université
PARIS-SACLAY

NNT : 2019SACL0021

INSTITUT
d'OPTIQUE
GRADUATE SCHOOL
ParisTech

# Design and implementation of high-performance devices for continuous-variable quantum key distribution

Thèse de doctorat de l'Université Paris-Saclay
préparée à l'Institut d'Optique Graduate School

École doctorale n°572 Ondes et Matière (EDOM)
Spécialité de doctorat : Physique

Thèse présentée et soutenue à Palaiseau, le 20 décembre 2019, par

**LUIS TRIGO VIDARTE**

Composition du Jury :

| | |
|---|---|
| Delphine MORRIS-MORINI<br>Prof., Centre de Nanosciences et de Nanotechnologies (C2N) | Président |
| Virginia D'AURIA<br>MCF, Université Nice Sophia Antipolis | Rapporteur |
| Valerio PRUNERI<br>Prof., Institut de Ciències Fotòniques (ICFO) | Rapporteur |
| Romain ALLÉAUME<br>MCF, Télécom Paris | Examinateur |
| Thierry DEBUISSCHERT<br>Ing. de recherche, Thales Research and Technology | Examinateur |
| Philippe GRANGIER<br>DRCE, Institut d'Optique Graduate School; CNRS | Directeur de thèse |
| Eleni DIAMANTI<br>DR, Sorbonne Université; CNRS | Co-directeur de thèse |

Thèse de doctorat

**Manuscript**

# Conception et réalisation de dispositifs de distribution de clé quantique à variables continues à haute performance

**Design and implementation of high-performance devices for continuous-variable quantum key distribution**

Luis TRIGO VIDARTE

Laboratoire Charles Fabry
(Institut d'Optique Graduate School)
-
Laboratoire d'Informatique de Paris 6
(Sorbonne Université)

# Acknowledgements

These initial words intend to express my gratitude to the people that have, in one way or another, contributed to the completion of this manuscript and my doctoral studies. The list is long, but I think all the names mentioned deserve to be here.

I would like to start by thanking all the members of the Jury for their dedication, reviewing effort and useful comments. I want to dedicate particular attention to my thesis directors, Eleni and Philippe, a team that is bigger than the sum of the parts and a gracious combination of research excellence and humanity.

I had the opportunity to work in different projects, where I was lucky to collaborate with many different people, in several institutions. I find it difficult to follow a particular acknowledge sequence so I will begin by thanking my fellow PhD companions in the CV-QKD adventure, with whom I had the chance to spend more time in the lab. My first lab partner was Mauro Persechino and I must say that it is a pleasure to interact with him, inside and outside the lab. Later I had the opportunity to work with François Roumestan, a very insightful engineer and engaging person. Víctor Román Rodríguez of course cannot be unnoticed, thank you for the work and the Spanish laughs. Almost at the end of my PhD Damien Fruleux and Adam Raptakis started theirs, but I foresee a successful PhD path for both of them. At long distance, but with fruitful results was the collaboration with Nathan Abrams and David Álvarez Outerelo, which gave me the opportunity to learn many things about integrated optics.

Not PhD students, but already CV-QKD experts by now are Adrien Cavaillès and Matteo Schiavon, as well as Amine Rhouni, our electronics expert that has a lot of patience with me. Special thoughts to the interns I had the chance to interact with, Alexandre Maïnos and Meriem Kemache. All my gratefulness for them.

Regarding my brief incursion in the world of quantum money I had the pleasure to work with Mathieu Bozzio, Adeline Orieux and Iordanis Kerenidis. I was introduced to quantum communication complexity by Niraj Kumar and Federico Centrone, and to more fundamental quantum optics by Simon Neves. Shouvik Ghorai gave the necessary support in the theoretical part of CV-QKD. Thanks a lot!

Coming back to integrated photonics my first collaboration was with C2N in the ANR QRYPTOS project, working with Paul Crozat, Delphine Marris-Morini, Mauro Persechino, Laurent Vivien and André Villing. Under the CRYSP project I could visit Keren Bergman's Lightwave Research Laboratory in Columbia University, New York.

There I had the opportunity to work with two fantastic PhD students, Nathan Abrams and Christine Chen.

At Nokia Bell Labs in Nozay, I could work with Amirhossein "Amir" Ghazisaeidi, Jérémie Renaudier, François Roumestan and Christian Simonneau. I would like to thank them and the rest of the team for hosting me during the time I spent there.

The free-space section could not have been possible without the persistence of Daniele Dequal at ASI and the help of Víctor Román Rodríguez and Anthony Leverrier, as well as the support of Giuseppe Vallone and Paolo Villoresi.

It was special to collaborate with people from University of Vigo, my home university, David Álvarez Outerelo and Francisco Javier Díaz Otero in the design of chips dedicated to quantum information tasks (with the help of Valentina Moskalenko). I would also like to thank Carlos Mosquera Nartallo and Marcos Curty, who introduced me to digital communications and quantum key distribution respectively, for the discussions related to my work.

A considerable time effort has been dedicated to the development of the electronics and cannot be neglected. In that sense I am deeply grateful to André Villing and Frédéric Moron at IOGS, Gérard Mouret at Télécom Paris, and Amine Rhouni at LIP6. Particular thanks to the IOGS mechanical workshop for providing us with reliable mechanical components.

I could dedicate part of my time to teach at IOGS in which was a very rewarding experience. I would like to thank all the students and the people who helped me during this task: Denis Boiron, Julien Villemejane, Fabienne Bernard, Julien Moreau, Franck Delmotte, Pierre Dussarrat, Remy Juvenal, Thibault Harlé, Anaïs Molineri, Thierry Avignon, Cedric Lejeune, Ilan Schlesinger, Matthieu Boffety, François Goudail, Vincent Lienhard, Clémence Briosne-Fréjaville, Julien Desprès and Yvan Sortais.

I was also involved in the organization of different events related to research, maybe the most intense was the participation in the local organizing committee of ICIQP 2018. I would like to thank the rest of the team: Eleni Diamanti, Pascale Senellart-Mandon, Sara Ducci, Maria Amanti, Carlos Antón Solanas and Florent Baboux, as well as the other people who helped in the event. Sara was also the organizer of the master that introduced me to research in France, so I am specially thankful for that and I use the occasion to remember my cohort colleagues and teachers.

I consider that the environment is a very important factor for successful research and I had nothing but good experiences in the different groups I participated.

Thank you *optique quantique* group at LCF (IOGS): Daniel Barredo, Rajiv Boddeda, Guillaume Boucher, Martin Bouillard, Ludovic Brossard, Antoine Browaeys, Senka Ćuk, Sylvain De Léséleuc, Júlia Ferrer Ortas, Igor Ferrier-Barbut, Yara Hodroj, Thierry

Lahaye, Florence Nogrette, Benjamin Pointard, Pascal Scholl, Kai-Niklas Schymik, Rosa Tualle-Brouri and Imam Usmani. Thank you Philippe Delaye for organizing the group seminars.

Thanks to everyone in the exponentially growing LIP6 QI team (and collaborators): Hossein Aghababa, Francesco Arzani, Robert Booth, Cyril Castagnet, Ulysse Chabaud, Léo Colisson, Ellen Derbyshire, Tom Douce, Pierre Emmanuel Emeriau, Frédéric Grosshans, Elham Kashefi, Dominik Leichtle, Yao Ma, Shane Mansfield, Atul Mantri, Damian Markham, Natansh Mathur, Clément Meignant, Rawad Mezher, Luka Music, Andrea Olivo, Harold Ollivier, Rhea Parekh, Alisa Russanova, Nathan Shettell, Shraddha Singh, Anu Unnikrishnan and Raja Yehia.

A little bit more distant in time, but still with a good impression in my memory, remains my period at Télécom ParisTech, where I could meet (and work with) Romain Alléaume, Martin Cordier, Leonardo Disilvestro, Masoud Ghalaii, Marc Kaplan, Niraj Kumar, Rupesh Kumar, Adrien Marie, Bill Plick, Hao Qin, Adel Sohbi, Julien Trapateau and Isabelle Zaquine. My attention also for non-quantum people: Danilo, Karel, Mario, Kasia, Jon, Andrea, Dalia, Leonardo, Michele, Mircea, Maura and Serena.

I would also like to thank the work done by PCQC that facilitated the interaction with researchers like André Chailloux, Kaushik Chakraborty, Ruben Cohen, Alex Grillo, Antoine Grospellier and Vivien Londe.

On the administrative side I would like to thank the teams of EDOM, Télécom ParisTech and LIP6, but very specially to all the people in human resources at IOGS, as well as the people in reception and reprography. They have been very efficient, professional and helpful at all times. The same can be said for the direction of LCF: thank you Patrick George and Maïké Seychelles.

Turning to less professional recognitions I would like to warmly thank Adel, Anambar, Danilo, Kate, Kaushik, Mylène, Niraj and Venkat for all the moments spent together during the last few years. I cannot forget the people who made the effort to visit me and are always welcome wherever I go: Alessandra, Alicia, Ana P, Ana SA, Anna, Claire, David, Eliana, Emily, Fran, Giorgio, Julia, Jurgita, Ola, Marine, Miguel, Monika, Sumit, Tamara, Typhaine, Thomas, Thuy, Viti, Yaiza, and of course Mery and Lucía! Many thanks also to my hosts in Paris: Evelyn, Pascale, Christina, Emmanuel and especially Anne-Solange.

Por último, pero non menos importante, gustaríame agradecer á miña familia todo o seu apoio e cariño ó longo de todos estes anos. Fíxome moita ilusión poder compartir esta experiencia con vós! Gracias!

*Luis Trigo Vidarte*

# Résumé en français

La distribution quantique de clé (QKD) est une des premières technologies quantiques qui ait atteint un stade commercial, en proposant une solution au problème de la distribution d'une clé cryptographique entre deux entités, et en garantissant une sécurité à long terme. Elle est maintenant proche de la maturité technologique, et plusieurs méthodes sont disponibles en pratique. Cette thèse étudie la distribution quantique de clé à variables continues (CV-QKD), qui a plusieurs éléments communs avec les communications optiques cohérentes classiques, et qui pourrait permettre à beaucoup d'utilisateurs d'accéder à la QKD.

L'utilisation de techniques de traitement numérique (Digital Signal Processor ou DSP), typiques en communications classiques, a été seulement partiellement exploitée dans les implémentations CV-QKD précédentes. Dans ce travail nous mettons en œuvre expérimentalement des techniques usuelles dans les communications classiques, comme la mise en forme d'impulsions, le filtrage adaptatif et la récupération de mode. Notre objectif est d'augmenter ainsi le taux de clé secrète, et d'optimiser l'utilisation de la bande passante disponible. Pour montrer l'application de ces techniques nous avons implémenté en parallèle deux expériences avec deux perspectives différentes : de bas en haut et de haut en bas. Pour une première implémentation nous avons conçu une plateforme flexible nous permettant de développer nos propres algorithmes en partant de zéro, le taux de répétition du système étant le principal facteur limitant en conditions commerciales. Une implémentation alternative a été mis en place pour tester des systèmes plus performants capables de fonctionner à un taux de symbole comparable aux systèmes de communication classiques. Pour ce deuxième alternative nous sommes parties d'algorithmes disponibles et nous avons étudié la viabilité de la CV-QKD dans ce type de systèmes.

La possibilité d'intégrer des composants dans un circuit photonique (PIC) est un autre avantage de CV-QKD. Nous avons testé un PIC en silicium intégrant un coupleur hybride 180$^{o}$ et deux photodiodes en germanium. Une implémentation expérimental à été mis en place pour tester le comportement de plusieurs unités de ce dispositif en travaillant avec un oscillateur local transmis en utilisant des impulsions de lumière. Avec ce système nous avons fait tourner le protocole GG02 pour montrer que les paramètres mesurés sont compatibles avec la génération de clé secrète dans ce conditions. Une notable amélioration des résultats est envisageable avec la correction de certains éléments dans le processus de fabrication et *packaging*.

Un des facteurs les plus limitants de QKD est la chute des performances dans les canaux ayant des pertes très élevées, typiquement des fibres optiques dont la longueur dépasse la centaine de kilomètres. Mais la distance utile peut être étendue notablement en utilisant des liens en espace libre, en particulier avec des satellites, où les pertes à une certaine distance peuvent être inférieures à celles des fibres. Nous considérons un modèle pour le canal descendant et prédisons les taux de clé secrète attendus à différentes altitudes pour CV-QKD. Ces résultats aboutissent à une technologie potentiellement utilisable pour les communications par satellite, en étendant la portée jusqu'à des distances intercontinentales.

# Preface

This document covers most of the work developed during my PhD (2016-2019). It is a period when commercial implementations of Quantum Key Distribution (QKD) are a reality, but they are still pursuing their technological maturity. This context creates a very interesting atmosphere where many research groups introduce their proposals to solve particular problems. In our case we focus on Continuous Variables QKD (CV-QKD) and propose two independent experimental solutions with the following objectives: (a) increasing the secret key rate by taking advantage of the techniques used in classical coherent communications; (b) facilitating the expansion of QKD by integrating the components in a photonic chip, reducing cost, size and consumption. Additionally we provide a theoretical analysis about the feasibility of CV-QKD over satellite links.

The content is divided into 10 chapters organized in different sections:

- **Section 1. Introduction** provides the context to understand CV-QKD.
  - **Chapter 1.** The security concepts and the contributions of QKD are discussed, as well as the current state of QKD technology.
  - **Chapter 2.** The fundamental aspects of CV-QKD are introduced. Basic security proofs using the entanglement based version of the protocol are explained, but the main focus are the "prepare-and-measure" implementations. Special emphasis is given to the study of the coherent detector accommodating the concepts typically used in Physics and Engineering.
- **Section 2. Bandwidth efficient CV-QKD.** We introduce relevant concepts of signal processing in the implementation of CV-QKD experiments. These ideas have been used in the classical optical coherent communication industry for a couple of decades but they are relatively new in the context of CV-QKD.
  - **Chapter 3.** The main tools used in classical coherent communications are explained. We focus on the tasks related to the digital signal processing (DSP): sampling, pulse shaping, adaptive filtering and frequency and phase recovery.
  - **Chapter 4.** The concepts in the previous chapter are adapted to CV-QKD and an experimental set up operating in real time at rates in the order of Msymbols/s is described.
  - **Chapter 5.** In this case a classical coherent communication system operating at rates in the order of Gsymbols/s is tested in CV-QKD conditions. The

parameter estimation is adapted to this kind of system and the preliminary results are presented.

- **Section 3. On-chip CV-QKD.** The possibility of integrating multiple functionalities inside a single photonic chip is a very promising alternative for CV-QKD. We discuss the integration of a coherent detector in a silicon chip.
  - **Chapter 6** gives an overview of the basic concepts required to understand the discussion in the next chapter.
  - **Chapter 7**. We describe the design, packaging and testing of a 180° hybrid with a balanced detector integrated in a silicon photonics chip. The results of the tests using the unit as part of Bob's receiver in a CV-QKD set up are shown.
- **Section 4. Free-space CV-QKD.** Fibre is not the only medium that can be used for CV-QKD communications. Free-space can be an attractive alternative in some cases, especially for intercontinental distances if satellites can be used. The work in this part is only theoretical, but proof-of-principle experiments are planned for the future.
  - **Chapter 8** is used as an introductory chapter for general free-space CV-QKD. We will see that the communication will suffer from fading, but it can be parametrized assuming certain impairments (effective parameters). We will describe a methodology consisting on a subdivision of the channel as a function of the transmittance (binning) to obtain positive secret key rates.
  - **Chapter 9** The previous technique is applied to the particular case of downlink communications (satellite-to-Earth). We show that it is possible to obtain positive secret key rates using low-Earth-orbit (LEO) satellites, and potentially for higher orbits using wider optics.
- **Section 5**. We wrap up the main new ideas and draw the conclusions and future steps in chapter 10.

The results would not have been possible without the involvement of many people. For the sake of facilitating a context maintaining clarity only the institutions will be cited here (more details in the acknowledgements). The work on bandwidth efficient CV-QKD was performed in close collaboration with Nokia Bell Labs (Nozay), and the real time proof-of-principle experiment developed at Sorbonne Université. The tests on the chips were carried out at IOGS and C2N*. The feasibility study on satellite CV-QKD was completed in collaboration with ASI (Italian Space Agency), INRIA and Università di Padova.

* Relevant work in this topic not covered by this document was also carried out at Columbia University and Sorbonne Université.

