloyd, Science **321**,1463 (2008).
[2] M. Szczykulska, T. Baumgratz, and A. Datta, Advances in Physics: X **1** 4 621-639 (2016).
[3] F. Albarelli, M. Barbieri, M.G. Genoni, and I. Gianani, Phys. Lett. A **384**, 126311 (2020).
[4] B. Lanyon, M. Barbieri, M. Almeida, T. Jennewein, T. C. Ralph, K. J. Resch, G. J. Pryde, J. L. O'Brien, A. Gilchrist, and A. G. White, Nat. Phys. **5**, 134-140 (2009).
[5] A. Bocharov, M. Roetteler, and K. M. Svore, Phys. Rev. A **96**, 012306 (2017).
[6] A. Babazadeh, M. Erhard, F. Wang, M. Malik, R. Nouroozi, M. Krenn, and A. Zeilinger, Phys. Rev. Lett. **119**, 180510 (2017).
[7] S. Muralidharan, C.-L. Zou, L. Li, J. Wen, and L. Jiang, New J. Phys. **19**, 013026 (2017).
[8] M. Taddei, J. Cariñe, D. Martínez, T. García, N. Guerrero, A. A. Abbott, M. Araújo, C. Branciard, E. S. Gómez, S. P. Walborn, L. Aolita, and G. Lima, PRX Quantum **2**, 010320 (2021).
[9] R. D. Gill and S. Massar, Phys. Rev. A **61**, 042312 (2000).
[10] C. Ferrie, Phys. Rev. Lett. **113**, 190404 (2014).
[11] D. H. Mahler, L. A. Rozema, A. Darabi, C. Ferrie, R. Blume-Kohout, and A. M. Steinberg, Phys. Rev. Lett. **111**, 183601 (2013).
[12] S. S. Straupe, JETP Letters **104**, 510–522 (2016).
[13] G. I. Struchalin, E. V. Kovlakov, S. S. Straupe, and S. P. Kulik, Phys. Rev. A **98**, 032330 (2018).
[14] F. Huszár and N. M. T. Houlsby, Phys. Rev. **A** 85, 052120 (2012).
[15] L. Pereira, L. Zambrano, J. Cortés-Vega, S. Niklitschek, and A. Delgado, Phys. Rev. A **98**, 012339 (2018).
[16] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, J. Math. Phys. **45**, 2171 (2004).
[17] D. M. Appleby, H. B. Dang, and C. A. Fuchs, Entropy **16**, 1484 (2014).
[18] J. Rehacek, B.-G. Englert, and D. Kaszlikowski, "Minimal qubit tomography," Phys. Rev. A **70**, 052321 (2004).
[19] W. M. Pimenta., et. al., ¨Minimal state tomography of spatial qubits using a spatial light modulator¨, Optics Express **24**, 24423 (2010).
[20] N. Bent, H. Qassim, A. A. Tahir, D. Sych, G. Leuchs, L. L. Sánchez-Soto, E. Karimi, and R. W. Boyd Phys. Rev. X **5**, 041006 (2015)
[21] R. Stricker, M. Meth, L. Postler, C. Edmunds, C. Ferrie, R. Blatt, P. Schindler, Th. Monz, R. Kueng, and M. Ringbauer PRX Quantum **3**, 040310 (2022).
[22] N. Li, C. Ferrie, J. A. Gross, A. Kalev, and C. M. Caves, Phys. Rev. Lett. **116**, 180402 (2016).
[23] H. Zhu and M. Hayashi, Phys. Rev. Lett. **120**, 030404 (2018).
[24] J. Cariñe, G. Cañas, P. Skrzypczyk, I. Šupić, N. Guerrero, T. Garcia, L. Pereira, M. A. S. Prosser, G. B. Xavier, A. Delgado, S. P. Walborn, D. Cavalcanti, and G. Lima, Optica **7**, 542 (2020).
[25] D. Martínez, E. S. Gómez, J. Cariñe, L. Pereira, A. Delgado, S. P. Walborn, A. Tavakoli, and G. Lima, Nat. Phys. **19**, 190 (2023).
[26] S. Pirandola et. al., ¨Advances in quantum cryptography¨, Adv. Opt. Photon. **12**, 1012-1236 (2020).
[27] A.K. Fedorov, N. Gisin, S.M. Beloussov, A.I. Lvovsky, ¨Quantum computing at the quantum advantage threshold: a down-to-business review¨, arXiv:2203.17181 [quant-ph] (2022).
[28] See the suplemmetal matterial.
[29] Richardson, D., Fini, J. and Nelson, L. Space-division multiplexing in optical fibres. Nature Photon **7**, 354–362 (2013).
[30] G. B. Xavier and G. Lima, "Quantum information processing with space-division multiplexing optical fibres," Commun. Phys. **3**, 9 (2020).
[31] Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt, L. K. Oxenløwe, npj Quantum Inf. **3**, 25 (2017).
[32] G. Cañas, N. Vera, J. Cariñe, P. Gonález, J. Cardenas, P. W. R. Connolly, A. Przysiezna, E. S. Gómez, M. Figueroa, G. Vallone, P. Villoresi, T. Ferreira da Silva, G. B. Xavier, and G. Lima, Phys. Rev. A **96**, 022317 (2017).
[33] S. Sarmiento, S. Etcheverry, J. Aldama, I. H. López, L. T. Vidarte, G. B. Xavier, D. A. Nolan, J. S. Stone, M. J. Li, D. Loeber, and V. Pruneri, New J. Phys. **24**, 063011 (2022).
[34] Zahidy, M., Ribezzo, D., De Lazzari, C. et al. Practical high-dimensional quantum key distribution protocol over deployed multicore fiber. Nat Commun**15**, 1651 (2024).
[35] Lee, H. J., Choi, S.-K. & Park, H. S. Experimental Demonstration of Four-Dimensional Photonic Spatial Entanglement between Multi-core Optical Fibres. *Sci. Rep.* **7**, 4302 (2017).
[36] Lee, H. J. & Park, H. S. Generation and measurement of arbitrary four-dimensional spatial entanglement between photons in multicore fibers. *Photon. Res.* **7**, 19 (2019).
[37] E. A. Ortega, K. Dovzhik, J. Fuenzalida, S. Wengerowsky, J. C. Alvarado-Zacarias, R. F. Shiozaki, R. Amezcua-Correa, M. Bohmann, and R. Ursin, PRX Quantum **2**, 040356 (2021).
[38] E. S. Gómez, S. Gómez, I. Machuca, A. Cabello, S. Pádua, S. P. Walborn, and G. Lima, Phys. Rev. Applied **15**, 034024 (2021).
[39] J. Shang, Z. Zhang, and H. K. Ng, Phys. Rev. A **95**, 062336 (2017).