# Detailed Contents

**Acknowledgements** **iii**

**Résumé en français** **vii**

**Preface** **ix**

**Detailed Contents** **xi**

INTRODUCTION **1**

**1 Introduction to cryptography** **3**
1.1 Security concepts . . . 3
1.1.1 Hiding the information . . . 4
1.1.2 Information-theoretical security . . . 5
1.1.3 Distribution of the key . . . 6
1.2 Quantum key distribution . . . 7
1.2.1 BB84 . . . 8
1.2.2 Common principles of QKD protocols . . . 9
1.2.3 Relevant concepts . . . 10
1.3 QKD today . . . 12
1.3.1 Quantum technologies ecosystem . . . 12
1.3.2 Criticism . . . 13

**2 Introduction to CV-QKD** **15**
2.1 Basic concepts . . . 15
2.1.1 Security conditions . . . 15
2.1.2 QKD using continuous-variables . . . 15
2.1.3 Conditions on the security proofs . . . 16
2.1.4 Considerations . . . 17
2.2 Coherent detection . . . 17
2.2.1 Coherent detection: regimes of operation . . . 19
2.2.2 Coherent detection in CV-QKD . . . 20
2.2.3 Coherent detection: noise consequences . . . 22
2.3 CV-QKD: entanglement version . . . 23
2.4 Some relevant security proofs . . . 25
2.4.1 Security proof against collective attacks for Gaussian modulation 25
2.4.2 Security proof against collective attacks under linear channel for QPSK modulation . . . 26
2.5 CV-QKD: Prepare and measure . . . 27
2.5.1 A CV-QKD protocol: GG02 . . . 27
2.6 Introduction of imperfections . . . 28
2.6.1 Noisy and inefficient detector . . . 29
2.6.2 Finite size effects on the parameter estimation . . . 31
2.7 Motivations of this thesis . . . 33

**BANDWIDTH EFFICIENT CV-QKD** **35**

**3 Coherent communications** **37**
3.1 Introduction . . . 37
3.2 Principles of coherent communications . . . 38
3.2.1 Channel coding . . . 38
3.2.2 Modulation formats . . . 39
3.2.3 Typical operation mode . . . 43
3.3 General scheme . . . 44
3.4 Channel model . . . 45
3.4.1 Fluctuating transmittance . . . 48
3.5 Digital signal processing (DSP) . . . 48
3.5.1 Sampling and time . . . 48
3.5.2 Pulse shaping: raised cosine . . . 49
3.5.3 Adaptive filter . . . 51
3.5.4 Frequency and phase recovery . . . 53
3.5.5 Synchronization . . . 54
3.5.6 DSP scheme . . . 54
3.6 Coherent communications and CV-QKD . . . 55

**4 Continuous Wave CV-QKD** **57**
4.1 Motivation . . . 57
4.2 CV-QKD using pulse shaping . . . 58
4.3 Is it secure? . . . 59
4.4 Proposed proof-of-principle experiment . . . 61
4.4.1 Hardware description . . . 61
4.4.2 DSP description . . . 62
4.4.3 Preliminary results . . . 65
4.5 Comments and possible improvements . . . 66

**5 High rate CV-QKD** **67**
5.1 CV-QKD using high rate optical coherent communications systems . . 67
5.1.1 Hardware set up . . . 68
5.1.2 DSP . . . 69
5.2 Parameter estimation . . . 71
5.2.1 Mutual information . . . 71
5.2.2 Estimation of detection efficiency: $\eta$ . . . 72
5.2.3 Estimation electronic and shot noise: $N_0$, $\sigma_{\mathrm{el}}^2$ . . . 73
5.2.4 Estimation of correlation: $\rho$ . . . 74
5.2.5 Estimation of $V_A$ . . . 74
5.2.6 Estimation of $V_B$ and $\xi_{\mathrm{Bob}}$ . . . 76
5.2.7 Estimation of $T$ and $\xi$ . . . 76
5.3 Results . . . 76
5.3.1 QPSK modulation . . . 77
5.3.2 PCS-QAM modulation . . . 77
5.3.3 Expected key rates . . . 77
5.4 Possible improvements . . . 78

On-chip CV-QKD 81

6 Integration of optical devices 83
6.1 Integrated circuits . . . . . . . . . . 83
6.2 PICs in CV-QKD . . . . . . . . . . 84
6.2.1 Additional considerations . . . . . . . . . . 85
6.3 Development of a PIC . . . . . . . . . . 86

7 Experimental evaluation of on-chip coherent detector 87
7.1 Description of the device under test . . . . . . . . . . 87
7.1.1 Development sequence . . . . . . . . . . 87
7.1.2 Test types . . . . . . . . . . 89
7.1.3 Alice . . . . . . . . . . 90
7.2 Description of the set up . . . . . . . . . . 92
7.2.1 Frame structure . . . . . . . . . . 96
7.2.2 Feedback control . . . . . . . . . . 96
7.3 Results . . . . . . . . . . 100
7.3.1 Detection efficiency . . . . . . . . . . 100
7.3.2 Electronic noise . . . . . . . . . . 101
7.3.3 Shot noise and clearance . . . . . . . . . . 102
7.3.4 Estimating $V_A$ . . . . . . . . . . 104
7.3.5 Protocol performance . . . . . . . . . . 105
7.3.6 Achievable secret key rates . . . . . . . . . . 110
7.4 Conclusions . . . . . . . . . . 112

Free-space CV-QKD. Satellite feasibility study 113

8 CV-QKD in free-space 115
8.1 Comparison fibre and free space . . . . . . . . . . 115
8.1.1 Losses . . . . . . . . . . 115
8.1.2 Channel fluctuations . . . . . . . . . . 117
8.2 Secret key over a fading channel . . . . . . . . . . 117
8.2.1 Holevo bound . . . . . . . . . . 118
8.2.2 Mutual information . . . . . . . . . . 119
8.2.3 Secret key rate . . . . . . . . . . 121
8.3 Secret key subdividing the fading channel . . . . . . . . . . 122
8.3.1 Classification of symbols in bins . . . . . . . . . . 122
8.3.2 Methodology . . . . . . . . . . 124
8.3.3 Example . . . . . . . . . . 125
8.4 Experimental proposal . . . . . . . . . . 130
8.4.1 Suitable schemes . . . . . . . . . . 130
8.4.2 Emulation of a free-space link . . . . . . . . . . 130
8.4.3 Proposal for a proof-of-principle free-space CV-QKD experiment 131
8.5 Conclusion . . . . . . . . . . 132

9 Feasibility study of satellite CV-QKD 133
9.1 Distinctive satellite communication properties . . . . . . . . . . 133
9.1.1 Scenario of analysis . . . . . . . . . . 135

9.2 Estimating secret key rate of a satellite passage . . . . . . . . . . . . . . 135
9.2.1 Satellite trajectories . . . . . . . . . . . . . . . . . . . . . . . . . . . . 136
9.2.2 PDTC of satellite passage . . . . . . . . . . . . . . . . . . . . . . . . 138
9.2.3 Expected secret key rates . . . . . . . . . . . . . . . . . . . . . . . . 140
9.3 Other scenarios . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 143
9.3.1 Uplink . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 143
9.3.2 Inter-satellite . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 144
9.3.3 Geostationary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 144
9.4 Conclusions . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 144
9.4.1 Extensions to the present analysis . . . . . . . . . . . . . . . . . . . 145

## CONCLUSIONS 147

**10 Conclusions 149**
10.1 Bandwidth efficient CV-QKD . . . . . . . . . . . . . . . . . . . . . . . . . 150
10.2 On-chip CV-QKD . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 151
10.3 Free-space CV-QKD . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 151

## APPENDIX 153

**A Phase space representation 155**
A.1 Phase space representation . . . . . . . . . . . . . . . . . . . . . . . . . . 155
A.1.1 Canonical quantization . . . . . . . . . . . . . . . . . . . . . . . . . . 155
A.1.2 Extension to multiple modes . . . . . . . . . . . . . . . . . . . . . . 156
A.1.3 Recapitulation . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 158
A.2 Interesting states in phase space . . . . . . . . . . . . . . . . . . . . . . . 158
A.2.1 Quadrature eigenstates . . . . . . . . . . . . . . . . . . . . . . . . . . 158
A.2.2 Coherent states . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 158

**B Gaussian states 161**
B.1 Properties of Gaussian states . . . . . . . . . . . . . . . . . . . . . . . . . 161
B.1.1 Symplectic spectrum and invariants . . . . . . . . . . . . . . . . . . 162
B.2 Some useful Gaussian states . . . . . . . . . . . . . . . . . . . . . . . . . . 165
B.2.1 One-mode Gaussian states . . . . . . . . . . . . . . . . . . . . . . . . 165
B.2.2 Two-mode Gaussian states . . . . . . . . . . . . . . . . . . . . . . . . 166
B.3 Gaussian operations . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 166
B.3.1 Symplectic transformations . . . . . . . . . . . . . . . . . . . . . . . 167
B.3.2 Completely positive maps . . . . . . . . . . . . . . . . . . . . . . . . 168
B.3.3 Partial measurements . . . . . . . . . . . . . . . . . . . . . . . . . . . 168
B.4 Entropy of continuous variables . . . . . . . . . . . . . . . . . . . . . . . . 170
B.4.1 Entropy of Gaussian states . . . . . . . . . . . . . . . . . . . . . . . . 170
B.4.2 Extremality of Gaussian states . . . . . . . . . . . . . . . . . . . . . 171
B.5 Recapitulation . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 171

**C Mutual information 173**
C.1 Mutual information and Holevo bound . . . . . . . . . . . . . . . . . . . . 173
C.1.1 Channel capacity . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 174
C.1.2 Modulation and reconciliation efficiency . . . . . . . . . . . . . . . . 175
C.1.3 Mutual information between Alice and Bob . . . . . . . . . . . . . . 176

C.1.4 Mutual information between Eve and Bob . . . . . . . . . . . . 177
C.2 Holevo bound . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 178
C.2.1 Holevo bound in CV-QKD . . . . . . . . . . . . . . . . . . . . . . . . 178

**D Probability Distribution of Transmittance (PDT) 181**
D.1 Probability Distribution of Transmission Efficiency (PDTE) . . . . . . . 181
D.2 Probability Distribution of Transmission Coefficient (PDTC) . . . . . . 182
D.3 Sources of uncertainty . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 183
D.3.1 Beam wandering . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 183
D.3.2 Atmospheric turbulence . . . . . . . . . . . . . . . . . . . . . . . . 183
D.3.3 Other sources . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 183

**E Doppler effect in satellites 185**
E.1 Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 185
E.1.1 Frequency mixing . . . . . . . . . . . . . . . . . . . . . . . . . . . . 185
E.2 Doppler effect . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 186
E.2.1 Fast evaluation of order of magnitude . . . . . . . . . . . . . . . . 186
E.2.2 Doppler shift cancellation . . . . . . . . . . . . . . . . . . . . . . . . 187

**Bibliography 189**

**Glossary 197**

# Figures

2.1 Optical hybrid scheme. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 18
2.2 Optical mixing of signal and LO as a function of the frequency offset. . . . 21
2.3 EPR scheme for the measurement of one quadrature at Bob's. . . . . . . . . 24
2.4 EPR scheme for the simultaneous measurement of two quadratures at Bob's. 24
2.5 Entanglement version of the protocol including detector imperfections. . . 30

3.1 High order modulation constellation before and after an AWGN channel. . 40
3.2 Devices for phase, amplitude and IQ modulation and their action in phase space. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 41
3.3 Coherent communication transmission and reception schemes. . . . . . . . 42
3.4 Distribution of symbols in phase space for a PCS-QAM modulation. . . . . 43
3.5 Achievable information rates (AIR) as a function of SNR. . . . . . . . . . . 43
3.6 General scheme for a double polarization coherent communication system. 45
3.7 Bandwidth corresponding to the I and Q components of the signal. . . . . 49
3.8 Raised cosine and root raised cosine time and frequency representations. . 50
3.9 QPSK sequence after pulse shaping with RRC filter (ROF=0.1). . . . . . . . 52
3.10 Butterfly structure of the adaptive filter. . . . . . . . . . . . . . . . . . . . . 53
3.11 Scheme of the DSP at the transmitter. . . . . . . . . . . . . . . . . . . . . . . 55
3.12 Scheme of the DSP at the receiver. . . . . . . . . . . . . . . . . . . . . . . . . 55

4.1 Power spectral densities at Alice's output and Bob's input. . . . . . . . . . 66

5.1 Scheme of the coherent communications set up. . . . . . . . . . . . . . . . . 68
5.2 Integrated coherent receiver (ICR) scheme. . . . . . . . . . . . . . . . . . . . 70
5.3 Photo of the coherent communications set up. . . . . . . . . . . . . . . . . . 70
5.4 ICR photodiode efficiency. . . . . . . . . . . . . . . . . . . . . . . . . . . . . 73
5.5 Measured power spectrum densities of ICR electronic and shot noise. . . . 74
5.6 ICR integrated electronic and shot noise between 1-5 GHz. . . . . . . . . . 75
5.7 Expected SKR as a function of $V_A$ at 100 m for different values of excess noise. 78
5.8 Expected SKR as a function of $V_A$ at 20 km for different values of excess noise. 78

6.1 Typical life cycle of a chip. . . . . . . . . . . . . . . . . . . . . . . . . . . . . 86

7.1 On-chip 180° hybrid detector layout and microscopic photo. . . . . . . . . . 88
7.2 Mezzanine PCB layout and final result. . . . . . . . . . . . . . . . . . . . . . 89
7.3 Mother board with inserted mezzanine board. . . . . . . . . . . . . . . . . . 89
7.4 Layout for on-chip Alice with feedback system. . . . . . . . . . . . . . . . . 92
7.5 Scheme of the on-chip coherent detector set up. . . . . . . . . . . . . . . . . 92
7.6 Frame structure: relation of frames, blocks and symbols. . . . . . . . . . . . 97
7.7 Calibration of amplitude modulator in one block. . . . . . . . . . . . . . . . 98
7.8 Calibration of phase modulator in one block. . . . . . . . . . . . . . . . . . 99
7.9 Evolution of the electro-optical modulator parameters during one frame. . 99
7.10 Efficiency as a function of the wavelength and fibre array scheme. . . . . . 100
7.11 Evolution of the electronic noise during 10 seconds. . . . . . . . . . . . . . 102
7.12 Evolution of the shot noise plus electronic noise during 10 seconds. . . . . 103
7.13 Shot noise as a function of the LO power and clearance. . . . . . . . . . . 104

7.14 Reference symbols after detection. . . . . . . . . . . . . . . . . . . . . . . . . . 106
7.15 Estimated evolution of phase in on-chip coherent detector. . . . . . . . . . . 107
7.16 Estimated evolution of correlation in on-chip coherent detector. . . . . . . . 108
7.17 Estimated evolution of channel transmittance in on-chip coherent detector. 108
7.18 Estimated evolution of variances in on-chip coherent detector. . . . . . . . 109
7.19 Evolution of estimated variances in on-chip coherent detector using logarithmic scale and SNU. . . . . . . . . . . . . . . . . . . . . . . . . . . 109
7.20 Evolution of estimated variances in bulk coherent detector using logarithmic scale. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 110
7.21 Expected SKR for on-chip detector for different values of excess noise. . . . 111
7.22 Expected SKR for on-chip detector for different values of detection efficiency.111

8.1 Transmission windows in the near infra-red regime at Mauna Kea. . . . . . 116
8.2 Effective overall transmittance $T_{\text{eff}}$ as a function of the variance $\text{Var}(\tau)$ for different average transmittances $\langle\tau^2\rangle$. . . . . . . . . . . . . . . . . . . . . . . 119
8.3 Excess noise due to fading $\xi_{\text{fad}}$ as a function of fading variance $\text{Var}(\tau)$ for different overall transmission efficiencies $T_{\text{eff}}$. . . . . . . . . . . . . . . . . . 120
8.4 Fading mutual information. . . . . . . . . . . . . . . . . . . . . . . . . . . 121
8.5 Distribution of the estimation of $\tau$ using different values in the transmitted variance. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 124
8.6 PDTC $\mathcal{P}(\tau)$ for a receiver with aperture radius $a = 0.75$ m, beam width at receiver $W = 2.0$ m and beam wandering variance $\sigma^2 = 0.2$ m$^2$. . . . . . . . 126
8.7 Variance of the transmission coefficient. . . . . . . . . . . . . . . . . . . . 127
8.8 Transformation of $\langle\tau\rangle$ and $\text{Var}(\tau)$ into $T_{\text{eff}}$. . . . . . . . . . . . . . . . . . . 127
8.9 Secret key rate as a function of $\tau$ for the values of $T_{\text{eff}}$ and $\xi_{\text{eff}}$ . . . . . . . . 128
8.10 Secret key rate as a function of $\tau$ for the values of $T_{\text{eff}}$ and $\xi_{\text{eff}}$. . . . . . . . . 128
8.11 Secret key rate as a function of bin width for different minimum symbols per bin. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 129

9.1 Satellite inclination angle and period with respect to the altitude for circular polar orbits. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 137
9.2 Satellite orbit scheme. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 138
9.3 Satellite slant range for two different altitudes and inclinations. . . . . . . . 138
9.4 Variation of parameters during satellite passage. . . . . . . . . . . . . . . . 140
9.5 Influence of receiver size and pointing in passage PDTC. . . . . . . . . . . . 140
9.6 Average SKR over a passage as a function of satellite altitude for aperture of 40 cm. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 142
9.7 Influence of offset in the performance of the binning. . . . . . . . . . . . . 142
9.8 Average SKR over a passage as a function of satellite altitude for aperture of 75 cm. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 143

B.1 Measurement of a bipartite state. . . . . . . . . . . . . . . . . . . . . . . . 169

E.1 Normalized Doppler shift depending on the elevation [122]. . . . . . . . . 186

# Tables

2.1 Relevant properties of coherent detectors. . . . . . . . . . . . . . . . . . . . . 22
2.2 Relations between elements in the covariance matrix and measured values for untrusted scenario. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 24
2.3 Relations between elements in the covariance matrix and measured values for trusted detector scenario. . . . . . . . . . . . . . . . . . . . . . . . . . . . 29

7.1 Measured current response for each photodiode as a function of input light in each of the ports. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 101

10.1 Main characteristics of the presented experimental set ups. . . . . . . . . . 149

A.1 Comparison of Hilbert and phase space representations. . . . . . . . . . . . 158

B.1 Comparison of Hilbert and phase space representations for Gaussian states. 171

# INTRODUCTION

# Introduction to cryptography 1

1.1 Security concepts . . . . . . . 3
Hiding the information . . . . 4
Information-theoretical security . . . . . . . . . . . . . . . . . . 5
Distribution of the key . . . . 6
1.2 Quantum key distribution . . 7
BB84 . . . . . . . . . . . . . . . . 8
Common principles of QKD protocols . . . . . . . . . . . . . . . . 9
Relevant concepts . . . . . . 10
1.3 QKD today . . . . . . . . . . 12
Quantum technologies ecosystem . . . . . . . . . . . . . . . . . . 12
Criticism . . . . . . . . . . . . 13

Collaboration is a powerful force to accomplish many practical goals. In order for two or more autonomous entities to collaborate, they need to communicate using at least one channel. Messages consisting of sequences of symbols with previously agreed meaning are distributed among the entities and they might act accordingly. In a scenario where all the parties collaborate, getting the messages without errors is the main desirable quality of the communication link. Channels are not ideal and the resources available for communication are not infinite, so it is not possible to take for granted that a plain message will arrive without errors to the destination. Fortunately Claude Shannon demonstrated in 1948 [1] that information can be transmitted through a noisy channel without errors if we add certain amount of redundant information. This settle the basis for information theory and the development of modern communication systems.

## 1.1 Security concepts

In many occasions a subset of the population might not trust some other part of the community, but they would like to continue communicating in order to collaborate. This creates a division of users in trusted and untrusted parties which might share the communication medium. The fact of operating in an environment where the communication might be affected not only by noise and imperfections, but also deliberately by certain users, requires arrangements to circumvent the security issues that can arise in those scenarios. Secure communications is the generic term to denominate this framework of tools, which can provide a relatively flexible set of services to adapt to most practical cases.

The typical services of interest for the trusted parties are confidentiality, authentication, integrity, non-repudiation, availability and anonymity. We talk about authentication when the entities have the capability of proving their identity. When we can confirm that the message is complete we talk about integrity, and it is usually associated with the non-repudiation of received messages and availability (robustness to denial of service attacks). The capacity of communicating anonymously or hiding (partially) that the communication is taking place might be interesting in some occasions. All the services come at the cost of resources and can be combined in different fashions to attain multiple objectives.

Confidentiality is perhaps the most relevant property for the trusted parties, meaning that the original message would remain secret to the untrusted parties even if they have access to the message transmitted through the channel. There are several solutions to this problem, and they will be treated in more detail in the next sections of this chapter.

### 1.1.1 Hiding the information

Throughout History many methods to hide information have been invented. A three phase process can be identified in the most basic and practical schemes:

- The transmitter Alice A has a box with two inputs: (1) the plain message $p$ and (2) the secret key $k$. The output of the box is the encrypted message $m_k$.
- The encrypted message $m_k$ is transmitted through the channel to Bob who receives it, but some untrusted entities can also read the message.
- Bob has a box with two inputs: (1) the received encrypted message $m_k$ and (2) the secret key $k'$[1] . If the secret key corresponds to the encrypted message the output of the box is the plain message $p$.

Note that the security of the communication relies on two factors: the secrecy of the keys and the algorithms performed on the boxes. The first intuition might indicate that it is better to come up with ingenious designs for the operations in the boxes and keep them secret. This is called security by obscurity and it is not recommended in practice, as it is not possible to rule out that the enemy knows the system (as occurred during the WWII with the Enigma machine). This is a typical practice since Auguste Kerckhoffs enunciated his desirable features for a cryptographic system [2] and it was reiterated more formally by Shannon in the 20th century.

The current trend is to publish the design of the boxes and rely only on the secrecy of the key to guarantee the confidentiality of the communication. Of course the algorithms performed by the boxes must be non elementary because in that case it would be possible for an attacker to guess the key. For example, shift cipher (or Caesar's cipher) is a simple cryptographic method where the boxes only shift the letters of the alphabet by the value of the key. If the alphabet is known and relatively small, it would be possible for an attacker to guess the message trying iterations of the key.

The previous example raises the question of whether some algorithms are more secure than others, and if so, if it is possible to construct a perfectly secure algorithm. Those dilemmas are not easy to solve without a little bit more context. In practice the attacker will require to perform some work to try to decipher the messages in the channel. This work can be quantified in processing power, so in this sense it is possible to run benchmarks on the average number of operations required to decipher a message encrypted by a particular algorithm, which is typically a function of the number of bits used in the key. Most of the modern algorithms require an exponential processing time with respect to the size of the key, which makes them intractable in most cases. The performance of the cryptoanalysis benchmarks for

[1] In many schemes $k = k'$ and we talk about symmetric cryptography.

a particular algorithm can improve for two reasons: (a) a conceptual error is discovered in the cryptography scheme; (b) a better algorithm to treat the problem is discovered.

Many different encryption algorithms have been developed during the 20th century, and from this experience we currently have a good choice of algorithms (ciphers) in our hands. Perhaps the most well known symmetric cipher is AES [3] which is the NIST standard at the moment of writing. The algorithms can be implemented in software, which makes them a very versatile solution, and they can also be implemented in hardware when very high throughputs are necessary. As long as no breakthrough discovery happens, they remain a reliable resource for confidentiality.

Even though symmetric cryptosystems are thought to be secure for the short and medium term, their security is always related to the computational resources of the attacker, so the uncertainty about whether a message was decoded cannot be ruled out. Strategies to mitigate this assumption are key refreshment (renew the key every few time units) or the increase of the key size (but this also affects the computational requirements for the trusted parties).

It would be interesting to use a scheme of communication whose security does not depend on the computational resources of the attacker. Those schemes are indeed possible and are said to be information-theoretically secure.

### 1.1.2 Information-theoretical security

In 1917 Gilbert Vernam constructed a cipher that used a punched tape to encode the message via a XOR operation[2] . It operated with a tape loop for the key, so some weaknesses in the security were noticed and other implementations used the key only once, hence the name one-time pad.

In 1945, Shannon proved[3] [5] that the one-time pad protocol is secure independently of the computational resources of the attacker as long as three conditions are fulfilled:

- The key and the message are strings of the same length and are kept secret.
- The key is completely random.
- The key is only used once.

A communication protocol of this type opens the possibility of long term security, since the security is not compromised by the elapsed time since the communication. Interesting as it might seem it is not the most practical scheme for implementation.

One drawback is the requirement of true randomness, which prevents the use of pseudo-random number generators. A good candidate for true randomness generation are quantum random number generators (QRNG) which generate the samples from the entropy characteristic to fundamental quantum mechanical processes. The evolution of QRNG

[2] 2: The story is not completely clear, since the first mention of the XOR mechanism for encryption dates from 1882 by a certain Frank Miller [4].

[3] 3: It seems that Soviet scientist Vladimir Kotelnikov arrived to the proof in 1941.

in terms of rate, cost and size during the last few years has been remarkable, so this difficult is becoming less important.

The other main drawback is the size of the keys, which needs to be equal to the total size of the messages. If the key is pre-shared there can be issues with the storage. If the key is distributed then the bandwidth is doubled at best, since a key of the size of the message needs to be distributed. In this sense other symmetric systems like AES are less secure but still very competitive, since a key of a few kilobits can encode a much higher amount of plain message.

Nevertheless all current cryptosystems rely on the secrecy of the keys and their renewal (with the same rate as the message for one-time pad or regularly for other symmetric schemes). This announces the next subject on secure communications and main topic of this thesis: how to distribute the keys between the trusted users.

### 1.1.3 Distribution of the key

One option to distribute keys for symmetric cryptography is to pre-share them or to distribute them physically via a trusted courier. Although an interesting option, especially with the current capacity storage cost, in many occasions it is not practical and other dynamic schemes need to be implemented.

One of the first proposals to distribute keys without pre-shared secret is due to Merkle [6], Diffie and Hellman [7]. The objective is to share a key $K$ and the basic idea is that each user has two related keys: a secret key $K_S$ that is only known to the user, and a public key $K_P$ that is known to all the users (and thus they can do operations with it). Different evolutions of this asymmetric public key scheme exist for encryption and signature, but the basic idea is that some operations are easy to perform knowing $K_S$ but difficult if it is unknown. Famous implementations are RSA [8], based on the complexity of factorizing large numbers and ElGamal [9], based on the discrete logarithm.

The main impairment of asymmetric protocols is that the secret key would be discovered if the attacker could solve the functions that guard the security of the protocol (e.g.: factoring, discrete logarithm...), so their security is clearly computationally based. Asymmetric cryptographic schemes are in a more adverse situation in terms of security than symmetric systems, since more efficient algorithms are known to tackle asymmetric systems. In particular Shor's algorithm [10] is capable of efficiently solve the factoring and discrete algorithm problems, compromising currently used RSA. Shor's algorithm requires a fault tolerant quantum computer to be implemented, which does not exist at the time of writing, but considerable efforts are being invested in its construction and it is expected to be operational in the future.

A fully operational quantum computer would be a formidable tool for cryptoanalysts, so it is interesting to design mechanisms that are not vulnerable to algorithms that could exploit the advantages of a quantum computer. This trend is known as post-quantum cryptography and its security lays on the assumption that the set of NP (nondeterministic polynomial time) problems is not fully contained in the BQP (bounded-error quantum polynomial time) complexity class, which contains the problems that could be solved efficiently by a quantum computer. The problem is that the frontier between BQP and NP is not well established and there is no proven certainty about the existence of NP problems outside BQP[4] . For a certain problem we only know that no known algorithms exist at the moment, but they could be discovered in the future.

[4] We know that some NP problems that do not belong to P (polynomial time) belong also to BQP. The most famous example is factoring.

The challenge of post-quantum cryptography is to discover algorithms that can be implemented classically, for which no counter analysis algorithm is known (even within quantum algorithms). This classical nature makes them very flexible, since a simple software update would suffice to deploy them, but their main weakness is that the security might decrease after the communication time, since new algorithms could be discovered. For this reason they are not advisable for long term security.

The properties of quantum mechanics allow the characterization of the privacy shared by two parties after the exchange of symbols under certain conditions. Those symbols can be processed to generate a secret key $K$ common to both parties solving the problem of key distribution. Imperfections can be characterized by an arbitrary small security parameter $\epsilon$ that will remain constant with time, making it a good candidate for situations where long term security[5] is needed.

[5] Note that this paragraph only relates to the key exchange. The cipher used afterwards should also provide long-term security if we want to have this characteristic globally.

Different quantum key distribution (QKD) protocols can exploit the properties of quantum mechanics and information theory in a different way, but they rely heavily in the characterization of the communication channel. This makes the implementation more complex with respect to the classical counterparts, that rely mainly on mathematical abstraction implementable by software. In the following section we study the most relevant characteristics of these protocols.

## 1.2 Quantum key distribution

An article by Nick Herbert on superluminal communication [11] triggered two famous counter articles by Wootters and Zurek [12] and Dieks [13] formally proving the impossibility of creating an identical copy of an unknown quantum state. This concept is known today as no-cloning theorem and the idea is related to the 1970 article by James Park [14] showing that it is not possible to create a non-disturbing measuring mechanism.

During the decade of 1970 Stephen Wiesner had the idea of using the properties of quantum mechanics to devise a system that could prevent the forgery of bank notes [15]. In a generalization of his scheme the banknotes are released by the bank with a serial number and a series of quantum states[*]. The quantum states can have four possible values

[*] The storage of the quantum states is one of the most important practical impairments of this protocol, since it requires the use of quantum memories, which are currently in an early development stage.

forming conjugate observables that are chosen randomly and are only known to the bank[6] . When the users want to exchange the banknote with the bank, they need to send the quantum states associated with the serial number for verification. An honest user would have no problems passing the verification, but the user of a cloned banknote would only pass the test with probability $p^N$, with $N$ the number of states[7] . As $N$ becomes large the probability of detecting forged money approaches 1.

### 1.2.1 BB84

The same idea of conjugate observables was used by Charles Bennett and Gilles Brassard with a new purpose. They assumed that the two trusted entities Alice and Bob have at their disposal a quantum insecure channel and a classical authenticated channel. Then they can exchange information through the quantum channel and characterize if the channel has been eavesdropped revealing some information through the classical channel. This opens the possibility of indefinitely expanding a secret key using an insecure medium. In their famous BB84 protocol [16] they provide a possible implementation of this idea.

In the original protocol the conjugate states are implemented based on the polarization of light. Alice has a single photon source and a mechanism that can prepare states in two non-orthogonal bases $\{|H\rangle, |V\rangle\}$ and $\{|+\rangle, |-\rangle\}$. A perfectly random generator generates two bits, one to choose the basis and the other to choose the state in the basis, and they are stored in Alice's memory. A sequence of $N$ states is transmitted through the quantum channel. Bob chooses randomly the basis in which the photons are detected and stores in his memory the basis and the measured value. Once the complete sequence is received, Alice reveals the sequences of bases used for preparation and Bob reveals the bases used for measurement and the slots without measurements. With this information they can retain only the coincident values. At this point the generated and measured values should coincide if no errors occurred during the communication phase. In order to check the errors, Alice and Bob need to reveal some part of the key and check the mismatches, i.e. the error rate. A subsequent phase can purify the correlated values of Alice and Bob as a function of the measured errors[8] to obtain a perfectly private key.

The distinct property of the protocols of this kind is that they are particularly sensitive to the effects suffered by the quantum states that carry the information. That includes the noise on the channel and the imperfections on the system, but more importantly for security, the presence of eavesdroppers in the channel. Remember that a measurement implies the collapse of the quantum state and it would need to be regenerated in order to avoid the abandon of this value in the secret key. We can argue that if at the moment of communication only Alice knows the basis of the state, an eavesdropper Eve will need to perform her measurement in a random basis and regenerate the qubit. For the value to be part of the key Alice and Bob need to use the same

[6] In his article Wiesner used the photons in four polarization states $|H\rangle$, $|V\rangle$, $|+\rangle$ and $|-\rangle$ as quantum states. This is equivalent to choosing randomly two values in two non-orthogonal bases.

[7] For the set of states in the article $p = 3/4$.

[8] As in BB84 and similar protocols the states are independently transmitted through the channel it is typical to talk about qubit error rate (QBER). There is an upper bound to the error supported by each protocol.

basis, so two things can happen with the measurement of Eve: (a) with probability 1/2 Eve measures in the correct basis and regenerates the same qubit; (b) with probability 1/2 Eve measures in the wrong basis and (b1) with probability 1/2 the measurement is projected on the right value at Bob's (b2) with probability 1/2 the measurement projects in the wrong value. In cases (a) and (b1) which count for 3/4 of the total, the presence of Eve is not detected, but case (b2) will introduce a mismatch in the strings with probability 1/4. If Alice and Bob are willing to sacrifice $n$ bits revealing them, they can detect an eavesdropper in the channel with probability $1 - (3/4)^n$.

Some noticeable remarks can be discerned from this protocol:

- All the wrong measurements are assumed to be caused by Eve, even though in practice they could be produced by noise or imperfections in the system. This makes the protocol very secure, but it can also be too conservative for some applications.
- It will stop working as soon as Eve interferes too much. We will assume that the objective of the eavesdropper is to obtain information without obstructing the communication, so denial of service (DoS) attacks will not be considered. There are always simpler methods to prevent communication having access to the channel.
- It does not transmit messages, only the key. The real communication will take place later, using the generated key.
- Several assumptions are made, for example the availability of a perfect single photon source or perfect preparation and measurement of states.
- A certain number of assumptions are used to construct a mathematical framework that will allow the analysis of the security. In this case the probability of error as a function of the activities of Eve.

Many more QKD protocols have been invented since 1984, but the great majority share all these characteristics. The main distinction is the assumptions they make and how they treat the security problem. We can say that the groundwork of QKD is to construct a satisfying model of the communication system and develop a mathematical framework that takes into consideration the laws of quantum mechanics. The mathematical framework is usually called security proof and it will be valid only when the hypothesis of the model are valid. The security does not need to be perfect, but the probability of successful eavesdropping must be arbitrary small within the context of the model.

### 1.2.2 Common principles of QKD protocols

Most of the available QKD protocols can be divided into the following steps:

- **Distribution of quantum states.** Quantum states are created, transmitted and measured between the two entities. A process to agree on the used bases (sifting) is usually needed. After this phase Alice and Bob share two sets of partially correlated values.

- **Parameter estimation.** Alice and Bob reveal a random part of their correlated values in order to estimate the channel. The revealed values will not be used in the final key, so there is a trade-off between the values revealed to have an accurate estimation of the channel and the final length of the key.
- **Reconciliation.** The correlation in the first phase is not perfect and needs to be corrected. Classical error correcting codes can be used in most cases. The output of this phase is a shared string of values with no errors.
- **Privacy amplification.** Not all the values in the previous string are secret, so a classical process is performed in order to adapt the string to the secret key length predicted by the security proof as a function of the estimated parameters[9] . The result is a shared secret key.

Remark that only the first phase involves quantum mechanics directly, the rest of the steps being completely classical. For this reason in proof-of-principle scenarios it is typical to complete the quantum distribution and obtain the estimated parameters. The security proof will predict the length of the key if the reconciliation efficiency is known. While a commercial product would require the completion of all phases we will use the proof-of-principle approach.

### 1.2.3 Relevant concepts

In 1991 Artur Ekert [17] published E91 a QKD algorithm that was conceptually different from BB84, since the security was based on the use of entangled photons. Other protocols based on entanglement like BBM92 [18] followed soon. This opened the division between entanglement-based protocols and non-entanglement-based ones. Very soon it was realized that there is a framework where an entanglement-based protocol has a non-entanglement equivalent and vice-versa. In some occasions the implementation is more natural using entangled states, but generally the non-entanglement version (also called prepare and measure) is preferred.

The concept of using entanglement for QKD is interesting because it expanded the idea of entanglement swapping to its use as quantum repeaters[19]. Optical amplifiers as used in classical communications would irreversibly corrupt the quantum states, so they cannot be used to recover the signal lost due to the channel attenuation. The idea behind quantum repeaters is to use quantum teleportation in order to guarantee the distribution of entangled photons between two locations. It is a promising but challenging field that would be useful not only for QKD, but for other communication protocols as well.

The losses in the channel will degrade the achievable key exchange between the trusted parties. As the losses are function of the channel distance this seriously limits the range of QKD. The limits for a repeaterless setting can be calculated independently of the protocol [20],

[9] The size of the key will decrease for worse conditions of the estimated parameters, becoming null after certain parameter conditions are exceeded.

although in practice some protocols will perform better than others at longer distances. A recently developed family of protocols called twin-field (TF-QKD) [21, 22] has been able to surpass the repeaterless limit, but it can be interpreted as a repeater model simplified for implementation.

One possible bypass to overcome the distance limit is the use of trusted nodes, i.e. dividing a long communication distance into several shorter point-to-point links. An interesting aspect of trusted nodes is that a network of trusted users could be constructed, but the inconvenience is that all the nodes have information about the key, so they need to be trusted. There should be also some physical security mechanism to ensure that the intermediate devices are not tampered with. The most extensive trusted node network at the moment of writing expands for more than 2 000 km between several major cities in China[23].

A possible concern with the proposals so far is that a malfunction (imperfection or malicious attack) in some of the components of the system could compromise the security of the system. In 1998 Mayers and Yao [24] introduced the idea that self-testing quantum systems would be useful to reduce this device dependence on QKD. Self-testing only considers the input-output statistics of a black box performing some operations, and in order to prove honesty from the black box a suitable function should be used. Ten years later Colbeck [25] proposed the use of Bell tests in order to verify the honesty of the devices. The protocols working under this settings have the advantage of removing unnecessary trust in the components, hence their name device independent protocols (DI-QKD). The concept can be extended to randomness expansion and randomness amplification. The main drawback is their complex implementation since it is difficult to obtain loophole-free Bell test measurements or equivalent [26–28].

A less restrictive approach is to assume that only the detectors can be untrusted leading to the family of measurement device independent [29] protocols (MDI-QKD). They are more easily implementable than DI protocols [30] and eliminate the dependence on the trustfulness of the detector (the measurements can even be done by a third untrusted party).

So far we have considered the exchanged states independently. It is possible to use some relation between the different states as the source of correlation between Alice and Bob. The family of protocols that uses the phase between consecutive states as resource is called distributed-phase reference QKD. The two main examples are differential phase shift (DPS)[31, 32] and coherent one-way (COW)[33]. Their main advantage is the simplification under some operational settings.

The great majority of the previous protocols work with states that can take only a discrete set of values. This simplifies the analysis of the system, but can make the implementation difficult since those states can be difficult to generate or detect. QKD can also be extended to an infinite dimensional Hilbert space in what is called continuous variable QKD (CV-QKD) in contrast to the previous ones, referred as discrete variable (DV-QKD). The infinite dimensional Hilbert space can be simplified to a finite dimension working in phase space, and for Gaussian states (and in particular coherent states) the information can be bounded in order to obtain security proofs. The main advantage of this family is the simplification of the implementation, as it is possible to construct a commercial QKD system using only standard telecommunication technology.

Some of the previous characteristics can be combined in order to adapt to different scenarios. For example it is possible to have MDI-CV-QKD taking the advantage of CV and MDI approaches. Not all the combinations are possible but many of the concepts can be combined.

## 1.3 QKD today

At the time of writing QKD is an emerging technology that is continuously evolving and expanding. Numerous groups in the world work on the development of new ideas and the improvement of the technology in order to facilitate the access to high secret key rates at convenient distances. Other groups focus on the weak points of protocols and implementations to ensure that they work as expected under malicious conditions in what is known as quantum hacking. This provides an iterative approach where protocols and implementations are improved to work in more realistic conditions. A simple example would be BB84 with decoy states[34], an evolution of BB84 that can work with weak coherent states of light instead of perfect single-photon sources.