C Demonstration of the Fidelity Beta Distribution Fit

In this section we will show that the state fidelity follows a beta distribution. If the state Alice prepares is $|i\rangle_B$ for $i = \{0,1,2,3\}$ and $B = \{Z,X\}$, and detector j shows C_j counts, the fidelity of the state is given by

$$F_i = \frac{C_i}{\sum_{j=0}^{3} C_j}. \tag{C.1}$$

However, instead of expressing it in terms of detector counts, we could write it in terms of the average photon number μ_i arriving at each detector (given that $\mu_i \propto C_i$ given enough detections to smooth out statistical fluctuations). We then have

$$F_i = \frac{\mu_i}{\sum_{j=0}^{3} \mu_j} \tag{C.2}$$

$$= \frac{\mu_i}{\mu_i + \sum_{j=0,\ j\neq i}^{3} \mu_j} \tag{C.3}$$

$$= \frac{\mu_i}{\mu_i + \mu'}, \tag{C.4}$$

where we took μ_i out of the sum and expressed the rest of it as μ'. By writing F_i in this way, we can take advantage of a concept known as the conjugate prior. It arises from a question in Bayesian statistics: suppose X is modeled by a probability distribution $p(y|x)$ parameterized by y. This assumes y is known and x is a possible outcome when measuring X. But suppose we invert the problem: what is the distribution $p(y|x)$ that models the result obtained for Y given a known x? The distribution $p(y|x)$ is known as the conjugate prior for $p(x|y)$.

In our case, the counts C follow a Poisson distribution,

$$C \sim \text{Pois}(\mu) \Rightarrow p(k|\mu) = \frac{\mu^k e^{\mu}}{k!}, \tag{C.5}$$

and the conjugate prior for the Poisson distribution is known to be the gamma distribution [21]

$$\mu \sim \text{Gamma}(\alpha, \beta) \Rightarrow p(\mu|\alpha, \beta) = \frac{\beta^{\alpha} \mu^{\alpha-1} e^{-\beta\mu}}{\Gamma(\alpha)}. \tag{C.6}$$

The mean of this distribution is known to be α/β, so for a sample of n measured photon counts k_m, α can be interpreted as the sum of photon counts $\sum_{m=1}^{n} k_m$ and β as the number of pulses n sent [77]. Therefore each detector will have an associated α_i, while $\beta_i = \beta$ is the same for all detectors (since they all receive the same number of pulses). Then

$$\mu_j \sim \text{Gamma}(\alpha_j, \beta). \tag{C.7}$$

Because the sum of gamma-distributed variables with the same β is gamma-distributed with the sum of their α_i [77], we can write

$$\mu' = \sum_{j=0,\ j\neq i}^{3} \mu_j \sim \text{Gamma}\left(\sum_{j=0,\ j\neq i}^{3} \alpha_j, \beta \right), \tag{C.8}$$

while for detector i we have $\mu_i \sim \text{Gamma}(\alpha_i, \beta)$. Gamma distributions have the property that, if two variables X and Y are gamma distributed,

$$\begin{aligned} X &\sim \text{Gamma}(\alpha, \beta), \\ Y &\sim \text{Gamma}(\alpha', \beta), \end{aligned} \tag{C.9}$$

$$\Rightarrow \frac{X}{X+Y} \sim \text{Beta}(\alpha, \alpha'), \tag{C.10}$$

where $\text{Beta}(\alpha, \alpha')$ is the beta distribution [77]. Given Eqs. C.4, C.7 and C.8, we find

$$F_i \sim \text{Beta}\left(\alpha_i, \sum_{j=0,\ j\neq i}^{3} \alpha_j\right). \tag{C.11}$$

Therefore, the fidelity follows a beta distribution.