It is not the purpose of this document to cover the whole field since extensive general QKD reviews can be found in the literature [35, 36], as well as more specific ones on CV-QKD [37]. We will only mention the features more closely related to this document.

The use of photonic integrated chips (PIC) for applications in quantum technology has grown extensively over the last years. Researches in Bristol [38] have recently developed silicon chips capable of running several DV-QKD protocols. The use of PICs for CV-QKD has also recently proven viable [39, 40] obtaining levels of shot noise compatible with the generation of key.

During several years the use of satellites for QKD was restricted to the general purpose satellites available in orbit, either using retro-reflecting satellites [41] or optical classical communication ones [42]. It was not until the use of satellites prepared for QKD by Japan [43] and China [44, 45] that the interest in the field exploded [46]. Its interest relies mainly on the possibility of communicating over intercontinental distances, exchanging key between different passages of low earth orbit (LEO) satellites.

### 1.3.1 Quantum technologies ecosystem

QKD can be understood as a primitive (a resource) for other tasks, and in this sense it is one of many of the primitives without classical equivalent that are expected to be provided by the so called second quantum revolution. The first revolution being the one that used the properties of quantum mechanics to construct the devices that allowed the current (classical) information age (lasers and integrated transistors), the second quantum revolution focuses more on the processing of information using its quantum properties. This affects communications, computing and sensing devices, as well as generators of entropy such as quantum random number generators (QRNG).

QRNGs are probably the most closely related technology to QKD since randomness is required to run the protocols. Many technologies are already available and interestingly some of them could be implemented as PIC [47–50] and be integrated in the same die as the QKD devices.

Quantum communications is a very diverse field, containing not only QKD but also other primitives like secret sharing[51], coin-flipping [16, 52], quantum money [53, 54], communication complexity [55, 56] and many other sub-fields. The capstone would be the construction of a Quantum Internet [57] capable of integrating all these services, task that is already under development [58].

Quantum computing can also benefit from the developments in QKD, since additional functionalities like blind computing or verification could use QKD as a primitive if required. In summary, QKD is evolving in an environment that is targeting technical maturity and this should be beneficial for the introduction of QKD and related technologies in more facets of the society.

### 1.3.2 Criticism

QKD is probably the first quantum information technology that has been successfully commercialized but, although functional, QKD systems require equipment and conditions that are not suitable for all needs. For example, a quantum channel might not be available or the hardware requires special conditions. This contrasts with classical solutions that can run on any software platform typically. This makes QKD in general less practical, but it provides a functionality that has no classical equivalent. The most promising classical alternative at this moment is post-quantum cryptography, that could probably provide a sufficient level of security for most users, but it is not guaranteed that its security would not decrease over time. It is likely that both technologies will evolve to find their place in the market and coexist in many environments.

One aspect that reduces the functionality is the limited achievable distance without repeaters. This requires the creation of a network of trusted nodes which is a far from optimal solution. The situation is expected to improve with the arrival of efficient repeaters and with the generalization of satellite QKD.

The typically low secret key rates are also a source of debate, since they would make the combination of QKD and one-time pad difficult in practice. An alternative is to combine QKD with AES or other symmetric cryptosystems, using AES to do the encryption and QKD to renew the key as frequently as possible. The increase of secret key rate will be one of the main topics of this manuscript.

The fact of requiring an authenticated channel means that there should be some pre-shared secret between the trusted parties before the beginning of the communications. This limits the possible scenarios for the application of QKD.

Another important criticism comes from the lack of standards, as with so many different protocols and configurations it is difficult to evaluate the security of a potential commercial system. This situation has recently changed with the creation of groups with the responsibility of developing security standards for QKD equipment and protocols, like the Industry Specification Group (ISG) on Quantum Key Distribution for Users (QKD) of ETSI [59]. ITU, IETF and IEEE are also making progress on the subject.

The elevated cost is claimed as one of the factors delaying the implementation of QKD. This is probably due to the fact that most of the systems are still in an early R&D phase. A reduction of the cost is expected from the integration of devices in chips of different kinds, maybe coexisting with other technologies like classical communications.

The previous arguments have led to the idea that QKD is a very specialized tool that can only serve niche applications. Although this might be true up to a certain point, it is also true that QKD is the only known method capable of distributing secret keys dynamically with proven long term confidence. This property has generated a lot of commercial interest, and all the advances that can be introduced (rate, range, cost, standards...) will improve the reception of QKD among more actors and scenarios.

# Introduction to CV-QKD 2

2.1 Basic concepts . . . . . . . . 15
Security conditions . . . . . 15
QKD using continuous-variables . . . . . . . . . . . . . . 15
Conditions on the security proofs . . . . . . . . . . . . . . . 16
Considerations . . . . . . . . 17
2.2 Coherent detection . . . . . 17
Coherent detection: regimes of operation . . . . . . . . . . . . . 19
Coherent detection in CV-QKD . . . . . . . . . . . . . . . . 20
Coherent detection: noise consequences . . . . . . . . . . . . . 22
2.3 CV-QKD: entanglement version . . . . . . . . . . . . . . . . . 23
2.4 Some relevant security proofs . . . . . . . . . . . . . . . 25
Security proof against collective attacks for Gaussian modulation . . . . . . . . . . . . . . . . . 25
Security proof against collective attacks under linear channel for QPSK modulation . . . . . 26
2.5 CV-QKD: Prepare and measure . . . . . . . . . . . . . . . . . 27
A CV-QKD protocol: GG02 27
2.6 Introduction of imperfections . . . . . . . . . . . . . . . . 28
Noisy and inefficient detector29
Finite size effects on the parameter estimation . . . . . . . . . . 31
2.7 Motivations of this thesis . 33

The objective of this chapter is to explain the basic concepts of CV-QKD, covering the most usual implementations and explaining their characteristics. Additional bibliography can be found in the previous theses of the group [60–66] and the abundant literature on the subject.

## 2.1 Basic concepts

The objective of QKD is to convert a set of $N$ exchanged states into a chain of $\ell$ secret bits common to Alice and Bob. The secret key rate (SKR) can be defined as

$$K \equiv \frac{\ell}{N} \tag{2.1}$$

It is desirable that the SKR is as high as possible under certain given conditions, but certain security conditions need to be satisfied.

### 2.1.1 Security conditions

Security is a rather abstract concept that does not have a straightforward definition. In what relates to QKD, the most widespread definition accepted by the community has been proposed by Renato Renner [67]. The underlying concept is the distance between a perfect key and the key obtained key after the QKD process, and the possibility of accepting an arbitrary small failure probability $\epsilon$. Written in simple words this implies that for a QKD protocol to be $\epsilon$-secure, the keys computed by Alice and Bob need to be (up to a small probability $\epsilon$)

- identical,
- uniformly distributed,
- independent of the knowledge of the adversary.

An interesting property of this definition is that it is composable [68] and can be extended to any QKD system.

### 2.1.2 QKD using continuous-variables

The previous notions are general for any QKD system including the systems based in continuous-variables (CV) that we are going to study in this document.

The use of CV states for QKD raises from the fact that the non-orthogonality property required for QKD can be obtained from the characteristics of quadrature measurements in phase space (appendix A). The first systems were conceived using squeezed states [69–71] but very soon the it was realized that coherent states could also be used [72, 73].

The possibility of using squeezed or coherent states is very interesting, since in one hand it is possible to use the mathematical machinery related to Gaussian states (family to which both squeezed and coherent states belong), and in the other hand, especially for coherent states, it simplifies the equipment required for the preparation and measurement of states. This fact is crucial, since those devices are easily and cost-effectively accessible, which is one of the most interesting characteristics of CV-QKD with respect to DV-QKD.

Non-orthogonality is not sufficient for QKD and a protocol is required in order to generate a secret key and guarantee the security at the same time. Different security proofs have been developed during the years comprising the many useful CV-QKD scenarios, but some of them still remain a challenge.

### 2.1.3 Conditions on the security proofs

The security of QKD is based on mathematical constructions over physical assumptions. The physical assumptions are in one hand the laws of quantum mechanics, which are imposed, and in the other the model of the system, that can be chosen. A mathematical framework over the physical assumptions estimating the secret information between Alice and Bob is called a security proof.

Different models of the system will have different security proofs and one model can have several security proofs, not necessary tight in terms of optimization of the secret key. Also for some models it might be hard to find a security proof and it is not available at the moment.

Some parameters that might influence the model are the type of states involved (coherent, squeezed, thermal...), the type of detector (one projection, simultaneous projections...), the length of the communication (asymptotic, finite), the modulation format (continuous, discrete, Gaussian, QPSK...), the characteristics of the channel and many more.

We will assume that the source of states will generate coherent states modulated using a discrete modulation that in some cases (Gaussian) can be well approximated to a continuous distribution. We will contemplate the cases of one projection measurements and simultaneous projection measurements.

Security of QKD relies on evaluating the transmission channel, and its evaluation may be unwarranted if the number of symbols used in the estimation is too small. Therefore one of the most difficult conditions to tackle is the finite number of symbols used in a key. We will assume that the number of exchanged states is sufficient to approach the asymptotic limit and only a practical consideration on the finite size effects will be taken in the parameter estimation.

The type of channel (lossy, noisy, linear, general...) is also important, as well as the resources assigned to the eavesdropper Eve. While the rest of resources are still considered unbounded, if we restrict the quantum capacities of Eve we can distinguish three possible attacks that she can perform:

- **Individual attacks**. Eve can interact individually with the states sent by Alice and store her ancillae in a quantum memory. She will be able to perform measurements on them only before the error correction phase.
- **Collective attacks**. Similar to individual attacks, but in this case Eve can wait until the end of the process to perform the best possible collective measurement on her ensemble of ancillae.
- **Coherent or general attacks**. In this case the interaction with Alice's states is done collectively and the measurements on Eve's ancillae can be performed jointly after the end of the process. They are the most powerful attacks allowed by quantum mechanics.

### 2.1.4 Considerations

A CV-QKD implementation can have at least two possible versions, one using entangled states called entanglement version, and other that does not use entangled states and is called prepare and measure (P&M). They are completely equivalent from the theoretical point of view and security, but typically it is easier to perform the mathematical procedures using the entanglement version, and the physical implementation with the prepare and measure version since it is generally easier to build.

We will start describing the process of coherent detection, taking into account the typical perspectives in Physics and Engineering. We will continue describing a basic scheme using the entanglement version of the protocol, demonstrating some simple but relevant security proofs. The GG02 protocol will be explained afterwards and the previous basic model will be extended to consider realistic imperfections on the system.

## 2.2 Coherent detection

We would like to work with coherent states with a low average photon number $\langle n \rangle$, which are difficult to detect using direct optoelectronic mechanisms, since their average power at the detection will be lower than the typical thermal noise. An option to improve this kind of detection is to use another coherent state of much higher power that interferes with the received signal. This state, that can be generated at the receiver and does not need to be modulated, is generally called local oscillator (LO) and serves as a local mode reference in coherent detectors, i.e. the results of the measurements are related to the polarization, frequency and phase of the LO.

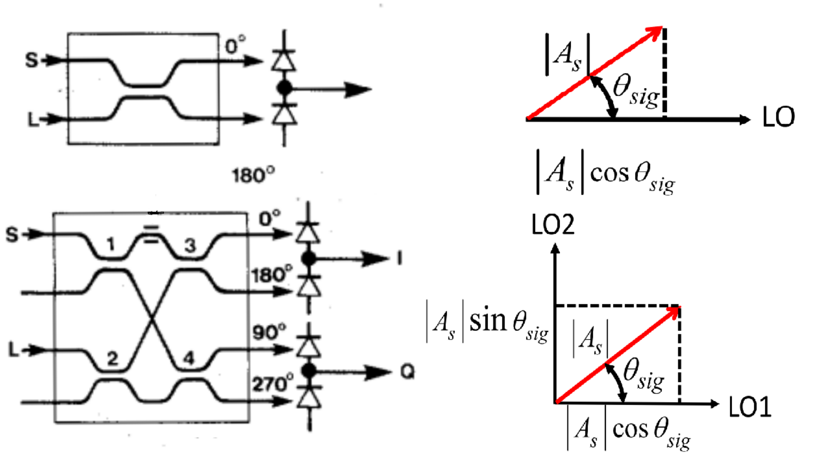


**Figure 2.1:** Optical hybrid scheme. Functional representation of 180° (top) and 90° hybrids with photodetectors in balanced configuration. The signal phasors with respect to the LO are represented in the right side for each case. Figure adapted from [74, 75].

The optical element that mixes the signal is called optical hybrid and can have different configurations. The most simple configuration corresponds to the 180° hybrid (a beam splitter) that has two inputs and two outputs differentiated by a phase of 180°, as can be seen in figure 2.1. At least one of the outputs needs to be read by a photodetector, but in order to maximize the efficiency it is convenient to read both outputs, and as they are in opposite phase if we use a balanced detector we can eliminate the continuous part of the detected signal, which typically does not add information. The photocurrents at each of the photodiodes in the upper part of figure 2.1 is

$$\begin{aligned} I_1(t) &= \frac{R}{2}\left[P_s(t) + P_\ell + 2\sqrt{P_s(t)P_\ell}\cos\left\{\omega_{IF}t + \theta_{sig}(t) - \theta_\ell(t)\right\}\right] \\ I_2(t) &= \frac{R}{2}\left[P_s(t) + P_\ell - 2\sqrt{P_s(t)P_\ell}\cos\left\{\omega_{IF}t + \theta_{siq}(t) - \theta_\ell(t)\right\}\right] \end{aligned} \tag{2.2}$$

and the difference of both in balanced configuration is

$$I(t) = I_1(t) - I_2(t) = 2R\sqrt{P_s(t)P_\ell}\cos\left\{\omega_{IF}t + \theta_{sig}(t) - \theta_\ell(t)\right\} \tag{2.3}$$

The measurement in a 180° hybrid gives a real value that can be interpreted as the projection over the LO mode, giving a phasor whose angle is illustrated at the top right part of figure 2.1.

Another possibility for the interference is to use a device with four inputs and four outputs where each output is separated by a phase of 90°. The outputs can also be grouped by 180° to take advantage of the balanced detection, but in this case we have two real values that correspond to the projections with the original LO and the LO with a phase of 90°. Those values are typically combined in a complex number and represent the measured values over the two IQ quadratures (in-phase and quadrature):

$$I_c(t) = I_I(t) + iI_Q(t) = R\sqrt{P_s(t)P_\ell}\exp\left[i\left\{\theta_s(t) + \theta_n(t)\right\}\right] \tag{2.4}$$

This last kind of devices is typically called 90° hybrid or coherent detector with phase diversity, and only two of the inputs are used. They can be duplicated adding a polarization beam splitter (PBS) in order to obtain diversity in polarization (i.e. two inputs and eight optical outputs). Note that the two types of detectors described are only sensitive to the phase, but its derivative (the frequency) will play an important role in the mode of operating the devices.

### 2.2.1 Coherent detection: regimes of operation

Coherent detectors can be operated in different conditions depending on the mode matching. Let us begin assuming that the polarization is controlled by an independent mechanism and that the interference is only dependent on the frequency and the phase. Alice will generate a baseband signal $a(t)$ of bandwidth $B$ that will be mixed by the carrier tone at frequency $\omega_s = \frac{c}{\lambda_s}$ to produce an optical signal of bandwidth $B$ centred at $\omega_s$. It can be represented as

$$s(t) = a(t)e^{i\omega_s t} \tag{2.5}$$

This signal will arrive with an average number of photons per symbol $\langle n_r \rangle$ at Bob's coherent detector and his objective will be to maximize the information from the photons arriving to his signal input. In the optical hybrid the LO with frequency $\omega_{\mathrm{LO}}$ will be mixed with the received signal in order to obtain (1) a gain by a factor $\sqrt{P_\ell}$ and (2) a reference for the phase. It is possible that the carrier frequency of the signal is not matched with the LO frequency and we have a beat at an intermediate frequency $\omega_{\mathrm{IL}} = |\omega_{\mathrm{LO}} - \omega_{\mathrm{s}}|$. We can use a scheme considering the positive and negative images of the signal involved in the mixing, like in figure 2.2. It is possible to distinguish three particular cases as a function of the value of $\omega_{\mathrm{IF}}$:

- $\omega_{\mathrm{IF}} = 0$ and both frequencies match. The overlap of the spectral images is perfect and the signal is directly in baseband, i.e. no additional demodulation is needed as the phase observed in the phasors of figure 2.1 does not depend on the $\omega_{\mathrm{IF}}$. This mode of operation is very interesting since the demodulation is direct and the noise the weakest possible, but it is difficult to obtain in practice since an optical phase locking loop (OPLL) needs to be implemented.
  - In a 180° hybrid equation 2.3 simplifies to

    $$I(t) = 2R\sqrt{P_s(t)P_\ell}\cos\left\{\theta_{sig}(t) - \theta_\ell(t)\right\} \tag{2.6}$$

    which is the projection of the signal phasor over the LO reference. Only one real signal is recovered, hence the information is limited to the positive part of the spectrum and only one projection is measured at the time[11] . The fundamental SNR is optimal and it corresponds [74] to $\mathrm{SNR_f} = 2\langle n_r \rangle / N_0$.

[11] A phase modulator can be introduced in order to measure arbitrary phases, but not simultaneously.

    - A 90° hybrid obtains a complex signal that can be used to recover all the information of the spectrum and the two quadratures are measured simultaneously, but with a penalty of 3 dB in the SNR with respect to the 180° hybrid.
- $\omega_{\mathrm{IF}} > B/2$ and there is no overlap in the spectrum. Both 180° and 90° hybrids can recover the entire spectrum and suffer from the uncertainty penalty of measuring the two quadratures at the same time. As can be inferred from equations 2.3 and 2.4 there is a residual modulation at $e^{i\omega_{IF}}$ that needs to be treated in order to recover the signal. This can be done using another mixing step (in the RF range typically) or directly digitally, but it can be noisy if the band is large.
- $0 < \omega_{\mathrm{IF}} < B/2$ and there is overlap in the spectrum.
    - The overlap in the spectrum is an issue for 180° hybrids since they cannot discriminate the content of the coincident part as they only provide one real value.
    - For a 90° hybrid it is possible to work with an overlapped spectrum, since the complex signal obtained contains the information of the two spectral images. This case is very interesting since it allows the operation with performances close to $\omega_{IF} = 0$ but without the need of an OPPL. In the absence of OPPL the detuning will be a function of time $\omega_{IF}(t)$, but the required bandwidth needs to be only slightly higher than the signal bandwidth to accommodate it. This mode of operation is generally called intradyne and typically the demodulation and the required processing are done digitally.

Table 2.1 summarizes the most relevant characteristics of the different modes of operation, but the main message is that measuring two quadratures simultaneously introduces a 3 dB impairment in the SNR and that the choice of hybrid will affect the possible modes of operation.

The telecommunications community typically uses the terms homodyne to refer to the operation when $\omega_{IF} = 0$ and heterodyne when $\omega_{IF} > B/2$, since they are typically more concerned with the demodulation steps. In physics the demodulation is usually direct ($\omega_{IF} = 0$) and the term homodyne refers typically to the fact of measuring only one projection, while heterodyne is used for the simultaneous measures of two projections (if the demodulation is direct a 90° hybrid is used). Due to this conflict of notation we will try to avoid these terms in the rest of the text and we will refer directly to the number of simultaneous quadratures projected (single or double projection) or the intermediate frequency[12] .

### 2.2.2 Coherent detection in CV-QKD

The great majority of CV-QKD implementations up to recent times were in the scenario $\omega_{IF} = 0$ in the line of [76]. This can be achieved using the same coherent source for signal and LO and in most cases the

[12] For the CV-QKD community homodyne can be understood as a 180° hybrid operating at $\omega_{IF} = 0$ and heterodyne to the rest of scenarios that measure two simultaneous quadratures.

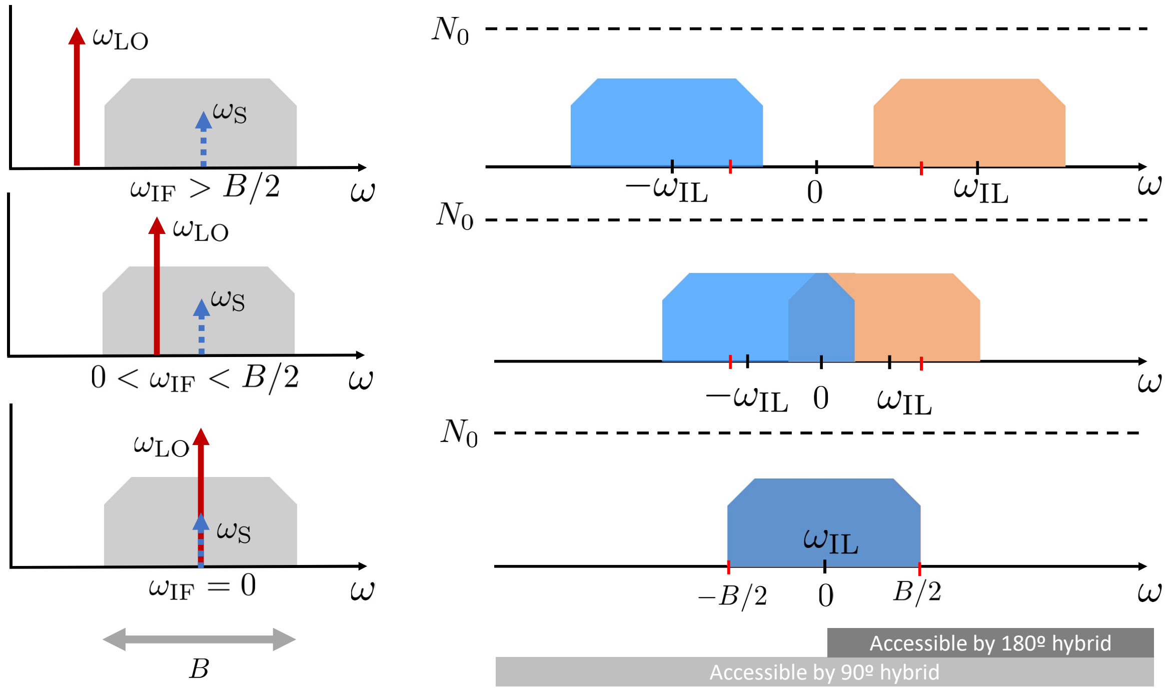


**Figure 2.2:** Optical mixing of signal and LO as a function of the frequency offset. The left side of the figure illustrates an optical signal of bandwidth $B$ centred at $\omega_{\mathrm{S}}$ before being mixed with a LO at frequency $\omega_{\mathrm{LO}}$. Three cases are studied depending on the frequency separation between the LO and the signal carrier. The right side of the figure depicts the result after mixing, reflecting the two spectral images and its possible overlap. Note that a 180° hybrid would produce a real sequence, which has a Hermitian spectrum, i.e. the left side of the spectrum does not provide information and it is not typically represented. This implies that a 180° hybrid would only be able to recover the positive side of the spectrum of the mixed signal. It is only when $\omega_{\mathrm{IF}} > B/2$ that a 180° hybrid could recover all the information of the original signal.

LO is transmitted through the same channel as the signal using some multiplexing mechanism. The signal and LO in those transmitted LO (TLO) schemes are mutually coherent, so only a global phase needs to be recovered between Alice and Bob, something that can be easily done even with single quadrature measurements. For this reason phase diversity is not typically implemented in those set ups, since a better SNR can be achieved without it, although nothing prevents from its application.

The transmission of the LO through the channel is not an optimal approach, since it is energy and bandwidth inefficient and can be a vulnerability for side channel attacks [77]. The trend in recent years is to transit from TLO schemes to real local LO (LLO) systems, transmitting only the signal through the channel and generating the LO at Bob's [78, 79]. The main difficulty of this scheme is to recover the mode of the two lasers. Regarding the frequency mixing, in general we will have $\omega_{IF} \neq 0$ and we can take three possible actions:

- Implement an optical phase locked loop (OPLL) and recover $\omega_{IF} = 0$. This is in general difficult and costly to do.
- Work at $\omega_{IF} > 0$ using a 90° hybrid [80].

**Table 2.1:** Relevant properties of coherent detectors.

| | **180° hybrid** | **180° hybrid** | **90° hybrid** |
|---|---|---|---|
| | $\omega_{IF} = 0$ | $\omega_{IF} > B/2$ | $\omega_{IF} \geq 0$ |
| **Photocurrent expression** | $I(t) = 2R\sqrt{P_s(t)P_\ell}$<br>$\times \cos\left\{\theta_{sig}(t) - \theta_\ell(t)\right\}$ | $I_c(t) = 2R\sqrt{P_s(t)P_\ell}$<br>$\times \exp\left[i\left\{\theta_s(t) + \theta_n(t)\right\}\right]$ | $I_c(t) = I_I(t) + iI_Q(t)$<br>$= R\sqrt{P_s(t)P_\ell}$<br>$\times \exp\left[i\left\{\theta_s(t) + \theta_n(t)\right\}\right]$ |
| **Measured quadratures** | 1 | 2 | 2 |
| **Fundamental SNR** | $2\frac{\langle n_r \rangle}{N_0}$ | $\frac{\langle n_r \rangle}{N_0}$ | $\frac{\langle n_r \rangle}{N_0}$ |
| **Demodulation** | Direct | Additional step required | Direct if $\omega_{IF} = 0$,<br>additional step otherwise |
| **Detector bandwidth** | $B/2$ | $> B$ | $> B$ |
| **Drawbacks** | Requires PLL<br>Only one quadrature | Higher noise<br>Cannot work if $0 < \omega_{IF} < B/2$ | Higher noise<br>Uses two (balanced) detectors |
| **Advantages** | Optimal SNR<br>Low detector bandwidth<br>Direct detection | Two quadratures with one (balanced) detector | Can work if $0 \leq \omega_{IF} \leq B/2$ (intradyne) |

- Work at $\omega_{IF} > B/2$ using a 180°.

The use of 90° hybrids and $\omega_{IF}(t) \approx 0$ (intradyne) with polarization diversity (double polarization, DP) is practical because the bandwidth of the mixed signal will fit on the bandwidth of the detector without further down-conversion to baseband. The four output signals can be digitized and all the processing can be done digitally correcting the signal accordingly and without the use of actuators like OPLL or polarization controllers. This is the most common approach in classical communications and the one on which we will focus in the next chapters.

### 2.2.3 Coherent detection: noise consequences

The fundamental noise in coherent detectors will be given by the Poissonian arrival of photons to the detector (shot noise) and the number of quadratures measured. As the main source of photons is the LO, the current variance in the detector is well approximated by

$$\left\langle \Delta I^2 \right\rangle = 2eI_\ell B \tag{2.7}$$

The fact that the shot noise depends only on the LO implies that this value should be calibrated. In most occasions it is more practical to do it after detection, amplification and digitalization, in the units managed by Bob's software (typically quantized volts). As shot noise does not come alone in this setting, it is important to distinguish it from other sources of noise like thermal noise.

In general, high values of LO power are interesting to overcome other noise sources, but it is important to satisfy the requirement of linear operation, i.e. the LO should not saturate the detectors and the detectors should not introduce classical noise that is function of the optical power (e.g. relative intensity noise RIN).

Briefly, if the detector is linear and the shot noise can be reliably calibrated, coherent detectors can be used for CV-QKD.

## 2.3 CV-QKD: entanglement version

Let us assume that Alice can generate a two-mode squeezed state[13] with covariance matrix $\Gamma$

$$\Gamma = \begin{pmatrix} V \cdot \mathbb{1}_2 & Z \cdot \sigma_z \\ Z \cdot \sigma_z & V \cdot \mathbb{1}_2 \end{pmatrix} \tag{2.8}$$

where $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ is the third Pauli matrix, $V = V_A + 1 = 2|\alpha|^2 + 1 = 2\langle n_t \rangle + 1$ is the variance of the state taking into account the fundamental shot noise $N_0$ (the shot noise will be referred as one shot noise unit: $N_0 = 1$ SNU), $V_A$ is the variance in the displacement of the state normalized to the fundamental shot noise, $\alpha$ is the displacement vector in phase space, $\langle n_t \rangle$ is the average number of photons per symbol at the input of the channel and $Z$ is a function of $V$ that will vary depending on the distribution of the states (we will see that for Gaussian modulation $Z = \sqrt{V^2 - 1}$).

Alice measures one part of the two-mode state using a double projection coherent detection and transmits the other part to Bob, along a lossy noisy channel with transmission efficiency $T$ and excess noise $\xi$*. Through a process of symmetrization[14] [64] it is possible to guarantee that the state after the transmission through the channel and before the measurement by Bob can be expressed by the following covariance matrix

$$\Gamma_{AB} = \begin{pmatrix} V \cdot \mathbb{1}_2 & Z \cdot \sigma_z \\ Z \cdot \sigma_z & (1 + TV_A + T\xi) \cdot \mathbb{1}_2 \end{pmatrix} \tag{2.9}$$

At this point Bob can apply a projective measurement considering one or two quadratures. The equivalent model of the described scenario is represented for both scenarios in figures 2.3 and 2.4. If no beam splitter is used and the measurement is considered only on one projection the covariance matrix after the measurement would be

$$\Gamma_{AB|b}^{1\text{quad}} = \begin{pmatrix} V - \frac{TZ^2}{1+TV_A+T\xi} & 0 \\ 0 & V \end{pmatrix} \tag{2.10}$$

[13] 13: Two-mode squeezing involves two modes of the electromagnetic field that, with a linear combination of the quadratures of the two fields, exhibits quantum noise reduction below the shot noise level.

[14] 14: The basic idea of symmetrization is to take advantage of some symmetries of the QKD protocols, like the invariance of the protocol to the order of exchanged symbols.

* The optimal point for Eve to attack is the input of the channel (the output of Alice), so in this document we will use this point as the reference for the excess noise $\xi$. In practice $\xi$ is estimated at Bob's and its value corresponds to $T\xi$ (or $\eta T\xi$ considering a detector of efficiency $\eta < 1$).

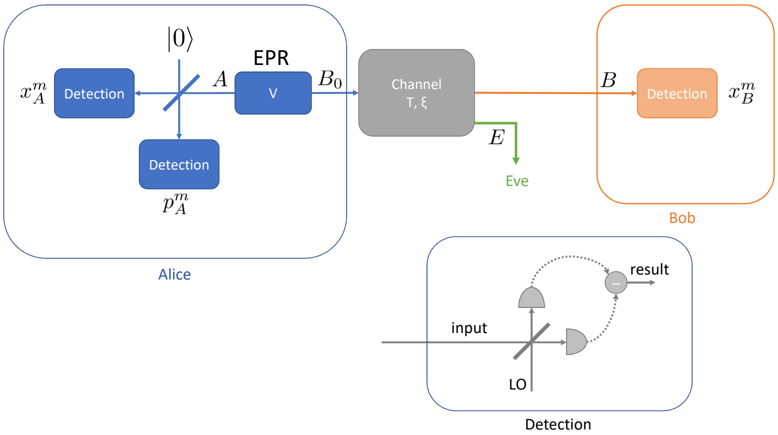


**Figure 2.3:** EPR scheme for the measurement of one quadrature at Bob's. Each detection block implies the coherent detection of the bottom block.

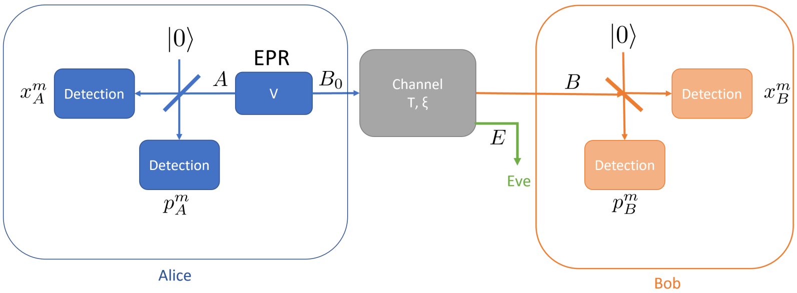


**Figure 2.4:** EPR scheme for the simultaneous measurement of two quadratures at Bob's. Each detection block is as in figure 2.3

If the projection is done over two projections the covariance matrix after the measurement would correspond to

$$\Gamma_{AB|b}^{2\text{quad}} = \begin{pmatrix} V_A + 1 - \frac{TZ^2}{TV_A+2+T\xi} & 0 \\ 0 & V_A + 1 - \frac{TZ^2}{TV_A+2+T\xi} \end{pmatrix} \tag{2.11}$$

These matrices, with three independent variables $V_A$, $T$ and $\xi$, will be important to bound the information that an eavesdropper can obtain from the communication. An interesting fact is that from the measurements done by Alice and Bob we can establish a system of three independent equations that groups the three previous variables (shown in table 2.2), i.e. we can construct the covariance matrix from the measurements. This is the cornerstone of CV-QKD and will allow us to construct security proofs depending on the conditions assumed for the implementation.

**Table 2.2:** Relations between elements in the covariance matrix and measured values for untrusted scenario. Note that in this model all the variances besides $V_A$ and $N_0$ are considered excess noise. The possible losses inside Bob's detector are also assumed untrusted and considered in $T$. Variances are considered normalized to $N_0$ and $N_0 = 1$ SNU.

| Single quadrature | Double quadrature |
|---|---|
| $\langle x^2 \rangle = V_A$ | $\langle x^2 \rangle = V_A$ |
| $\langle xy \rangle^2 = TV_A$ | $\langle xy \rangle^2 = TV_A$ |
| $\langle y^2 \rangle = 1 + TV_A + T\xi$ | $\langle y^2 \rangle = 2 + TV_A + T\xi$ |
| $\text{SNR} = \frac{TV_A}{1+T\xi} = \frac{2T\langle n_t \rangle}{1+T\xi}$ | $\text{SNR} = \frac{TV_A}{2+T\xi} = \frac{T\langle n_t \rangle}{1+T\xi/2}$ |

Note that $V_A$ and $\xi$ are conserved in the two schemes, but the division of the signal in two in the double projection scheme doubles the shot noise, reducing the SNR.

In the next section some security proofs for the proposed scheme will be covered before continuing with the presentation of prepare and measure schemes.

## 2.4 Some relevant security proofs

The possible security proofs are very diverse and here we will only sketch the most relevant and straightforward given the previous model. Security proofs against general attacks and comprising finite size effects are in practice the most challenging to obtain. We will describe the principles of asymptotic security proofs against collective attacks for the described entanglement model.

### 2.4.1 Security proof against collective attacks for Gaussian modulation

A Gaussian modulation can be described as the 2-dimensional normal probability distribution over the phase space points $(x_I, x_Q)$ with zero mean and variance $\sigma^2$:

$$f(x_I, x_Q) = \frac{1}{2\pi\sigma^2} \exp\left[-\frac{x_I^2 + x_Q^2}{2\sigma^2}\right] \tag{2.12}$$

When the states modulated by Alice follow a Gaussian distribution it can be proven [81, 82] in the asymptotic limit that the resulting key rate is

$$K_{\text{coll}}^{\text{asympt}} = I(a:b) - S(b:E) \tag{2.13}$$

where $I(a:b)$ is the mutual information between Alice and Bob after correcting the errors in the received values, and $S(b:E)$ is the Holevo bound between Bob's string and Eve's quantum state that we have calculated before.

Eve's state can be written as $\rho_E = \text{tr}_{AB}(\rho_{ABE})$ which implies that $\rho_{ABE}$ is pure, and after measurement by Bob $\rho_{AE}$ is still pure. Using the properties of Von Neumann entropy we can write

$$S(AB) = S(E)$$
$$S(A|b) = S(E|b)$$

which lead to

$$\begin{aligned} S(b:E) &= S(E) - S(E|b) \\ &= S(AB) - S(AB|b) \end{aligned} \tag{2.14}$$

We can prove that $f : \rho_{AB} \to f(\rho_{AB}) = S(b:E)$ satisfies the property of extremality of Gaussian states (see appendix B) and $f(\rho_{AB}) \leq f\left(\rho_{AB}^G\right)$, i.e. we can compute $S(b:E)$ assuming that the state $\rho_{AB}$ is Gaussian obtaining a general bound on $S(b:E)$ and the SKR satisfies

$$K_{\text{coll}}^{\text{asympt}} \geq I(a:b) - f\left(\rho_{AB}^G\right) \tag{2.15}$$

This shows that 2.13 is a lower bound for the SKR using Gaussian modulation. In order to compute the length of the key after the transmission of $N$ states we need to:

- Calculate $I(a:b)$. It can be done directly after error correction or before error correction having an estimation of the efficiency of the communication $\beta$ (see appendix C).
- Calculate the Holevo bound using matrices $\Gamma_{AB}$ and $\Gamma_{AB|b}$ taking into account that for Gaussian modulation $Z = \sqrt{V^2 - 1}$.

We know from appendix B that $\Gamma_{AB}$ and $\Gamma_{AB|b}$ are characterized by their symplectic spectra $\{\nu_i\}_{i=1}^3$ (see appendix B for calculations) and the Holevo bound can be obtained directly from those eigenvalues and the function $g(x)$

$$g(x) = (x+1)\log_2(x+1) - x\log_2 x \tag{2.16}$$

resulting in

$$S(b;E) = g\left(\frac{\nu_1 - 1}{2}\right) + g\left(\frac{\nu_2 - 1}{2}\right) - g\left(\frac{\nu_3 - 1}{2}\right) \tag{2.17}$$

The SKR for collective attacks converges to the SKR for coherent attacks in the asymptotic case [83]. In the finite size regime similar conclusions can be obtained [84]. We will consider only the case of collective attacks in the following.

### 2.4.2 Security proof against collective attacks under linear channel for QPSK modulation

Quadrature phase-shift keying (QPSK or 4-QAM) is a very common modulation format in classical communications characterized by four points of equal modulus separated by phase factors of $\pi/2$. The four possible coherent states $\{|\alpha_k\rangle\}_{k=0\ldots3}$ can be described as

$$|\alpha_k\rangle := \left|i^k\alpha\right\rangle = e^{-\alpha^2/2}\sum_{n\geq 0}\frac{\alpha^n}{\sqrt{n!}}e^{ikn(\pi/2)}|n\rangle \tag{2.18}$$

QPSK modulations do not share the properties of Gaussian distributions, but equation 2.13 still holds for QPSK modulations if the channel is assumed to be linear [85]. In this case, for low values of $V_A$

$$Z = 2\alpha^2 \sum_{k=0}^{3} \frac{\lambda_{k-1}^{3/2}}{\lambda_k^{1/2}} \tag{2.19}$$

where

$$\begin{cases} \lambda_{0,2} = \frac{1}{2} e^{-\alpha^2} \left(\cosh\left(\alpha^2\right) \pm \cos\left(\alpha^2\right)\right) \\ \lambda_{1,3} = \frac{1}{2} e^{-\alpha^2} \left(\sinh\left(\alpha^2\right) \pm \sin\left(\alpha^2\right)\right) \end{cases} \tag{2.20}$$

This security proof has the advantage of simplicity, but the constraint of been limited to linear channels. More advanced proofs have been proposed recently without this constraint [86–88] but use more sophisticated techniques like semi-definite programming (SDP). In general QPSK will require lower levels of $V_A$ to operate with respect to a Gaussian modulation and will be more sensitive to the excess noise.

## 2.5 CV-QKD: Prepare and measure

The previous schemes could be implemented with two-mode squeezed states, but the generation and distribution of those states is experimentally impractical. Fortunately there is a perfect equivalence between the previously illustrated EPR version and a version of the scheme in which Alice encodes the information in the phase space quadratures of the coherent states[72, 89]. This simplifies the generation of the states, since they can be provided by a coherent source (a laser) and a modulator, two much more accessible devices than the EPR sources.

### 2.5.1 A CV-QKD protocol: GG02

The most widespread protocol for CV-QKD is known as GG02 and was proposed in 2002 by Frédéric Grosshans and Philippe Grangier [72, 73] and it has most of the protocol characteristics described previously. It was proposed initially for coherent state sources and Gaussian modulation with 180° hybrids and $\omega_{IF} = 0$, but it can be easily extended to other configurations. The main steps are:

1. Alice draws $N$ 2-dimensional samples from a random distribution $\mathcal{D}$ and uses them to modulate a coherent source obtaining the $N$ coherent states $|q_1 + ip_1\rangle, \cdots, |q_n + ip_N\rangle$, that are sent through an insecure quantum channel of transmittance $T$ and excess noise $\xi$. For a desired $V_A$ of operation, the average number of transmitted photons $\langle n_t\rangle$ should satisfy the relation $V_A = 2\langle n_t\rangle$.
2. Bob performs the measurement of the received states, after which Alice and Bob share $N$ pairs of correlated variables.
    a) If Bob has a suitable detector he can measure simultaneously the two quadratures.

   b) With a single quadrature detector, Bob is required to measure randomly one of the two quadratures, for which a phase modulator is generally needed. Bob also needs to communicate the bases to Alice after the measurement phase so that she can take them into account when calculating the correlation with Bob (sifting).

3. Alice and Bob reveal the data $(x_{i_1}, y_{i_1}), \cdots, (x_{i_m}, y_{i_m})$ of $m$ randomly chosen indices $\{i_1, \cdots, i_m\} \in \{1, \cdots, N\}$. With these parameters they will perform the parameter estimation. The security bounds can be calculated for estimated parameters to obtain the length $\ell$ of the final key.
4. Alice and Bob need to correct the errors on the $n = N - m$ remaining values they share. In practice they use the shared values to establish a common bit string $U$ with the help of classical error correcting codes.
   - Direct reconciliation is the method using the values of Alice as reference for the error correction, where she performs the coding and Bob the decoding (much harder task). The security of this method cannot be extended beyond 3 dB losses, so it is rarely used in practice.
   - A more useful method is reverse reconciliation, where the values of Bob are used as basis for the error correction. In this case it is Alice the one performing the computationally demanding task of decoding and there is no theoretical limit to the attenuation apart from the efficiency of the error correcting code.
5. After reconciliation Alice and Bob share two identical strings $U$ that are not completely secret. With $U$ and the length of the key $\ell$ it is possible to implement a process of privacy amplification using 2-universal hashing. This process is common to all QKD protocols and when applied in both entities, Alice and Bob obtain two identical copies of the secret key of size $\ell$.

The security of the protocol requires that entropy used for the generation of the samples is completely random (e.g. from a quantum random number generator, QRNG). A good calibration of the different parameters is also important and its imperfections will be discussed in the next section.

## 2.6 Introduction of imperfections

As mentioned earlier, in many occasions it is possible to accommodate the security proofs to different physical models of the set up. In these models it is possible to include imperfections on different parts [90] such as modulation, detection, laser noise... We will focus on two imperfections relevant to most CV-QKD experiments: the study of lossy noisy detectors and the effects arising from the fact that the parameters are estimated using a finite number of values.

### 2.6.1 Noisy and inefficient detector

The model we used to introduce the subject in section 2.3 is particularly simple, since it assumes that the only noise present is the fundamental quantum noise and that all the photons arriving to the input of Bob are measured by the detectors. In practice the detectors have losses and not all the photons are detected. Also, the readout electronics are subject to the effects of thermal noise, which produces additional independent electronic noise that adds to the fundamental noise.

Assuming that the different sources of noise at Bob's can be calibrated, it is possible to modify the entanglement version of the protocol adapting the model in the following way:

- The losses between Bob's input and the output of the photodiodes can be modelled as a beam splitter of transmittance $\eta$. The signal arriving from the channel is introduced in one of the inputs of the beam splitter, and vacuum in the other, assuming that the detector is trusted.
- The electronic noise is assumed to be accessible only to Bob and can be modelled as an additional EPR source of variance $v$ that is introduced in the second input of the beam splitter. The value of $v$ will be different depending on the type of detection.

With these modifications the entanglement version of the protocol is illustrated in figure 2.5. This model is especially important in actual implementations, where the electronic noise can be a considerable fraction of the fundamental noise. It also improves the estimation of $T$, since now the transmittance is divided into a trusted part $\eta$ and an untrusted part $T$. The assumptions are in general considered realistic, since Eve would need to entangle herself with the EPR source causing the electronic noise, which is inside Bob who we assume entirely trusted. The efficiency $\eta$ should be fairly constant during normal operation. The improvements in terms of key rate are substantial and this is typically called the realistic or trusted detector scenario, in contrast to the model in section 2.3 which might be too paranoid in some cases[*] and receives the name of untrusted scenario, since all the noise and losses are assumed under the control of Eve. The new relations with the values of the covariance matrix are provided in table 2.3.

| Single quadrature | Double quadrature |
|---|---|
| $\left\langle x^2 \right\rangle = V_A$ | $\left\langle x^2 \right\rangle = V_A$ |
| $\langle xy \rangle^2 = \eta T V_A$ | $\langle xy \rangle^2 = \eta T V_A$ |
| $\left\langle y^2 \right\rangle = 1 + V_{\mathrm{el}} + \eta T V_A + \eta T \xi$ | $\left\langle y^2 \right\rangle = 2 + 2V_{\mathrm{el}} + \eta T V_A + \eta T \xi$ |
| $\mathrm{SNR} = \frac{\eta T V_A}{1+V_{\mathrm{el}}+\eta T \xi} = \frac{2\eta T \langle n_t \rangle}{1+V_{\mathrm{el}}+\eta T \xi}$ | $\mathrm{SNR} = \frac{\eta T V_A}{2+2V_{\mathrm{el}}+\eta T \xi} = \frac{\eta T \langle n_t \rangle}{1+V_{\mathrm{el}}+\eta T \xi /2}$ |

**Table 2.3:** Relations between elements in the covariance matrix and measured values for trusted detector scenario. Variances are considered normalized to $N_0$ and $N_0 = 1$ SNU.

[*] For weak values of $V_{\mathrm{el}}$ the resulting SKR of the realistic model with electronic noise $V_{\mathrm{el}}$ is comparable to the SKR using the paranoid model without considering $V_{\mathrm{el}}$, so it can be used as a quick reference for the realistic model.

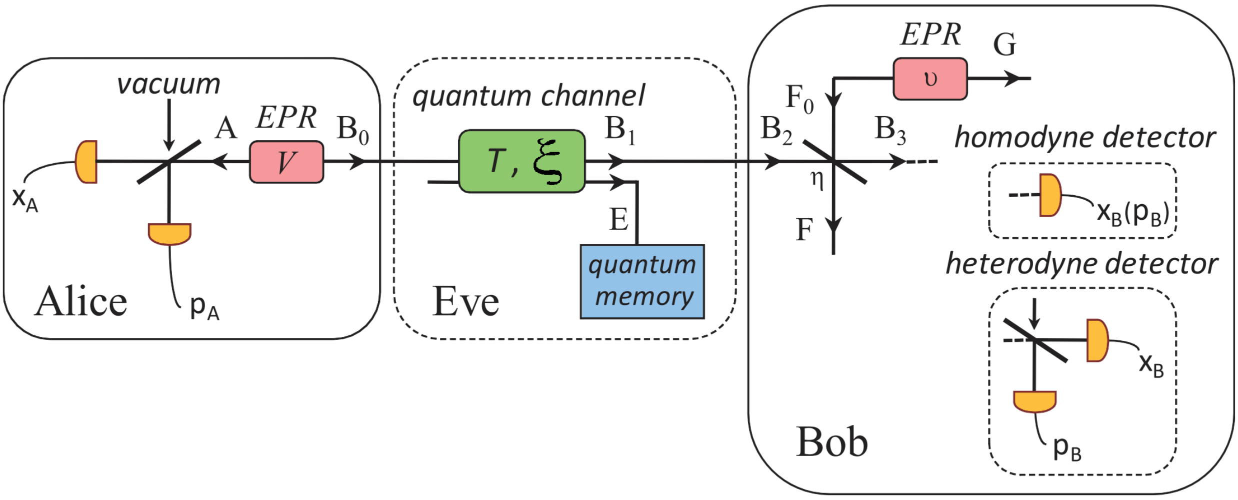


**Figure 2.5:** Entanglement version of the protocol including detector imperfections. Single (homodyne) and double (heterodyne) projections are considered. Each yellow block comprises a coherent detector as in figure 2.3.

### Calculating the security bounds in the realistic case

The bounds for the SKR can be calculated using the same procedure as in section 2.3, the state $\rho_{AB}$ being described by the same matrix $\Gamma$, but the two-mode state shared between Alice and Bob will interact with the state from the EPR source generating the electronic noise via the beam splitter of efficiency $\eta$. This will produce a state $\rho_{\mathrm{AB_3FG}}$ described by a $8 \times 8$ covariance matrix $\gamma_{\mathrm{AB_3FG}}$ that we will rearrange to obtain $\gamma_{\mathrm{AFGB_3}}$ and the state after measurement by Bob described by the $6 \times 6$ covariance matrix $\gamma_{\mathrm{AFG|b}}$ will be used to calculate the Holevo bound. The notation is as in figure 2.5 and the procedure is as follows:

The EPR state of variance $v$ is described by the covariance matrix

$$\gamma_{\mathrm{F_0G}} = \begin{bmatrix} v \cdot \mathbb{1}_2 & \sqrt{(v^2-1)} \cdot \sigma_z \\ \sqrt{(v^2-1)} \cdot \sigma_z & v \cdot \mathbb{1}_2 \end{bmatrix} \tag{2.21}$$

The state is independent with respect to the state $\rho_{AB}$ at the other input of the beam splitter, so the state at that point can be described as $\gamma_{\mathrm{AB_1}} \oplus \gamma_{\mathrm{F_0G}}$. The beam splitter transformation between two modes can be described as

$$Y^{\mathrm{BS}}_{\mathrm{B_2F_0}} = \begin{bmatrix} \sqrt{\eta} \cdot \mathbb{1}_2 & \sqrt{1-\eta} \cdot \mathbb{1}_2 \\ -\sqrt{1-\eta} \cdot \mathbb{1}_2 & \sqrt{\eta} \cdot \mathbb{1}_2 \end{bmatrix} \tag{2.22}$$

but extending it to accommodate $A$ and $G$ gives the symplectic transformation $Y^{\mathrm{BS}} = \mathbb{1}_{\mathrm{A}} \oplus Y^{\mathrm{BS}}_{\mathrm{B_2F_0}} \oplus \mathbb{1}_{\mathrm{G}} = \mathbb{1}_2 \oplus Y^{\mathrm{BS}}_{\mathrm{B_2F_0}} \oplus \mathbb{1}_2$ that acts on $\gamma_{\mathrm{AB_1}} \oplus \gamma_{\mathrm{F_0G}}$ to give

$$\gamma_{\mathrm{AB_3FG}} = \left(Y^{\mathrm{BS}}\right)^T \left[\gamma_{\mathrm{AB_1}} \oplus \gamma_{\mathrm{F_0G}}\right] Y^{\mathrm{BS}} \tag{2.23}$$

and can be rearranged to obtain the desired configuration

$$\gamma_{\mathrm{AFGB_3}} = \begin{bmatrix} \gamma_{\mathrm{AFG}} & \sigma^T_{\mathrm{AFGB_3}} \\ \sigma_{\mathrm{AFGB_3}} & \gamma_{\mathrm{B_3}} \end{bmatrix} \tag{2.24}$$

The matrix $\gamma_{\mathrm{AFG}}$ can be extracted in order to calculate the resulting covariance matrix after measurement $\gamma_{AFG|b}$ and its three symplectic eigenvalues $\{\nu_3, \nu_4, \nu_5\}$ can be calculated[15] (see appendix B.1.1). Along with the two eigenvalues already calculated for $\Gamma$ $\{\nu_1, \nu_2\}$, the Holevo bound is calculated as

$$S(b:E) = g\left(\frac{\nu_1 - 1}{2}\right) + g\left(\frac{\nu_2 - 1}{2}\right) - g\left(\frac{\nu_3 - 1}{2}\right) - g\left(\frac{\nu_4 - 1}{2}\right) \tag{2.25}$$

### 2.6.2 Finite size effects on the parameter estimation

The relations of covariance matrices parameters with the measured values of table 2.2 can be updated to those of table 2.3. Note that the imperfect scenario is based on the trust in the estimations done for $\eta$ and $V_{\mathrm{el}}$ (reason why sometimes it is called trusted detector scenario). If these parameters are assumed stable they can be measured off-line with arbitrary precision, but for the other parameters we will only have a fraction $m/N$ of symbols to perform the parameter estimation and the precision in the estimation will be limited by those parameters.

The uncertainty in the parameter estimation is only a small part of the denominated finite size effects, which arise from the fact of working with keys of finite size. In general the effects will tend to disappear as the lengths of the keys grow larger, but in general they need to be taken into account. We will use the same technique employed in [76] that relies in a linear channel hypothesis, which is not fully general:

$$y = tx + z \tag{2.26}$$

with $t = \sqrt{\eta T}$ and variances

$$\sigma_z^2 = \sigma_0 + \eta T \xi \tag{2.27}$$

$$\sigma_B^2 = \eta T V_A + \sigma_z^2 \tag{2.28}$$

Where $\sigma_0$ is the noise measured without signal, i.e. electronic and shot noise (for 1 projection $\sigma_0 = N_0(1 + V_{\mathrm{el}})$, for two projections $\sigma_0 = 2N_0(1 + V_{\mathrm{el}})$). We can use maximum likelihood estimators for the linear models

[15] 15: The last eigenvalue is always one, so it does not influence the Holevo bound as $g(0) = 0$.

[91] using $N$ symbols for the estimation during protocol execution and $N'$ for the off-line estimations ($N' > N$):

$$\begin{aligned}\hat{t} &= \frac{\sum_{i=1}^{N} x_i y_i}{\sum_{i=1}^{N} x_i^2} \\ \hat{\sigma}_z^2 &= \frac{1}{N}\sum_{i=1}^{N}(y_i - \hat{t}x_i)^2 \\ \hat{\sigma}_0^2 &= \frac{1}{N'}\sum_{i=1}^{N'} y_0^2 \\ \hat{V}_A &= \frac{1}{N}\sum_{i=1}^{N} x_i^2\end{aligned} \tag{2.29}$$

The previous estimators are independent and their distributions are characterized by:

$$\begin{aligned}&\hat{t} \sim \mathcal{N}\left(t, \frac{\sigma_z^2}{\sum_{i=1}^{N} x_i^2}\right) \\ &\frac{N\hat{\sigma}_z^2}{\sigma^2}, \frac{N'\hat{\sigma}_0^2}{\sigma_0^2}, \frac{N\hat{V}_A}{V_A} \sim \chi^2(m-1)\end{aligned} \tag{2.30}$$

And we can find confidence values for those parameters:

$$\Delta T = z_{\epsilon_{\mathrm{PE}}/2}\sqrt{\frac{\hat{\sigma}_z^2}{NV_A}} \tag{2.31}$$

$$\Delta\sigma_z^2 = z_{\epsilon_{\mathrm{PE}}/2}\frac{\hat{\sigma}^2\sqrt{2}}{\sqrt{N}} \tag{2.32}$$

$$\Delta\sigma_0^2 = z_{\epsilon_{\mathrm{PE}}/2}\frac{\hat{\sigma_0}^2\sqrt{2}}{\sqrt{N'}} \tag{2.33}$$

$$\Delta V_A = z_{\epsilon_{\mathrm{PE}}/2}\frac{\hat{V}_A\sqrt{2}}{\sqrt{N}} \tag{2.34}$$

A typical confidence value is $\epsilon_{\mathrm{PE}} = 10^{-10}$ and $z_{\epsilon_{\mathrm{PE}}/2}$ is such that $1 - \mathrm{erf}\left(z_{\epsilon\mathrm{PE}/2}/\sqrt{2}\right)/2 = \epsilon_{\mathrm{PE}}/2$. $\mathrm{erf}(x)$ can be calculated as

$$\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2}dt \tag{2.35}$$

The excess noise can be extrapolated from $\xi = \frac{\sigma^2 - \sigma_0^2}{\hat{t}^2}$, so the estimation of the parameters that are estimated during the execution of the protocol can be adapted as

$$\hat{V}_{A,\mathrm{FSE}} = \hat{V}_A - z_{\epsilon_{\mathrm{PE}}/2}\frac{\hat{V}_A\sqrt{2}}{\sqrt{N}} \tag{2.36}$$

$$\hat{T}_{\mathrm{FSE}} = \hat{T} - z_{\epsilon_{\mathrm{PE}}/2}\sqrt{\frac{\hat{\sigma}_z^2}{NV_A}} \tag{2.37}$$

$$\hat{\xi}_{\mathrm{FSE}} = \frac{\sigma_z^2 + \Delta\sigma_z^2 - \sigma_0^2 - \Delta\sigma_0^2}{\eta\hat{T}_{\mathrm{FSE}}} \tag{2.38}$$

The estimated values resulting of this procedure are always more pessimistic than the initial estimations, but the finite size effects on the parameters will decrease as the number of symbols used in the estimation increases.

## 2.7 Motivations of this thesis

After this brief introduction, CV-QKD appears to be a very interesting technology, but many challenges need to be overcome before it becomes a user friendly and commercially viable technology. Each of the three following sections of this thesis will focus on improving a particular aspect of CV-QKD:

Section 2 Optimize the bandwidth efficiency. CV-QKD shares many aspects with classical optical coherent communications, but for the moment most of the implementations have not used all the available resource tool kit. We will show the principles of classical communications (chapter 3) and how they can be used in CV-QKD, with an *ad hoc* proof-of-principle in chapter 4 and in a development platform for high rate commercial systems in chapter 5.

Section 3 Improve the integrability. CV-QKD systems have the potential of been more cost effective than their DV counterpart since the devices are easily implementable. One possibility is to integrate them in photonic integrated circuits (PIC) that can perform the same tasks as the bulk components at a fraction of the cost and size. We study the performance of different devices developed for CV-QKD.

Section 4 Increase the achievable distances. One of the main challenges in CV-QKD is the tolerance to losses, which is especially critical in fibre deployments since the losses grow exponentially with the distance. In free space channels the signal losses are quadratic with the distance, but they can suffer from fading. We study them as a possibility to extend the communication range and in particular the use of satellites in order to potentially achieve intercontinental distances with CV-QKD.

# Bandwidth efficient CV-QKD

# Coherent communications | 3

This section will study the current optical coherent communication systems focusing on the classical objective of information theory, i.e. maximize the mutual information between transmitter and receiver (see appendix C). The field of classical communication is broad and many standard books [92, 93] and articles [74] are available. In this chapter only basic techniques to operate in a fibre medium will be presented.

3.1 Introduction . . . . . . . . . . 37
3.2 Principles of coherent communications . . . . . . . . . . . . . . 38
Channel coding . . . . . . . 38
Modulation formats . . . . . 39
Typical operation mode . . 43
3.3 General scheme . . . . . . . 44
3.4 Channel model . . . . . . . . 45
Fluctuating transmittance . 48
3.5 Digital signal processing (DSP) . . . . . . . . . . . . . . . . 48
Sampling and time . . . . . 48
Pulse shaping: raised cosine 49
Adaptive filter . . . . . . . . 51
Frequency and phase recovery . . . . . . . . . . . . . . . . . 53
Synchronization . . . . . . . 54
DSP scheme . . . . . . . . . . 54
3.6 Coherent communications and CV-QKD . . . . . . . . . . . . . 55

## 3.1 Introduction

The concepts of information theory introduced in chapter 2 and in appendix C can be applied to both analogue and digital systems*. The easy access to high performance and low cost digital devices makes that nowadays communication industry relies almost completely on digital systems for the exchange of information.

Theoretical ideas of the mid 20th century for efficient communication schemes became a practical reality in the last decades due to the improvement of technology, but the demand for information grew at a very fast pace during the same time. The optical regime of electromagnetic waves can provide high information data rates, since the carrier (in the order of hundreds of THz) can be modulated and detected over bandwidths approaching the hundreds of GHz in some occasions.

Although it is possible to establish optical communications in free space as we will see in section 4, the most usual medium for optical communications is fibre. Optical fibres are flexible and thin threads of silica that are transparent to certain wavelengths in the near infrared part of the spectrum[17] and provide a guided medium to the light. Single mode fibres (SMF), which only allow the propagation of one spacial mode are the most common choice for communication applications, and wavelength multiplexing (WDM) is a common choice to aggregate more bandwidth using multiple wavelengths over the same medium.

[17]: The most interesting parts of the spectrum are the C-band around 1.5 $\mu$m where fibres induce the minimum attenuation (typically 0.2 dB/km) and the O-band around 1.3 $\mu$m where the dispersion due to the medium is minimal (attenuation is higher but for short distances it can be beneficial to reduce the dispersion).

The losses in the fibre will increase exponentially with the factor of attenuation per distance. Even if this factor is low, it can translate into 20 dB of loss after 100 km, which is detrimental for the communication. This is one of the main problems for the implementation of long distance QKD systems, but in classical communications it is possible to regenerate the signal using optical amplifiers, erbium-doped fibre amplifiers (EDFA) being the most extensively used. This allows the possibility of transferring high data rates over long distances. For this

* The approach in early CV-QKD systems was relatively close to an analogue system, since close to continuous Gaussian modulations were used, along with very long words for error correction.

reason classical optical communications are the dominant technology for the backbone of Internet, and as technology gets more accessible it also provides access to the final users.

The first attempts to use light for digital communications relied on the concept of intensity modulation and direct detection (IM-DD), where the receiver is a photodetector that can detect the intensity of the light that was modulated in intensity by the source (e.g.: a laser). This method does not exploit all the available bandwidth, but it is simple and robust, as it is not sensitive to phase and polarization misalignments. The symbols will correspond to positive real number values, so it is equivalent to having one degree of freedom. Modulation methods like on-off keying (OOK) or frequency shift keying (FSK) can be used to exploit those systems.

Coherent communications is the generic term used for systems that can recover the relative phase of the transmitted symbols. The symbols now belong to the realm of complex numbers and it is equivalent to having two degrees of freedom, potentially doubling the bandwidth with respect to IM-DD. As indicated in the previous chapter, in order to obtain a phase reference it is necessary to make an interferometric measurement between the signal arriving from the channel and a local oscillator operating in the receiver with a mode as close as possible to the one received. In order to achieve this it is necessary to establish phase-locked loops to maintain the relation between transmitter and receiver, but with the current processing power of digital electronics, it is more convenient to use digital signal processing techniques to achieve this purpose. The detection is performed with at least two balanced detectors.

In a similar way, another degree of freedom could be employed if we are capable of discerning two polarizations in the received signal. If so a double polarization modulator could be used at the transmitter and a double polarization interferometer (DP 90° hybrid) could be used before the detection with four balanced detectors. This scheme could potentially duplicate the data rate with respect to a single polarization scheme.

## 3.2 Principles of coherent communications

Adopting a very abstract point of view, we can separate the problem of transmitting a message from Alice to Bob into two steps: (1) preparing the message to tolerate the errors in the communication, and (2) adapting the message to the medium and the capabilities of transmitter and receiver. Alice and Bob should previously agree on the schemes to use in those two steps.

### 3.2.1 Channel coding

We know that the equivalent communication channel will be noisy, with error variance $\sigma_n^2$. If a fraction $\eta$ of the transmitted power $P_{\mathrm{tx}}$

arrives to the receiver we will have a signal-to-noise ratio

$$\mathrm{SNR}\,(\mathrm{dB}) = 10\log_{10}\left(\frac{\eta P_{\mathrm{tx}}}{\sigma_n^2}\right) \tag{3.1}$$

Shannon [1] tells us the maximum information that we can achieve if we assume that the channel only introduces additive white Gaussian noise (AWGN) and losses. The fact that it is not infinite means that we can have errors and the way to have a reliable communication without errors is to add redundancy to the message. If we assume that the original message is encoded in a logical string of bits, the way to add redundancy is to divide the original message into a sequence $\{m_i\}_{i=0}^{k-1}$ of size $k$ bits. A code will associate each possible string $\{m_i\}_{i=0}^{k-1}$ with a codeword $\{c_i\}_{i=0}^{n-1}$ of size $n$ bits adding $n-k$ redundancy bits to the information. Multiple sequences of codewords can be concatenated to complete the entire message. The codes will typically operate in a forward direction, that is without requiring acknowledgement from the receiver, hence the usual name forward error correcting (FEC) code.

An important property of the code is the *code rate*, which can be defined as the ratio of message bits over total bits of the codeword $k/n$, and it is always smaller than one. In principle we would like to have rates as close as possible to one, but this can go in detriment of the robustness of the code as it will start to fail with probability $\mathcal{P}_{\mathrm{ec}}$. That means that in general there will be a trade-off between $\mathcal{P}_{\mathrm{ec}}$ and the $k/n$.

Fortunately some families of very efficient codes that are also very robust have been developed over the years (low-density parity-check codes (LDPC), Turbo Codes, Raptor Codes...). They do it at the expense of working with longer codewords (high values of $k$ and $n$), which makes them computationally complex to implement, especially on the receiver side.

For a communication link it is desirable to use the FEC with highest rate that supports a given SNR with negligible $\mathcal{P}_{\mathrm{ec}}$. In practice the optimality in terms of rate depends on the SNR, so if the SNR changes it is advisable to change the code in order to work in the best conditions.

### 3.2.2 Modulation formats

Codewords are logical entities (e.g. bit strings) and they need to be adapted to the real communication channel. In digital communication schemes it is common to map a sequence of bits to a position in the phase space. The set of coordinates of this position is known mathematically as symbol and for practical reasons it can take a set of discrete values. The set of possible symbols of a modulation scheme constitute the constellation and typically constitute a power of two, providing the possibility of mapping an integer number of bits to each symbol deterministically[18] . A transmitter will convert the logical string $\{c_i\}_{i=0}^{n-1}$ of size $n$ into a sequence of $N$ physical symbols $\{x_i\}_{i=0}^{N-1}$, while the receiver will do the reverse mapping to convert the received

[18] Some examples of constellations are BPSK (1 bit/symbol), QPSK/4-QAM/4-PSK (2 bits/symbol), 8-PSK (3 bits/symbol), 16-QAM (4 bits/symbol), M-QAM (d bits/symbol with $M = 2^d$).

symbols $\{y_i\}_{i=0}^{N-1}$ into the logical string $\{\tilde{c}_i\}_{i=0}^{n-1}$, which might not be the same if errors occurred.

The idea behind using coordinates of phase space as symbols is to allow the receiver to associate the environment of those points to the decision about the symbol that has been transmitted. Even if the transmitter prepares the symbols correctly the measurements at the detector will be influenced by additive noise and other imperfections (an example for an AWGN with a high order constellation can be seen in figure 3.1). The possible criteria on the decision are diverse and are mostly derived from statistical techniques, but the most general problem consists in deciding the symbol that has been transmitted as a function of the symbol that has been received. In order to recover the transmitted symbols at the receiver the most common approach is to use a maximum likelihood estimation (MLE) or some related method.

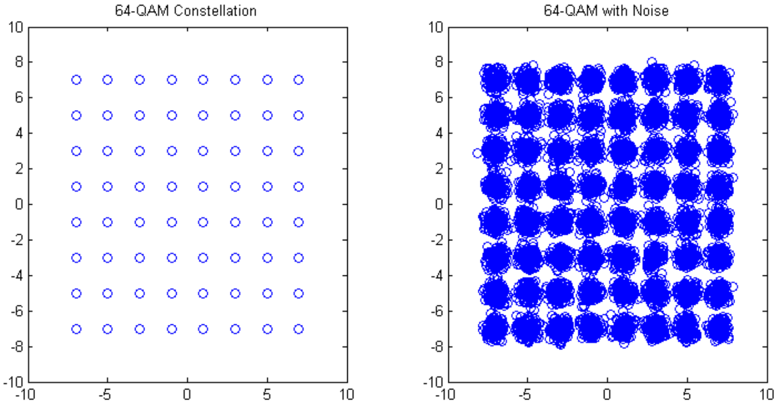


**Figure 3.1:** High order modulation constellation before and after an AWGN channel.

### Components at the transmitter

Optical modulators are devices capable of changing the amplitude, phase or polarization of the electromagnetic wave under certain control commands (see figure 3.2). They generally consist in a wave guide of a material that can change its refractive index as a function of the control signal. The control signals typically used are electromagnetic (electro-optic modulators) or mechanic (acousto-optic modulators). The lithium niobate $LiNbO_3$ electro-optic modulators are the most extended in the telecommunications market due to their fast response, allowing bandwidths in the order of GHz. The basic modulation scheme would comprise a modulation in one polarization of the phase and the amplitude. This can be done using a succession of amplitude and phase modulators or directly an IQ modulator. The relations between the values corresponding to the amplitude/phase and IQ schemes come directly from the Cartesian and polar representations of complex numbers. If $a(t)$ is the temporal modulation signal that we want to apply, we see that both methods are equivalent ($\angle a(t)$ denotes the angle of $a(t)$):

$$\begin{aligned} a(t) &= \mathrm{Re}\{a(t)\} + i\,\mathrm{Im}\{a(t)\} = a_I(t) + i\,a_Q(t) && (3.2)\\ &= |a(t)|e^{i\angle a(t)} && (3.3) \end{aligned}$$

When the modulation $a(t)$ is mixed with the carrier signal at frequency $f_c = c/\lambda_c$ the equivalent band pass signal $s(t)$ at the output of the modulator is expressed as

$$s(t) = \mathrm{Re}\{a(t)e^{i2\pi f_c t}\} \tag{3.4}$$

A typical scheme for the transmitter with an IQ modulator can be seen in the upper part of figure 3.3. The signal $a_I(t)$ and $a_Q(t)$ that act on the arms of the modulator come from digital to analogue converters (DAC) that act on the order of the digital signal processing (DSP) algorithms of the transmitter. These algorithms are of great importance for the operation of modern digital communication systems and will be covered in a latter chapter.

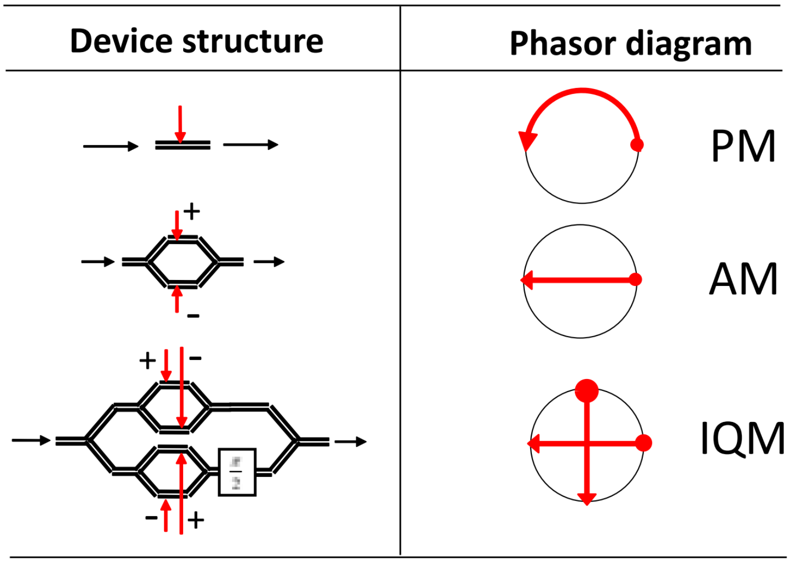
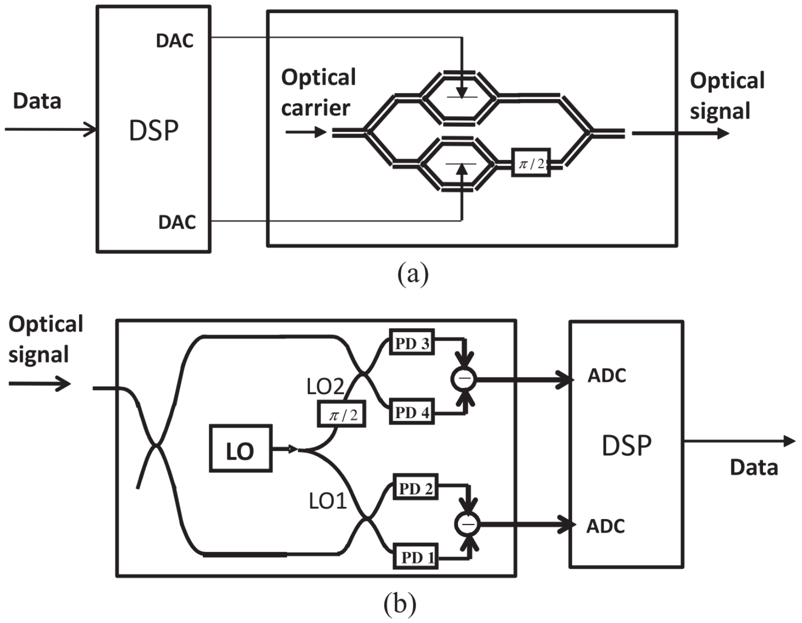


**Figure 3.2:** Devices for phase, amplitude and IQ modulation and their action in phase space. Image source: [74].

### Components at the receiver

In order to recover the signal $a(t)$ at the receiver side we also need to perform electro-optical operations over the signal $\tilde{s}(t)$, which is the signal $s(t)$ with the effects of the channel $\tilde{s}(t) = s(t) * h(t)$. The process can be followed in figure 3.3. The optical part consists in the interference of $\tilde{s}(t)$ with the local oscillator tone that will not be perfectly matched in frequency, phase and polarization. The interferometry can be performed with discrete components, but they are typically integrated in a 90° hybrid, as defined in the previous chapter. Only the AC part of the signal is of interest, so the outputs of the 90° are detected by pairs of photodiodes connected in a balanced configuration that subtracts the DC component[19] . Each balanced detector output will correspond to a

[19] In practice there will be some resilient part that is measured with the common mode rejection ratio (CMRR).


(a)

(b)

**Figure 3.3:** Coherent communication transmission and reception schemes. Image source: [74].

projection of the phase space and the signal will be typically amplified before the digitalization in an ADC. The receiver part of the DSP will treat the received values to recover the information.

The scheme uses one polarization to simplify the illustration, but it can be duplicated using beam splitters and a polarization rotator to work with two polarizations. Most commercially available systems work with two polarizations, especially at the receiver size, since it can recover rotations in polarization of a signal that has been modulated in one polarization. An alternative scheme would be to implement a polarization tracking that dynamically corrects the polarization rotation, but it tends to be more complex in classical systems.

There are very extended standards for the commercialization of integrated coherent receivers (ICR) that fulfil the typical requirements for classical coherent communications and allow interoperation. Some examples are OIF-DPC-RX-01.2 or OIF-DPC-MRX-01.0.

Transceivers, a combination of transmitter and receiver in the same device, are also widely extended in coherent communications, since the same laser can be used for transmission and as local oscillator.

### Probability constellation shaping (PCS)

If the original codeword has an equally probable distribution of bits, the corresponding symbols will be equally probable as well, and the distribution along the constellation will be homogeneous, as it can be seen in the left part of figure 3.4. Using more complex mathematical machinery it is possible to use a mapping that reshapes the constellation to have more probability in the center, like in the right part of the figure. The intention of this technique is to approach the capacity of the channel, since the distribution resembles more a bidimensional Gaussian distribution, which is the (continuous) distribution that more closely approaches the capacity bound. The mapping is done probabilistically hence the name probability constellation shaping (PCS) and can be applied to any high order constellation, like 64-QAM and above. Note that the separation of the points would be the same as before the shaping, only the probability distribution changes.

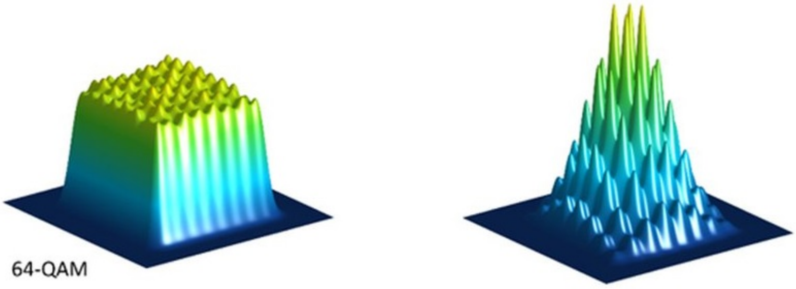


**Figure 3.4:** Distribution of symbols in phase space for a PCS-QAM modulation. Image courtesy of Nokia Bell Labs.

### 3.2.3 Typical operation mode

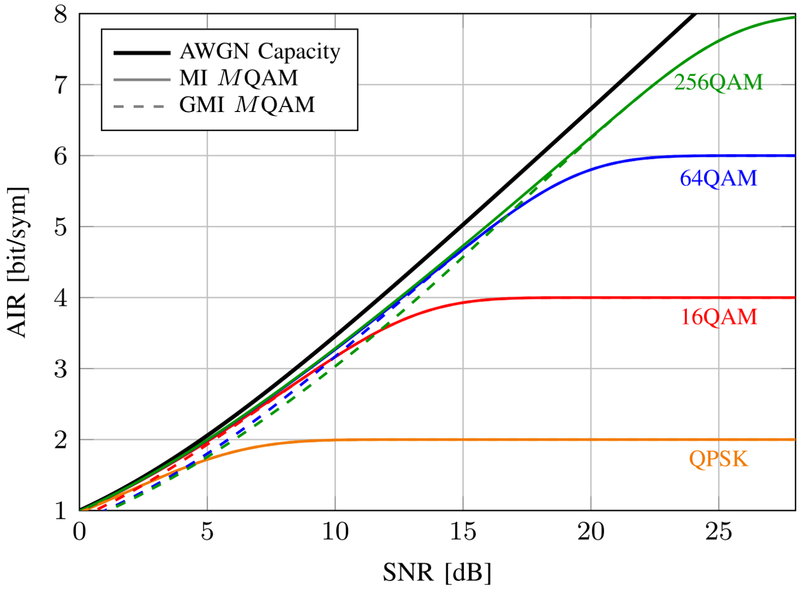


**Figure 3.5:** Achievable information rates (AIR) as a function of SNR. GMI stands for Generalized Mutual Information and is equivalent to AIR in systems using soft decision forward error correction (SD-FEC). Image source: [94].

The achievable information rate (AIR) is the optimal mutual information (MI) that we can obtain using a given combination of modulation format and FEC as a function of the SNR. The MI will be lower than the AIR, as it is also be affected if we use additional symbols to facilitate the communications (e.g.: synchronization symbols, phase reference symbols...). In figure 3.5 we can see the typical curves of AIR as a function of the SNR for commonly used discrete modulations and their comparison with the capacity of the channel (that could be achieved with a continuous Gaussian modulation and a code of infinite size). We remark that for discrete modulations the AIR saturates after certain SNR, meaning that for a channel with good SNR it should be convenient to use a higher density constellation to optimize the MI. There is also a gap between the capacity and the AIR that increases with the SNR that can be attributed to the quantization error and the efficiency of the codes.

The selected coding and modulation scheme will determine the achievable information rate (AIR) between Alice and Bob, as can be seen in figure 3.5. We can introduce the communication efficiency $\beta$, that will be function of the SNR $s$, as the ratio of AIR and channel capacity:

$$\beta(s) = \frac{\mathrm{AIR}(s)}{C(s)} \tag{3.5}$$

In order to optimize the communication rate this quantity should be as close as possible to one. Typically the SNR of the link is known and a good combination of modulation and code needs to be selected. For high SNR the sensible choice is to select a modulation whose AIR does not saturate at that SNR and then select a FEC that can work in that regime. For low SNR all the modulations approach to the channel capacity and it is interesting to work with the one with lowest density, as the algorithms to work with them are more robust and the main difficulty is to obtain a FEC that can work at low SNR[20] .

Channel coding and modulation are very related concepts, but they can be studied independently as there is a direct mapping between the symbols used in the modulation/demodulation system and the logical strings (of bits) used by the codes. The performance factor that both modules use to interact is the SNR which can be related to the correlation between the symbols of Alice and Bob $\{x_i, y_i\}$ at the modulation level, as well as to the bit error rate (BER) resulting from the code.

In the following we will assume that there is a provision of codes that can reliably work by a factor $\beta$ of the channel capacity at any reasonable SNR, and we will focus mainly on the symbol level.

## 3.3 General scheme

The complete scheme of a typical double polarization classical coherent communication system is illustrated in figure 3.6, separating the three integral parts: Alice (in red), the channel (in green) and Bob (in blue).

Alice is using a laser that generates a light beam at a fixed frequency $f_A = c/\lambda_A$. This beam is modulated by a double polarization IQ modulator driven by an analogue signal generated by four DACs (an amplifier is usually required between the DAC and modulator, but it is not shown in the figure). Each digital signal at the input of the DAC has been generated by the transmitting part of the DSP.

Bob is composed of an interferometric part, that mixes the received signal from the channel with the local oscillator at frequency $f_B = c/\lambda_B$ (we will assume that the mixed signal fits in the bandwidth of the detector without further conversions). The mixed signal is detected using pairs of balanced photodiodes whose output photocurrent is amplified with transimpedance amplifiers (TIA) before arriving to the

[20] In CV-QKD it is typical to work at low SNR, so the main element influencing $\beta$ is the error correcting code (see appendix C). The error correcting code in CV-QKD is used after the symbol exchange as part of the reconciliation. It can be based on Alice's symbols (direct reconciliation, DR) or more typically in Bob's (reverse reconciliation, RR). This is also true for any SNR if the modulation is Gaussian.

ADCs. The signal is processed by the DSP to maximize the mutual information between Alice and Bob.

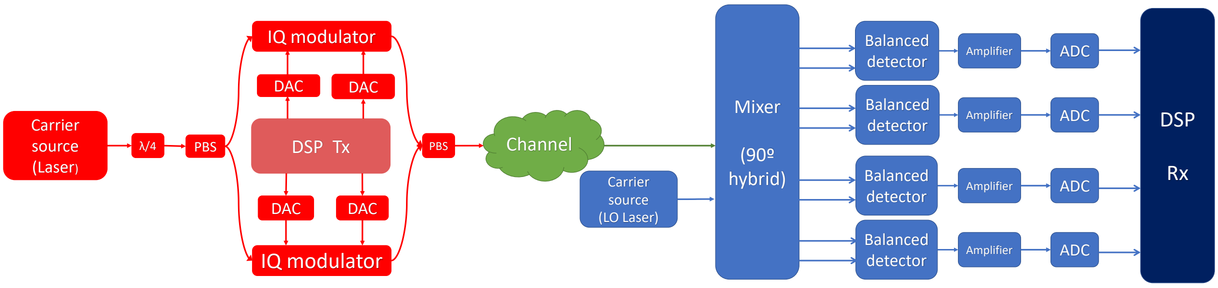


**Figure 3.6:** General scheme for a double polarization coherent communication system.

Note that with this scheme, for given hardware and channel, the performance of the system will depend crucially on the algorithms running on the DSP. Note also that the coding and the modulation can be treated independently, so the DSP characteristics will only depend on two factors:

- **The available hardware.** The DSP needs to know the characteristics of the equipment. Some examples are the linewidth and optical power of the lasers, the resolution, bandwidth and sampling rate of the DAC/ADC, the polarizations diversity in transmission/reception, the expected electronic noise...
- **The channel**. The channel will introduce loss and other undesirable effects on the received signal. Depending on its characteristics the DSP can be customized to operate under certain channel conditions.

Before studying the main characteristics of the DSP we will cover the more common effects on fiber channels.

## 3.4 Channel model

A coherent transmission between two entities Alice and Bob can be modelled under several assumptions and the characteristics of the DSP should be adapted to the expected model and conditions.

We assume that Alice modulates a nearly monochromatic pulse of light of wavelength $\lambda$ and linewidth $\Delta\nu$ using a double polarization IQ modulator (or equivalent system) of bandwidth $B$. The original polarization of the laser is linear, but at the output of the modulator the two orthogonal principal polarizations ($H$ and $V$) will carry information on the two projections ($I$ and $Q$), allowing three degrees of freedom (time, polarization and projection). We will treat the symbols as pairs of complex numbers and we will notate the $k$-th symbol transmitted by Alice by

$$\mathbf{x}_k = \begin{bmatrix} x_{H,k} \\ x_{V,k} \end{bmatrix} = \begin{bmatrix} x_{H,k,I} + jx_{H,k,Q} \\ x_{V,k,I} + jx_{V,k,Q} \end{bmatrix} \tag{3.6}$$

The discrete sequence $\{\mathbf{x}_k\}_N$ will be converted to a continuous signal $\mathbf{x}(t)$ and used to cause a modulation in Alice's laser that will be transmitted through the channel once it is appropriately attenuated. Bob will be equipped with an independent IQ intensity detector that can obtain two projections ($I$ and $Q$) per principal polarization ($H$ and $V$), i.e. four values that are noted by $\mathbf{y}_k$ in a way analogous to $\mathbf{x}_k$. If we can construct a baseband equivalent model consisting of a channel with temporal response $\mathbf{h}(t)$ and additive noise $\mathbf{z}(t)$ the signal $\mathbf{y}(t)$ received at Bob's will be the convolution of the original signal with the channel plus the additive noise:

$$\mathbf{y}(t) = \mathbf{x}(t) * \mathbf{h}(t) + \mathbf{z}(t) \tag{3.7}$$

Note that the previous expression relates to electronic signals and $\mathbf{h}(t)$ is the equivalent baseband channel seen in the electronic domain, although the real channel is optical. Classical coherent communication systems need to deal with certain challenges, mainly:

- Modern systems work in the digital domain, so the signal $y(t)$ needs to be: (1) sampled at a sampling rate $s_r R$; (2) quantized to $2^d$ values where $d$ is the resolution in bits.
- The clocks of Alice and Bob might not be synchronized, so the optimal sampling time needs to be estimated in order to obtain the samples at the most convenient time.
- In order to maximize the mutual information, the effects $\mathbf{h}(t)$ of the channel need to be inverted to a certain degree.

The first task is performed by the analog-to-digital converter (ADC), while the last two are performed by the digital signal processing routines at the reception (DSPrx). The performance of those two systems and the effects introduced in $\mathbf{h}(t)$ will determine the portion of information that will be recovered from the communication. In order to increase the performance of the system, two additional concepts are typically used:

- Some side information (references), known *a priori* by both entities can be transmitted by Alice so that Bob can estimate $\mathbf{h}(t)$ with certain degree of accuracy.
- The information transmitted by Alice can have some redundancy in order to be able to reconstruct the original message even if some parts were not correctly estimated without the need to retransmit the message. This is done with forward error correcting codes (FEC).

Clearly there is a compromise between the amount of side information and redundancy we transmit and the useful information rate, so efficient classical communications require a trade-off between these resources and the useful symbols as a function of the conditions of the channel.

### Constant amplitude non dispersive channel

The simplest realistic channel to consider is the one of constant transmission efficiency $\mathcal{T}^2$ and random instantaneous phase $\phi(t)$. The polarization axes might have rotated in the channel, so some information could have been interchanged at the receiver. With these assumptions and considering a delay $t_d$ between Alice and Bob (Bob is the reference for $t = 0$), the channel temporal response can be written as:

$$\mathbf{h}_a(t) = \left[\mathbf{R}(\theta(t))\right] \begin{bmatrix} \mathcal{T} e^{j\phi(t)} \\ \mathcal{T} e^{j\phi(t)} \end{bmatrix} \delta(t + t_d) \tag{3.8}$$

where $\theta(t)$ is the instantaneous angle discrepancy between Alice and Bob's polarization axes, and the matrix $\mathbf{R}(\theta(t))$ is given by:

$$\left[\mathbf{R}(\theta(t))\right] = \begin{bmatrix} cos(\theta(t)) & sin(\theta(t)) \\ -sin(\theta(t)) & cos(\theta(t)) \end{bmatrix} \tag{3.9}$$

This can be a good model for fixed length fiber or controlled free-space systems where the symbols do not interact between themselves, e.g.: a system transmitting separated optical pulses.

### Polarization dispersion

Imperfections in the fiber can cause the two polarizations to perceive different refractive indices, therefore they will travel at different speeds causing a differential group delay (DGD) between the two axes. This can be modelled by the following Jones matrix where $\Delta\tau$ is the delay in the communication path:

$$\left[\mathbf{J}(\theta(t), \Delta\tau)\right] = \begin{bmatrix} cos(\theta(t))e^{j\Delta\tau/2} & sin(\theta(t)) \\ -sin(\theta(t)) & cos(\theta(t))e^{-j\Delta\tau/2} \end{bmatrix} \tag{3.10}$$

The resulting equivalent channel is:

$$\mathbf{h}_b(t) = \left[\mathbf{J}(\theta(t), \Delta\tau)\right] \begin{bmatrix} \mathcal{T} e^{j\phi(t)} \\ \mathcal{T} e^{j\phi(t)} \end{bmatrix} \delta(t + t_d) \tag{3.11}$$

The compensation of the polarization dispersion is important in long communication channels. For short channels $\Delta\tau \longrightarrow 0$ and $\mathbf{J} \longrightarrow \mathbf{R}$.

**Temporal dispersion**

A typical effect in communications is the temporal dispersion of the energy of the symbols, the channel will not only contain a temporal coefficient at $\delta(t)$, but a more general response taking into account the the effects of the dispersion $\mathbf{h}_{\text{disp}}$:

$$\mathbf{h}_c(t) = \left[\mathbf{J}(\theta(t), \Delta\tau)\right] \mathbf{h}_{\text{disp}}(t) \tag{3.12}$$

The information of a symbol is spread in time, causing the interference with contiguous symbols in what is called inter-symbol interference (ISI). We can simplify $\mathbf{h}_{\text{disp}}(t)$ assuming that the maximum value of the transmittance occurs at $t = 0$ and it decreases for contiguous values, i.e.: $|h_{\text{disp},X}(0)| = |h_{\text{disp},Y}(0)| = \mathcal{T}$ and $|h_{\text{disp}}(t \neq 0)| < \mathcal{T}$

### 3.4.1 Fluctuating transmittance

In some channels the transmittance is not constant and $\mathcal{T} \rightarrow \mathcal{T}(t)$. This complicates the analysis, since $\mathcal{T}$ is a fundamental parameter for CV-QKD, and it will be treated in section 4 for the case of free-space channels.

## 3.5 Digital signal processing (DSP)

### 3.5.1 Sampling and time

The DSP will work mainly with two different kinds of values in the digital domain: symbols and samples. Symbols will be the more abstract entity of the two and the one we are going to use to perform the calculations related to information theory. The operations related to signal processing will be performed in samples due to the need of representing signals evolving in time. The sampling theory indicates that in order to correctly reproduce a temporal signal in the digital domain we need at least two samples per symbol.

Typically we want to establish a communication at a certain symbol rate $R$ common to Alice and Bob (usually given in Bauds, 1 Baud = 1 Bd = 1 symbol per second), that will be directly related with the bandwidth $B$ of the modulated signal. The DSP operations at Alice and Bob will be performed using $s_A$ and $s_B$ samples per symbol respectively, both not lower than two but not necessarily equal meaning that Alice and Bob can use different sample rates even at the same symbol rate[21] . Samples are related to the symbols by a series of digital transformations and will be more linked to the actual modulated or received values than the symbols.

Notice that if $B$ is the bandwidth of the optically modulated IQ signal, the bandwidth of the electronic signals I and Q will be $B/2$ and can be represented as in figure 3.7. It is important to remark that even if the

[21] It is typical to adapt the sampling rate of the DSP to the to the sampling rate of the DAC in Alice, and that of the ADC in Bob.

bandwidth of each of the electronic signals is half of the optical one, the sampling condition needs to be maintained.

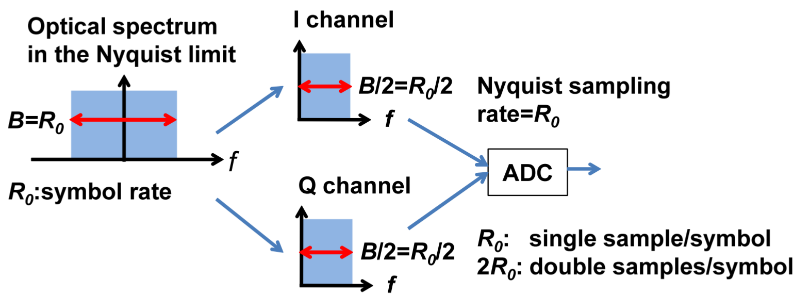

Optical spectrum in the Nyquist limit
$B$=$R_0$
f
$R_0$:symbol rate
I channel
$B/2$=$R_0/2$
f
Nyquist sampling rate=$R_0$
ADC
Q channel
$B/2$=$R_0/2$
f
$R_0$: single sample/symbol
$2R_0$: double samples/symbol

**Figure 3.7:** Bandwidth corresponding to the I and Q components of the signal [74].

One important factor when working with two separated entities with independent clocks is the frequency and phase synchronization between both clocks. The frequency offset in the clock can be estimated at the receiver using DSP techniques and corrected acting on the clock that triggers the ADC. We will assume that the deviation on the clocks is sufficiently accurate for the rates we are managing.

The sampling theorem states that it is possible to perfectly recover the original signal with only two samples per symbol at the receiver. For this it is required that the sampling time is optimal (the center of the transmitted symbol coinciding at one of the two samples), something that will not occur in general since the clock phase of Alice and Bob is not the same. Fortunately it is possible to insert a phase delay in the digital domain to adjust the clock phase of the receiver to the clock phase of the transmitter. The pulse shaping filter will help to correct the clock phase and the inter-symbol interference (ISI) discussed in the previous section.

### 3.5.2 Pulse shaping: raised cosine

Pulse shaping is the process of transforming the original symbols of the constellation into samples adapted to the channel. This is done passing the signal through a filter with certain properties. The most interesting property in most cases is the mitigation of the ISI without extending the original bandwidth.

It is practical to design the shaping filter in frequency trying to obtain a flat spectral response when transmitting a long sequence of symbols. The first choice could be the rectangular window, which has a sinc response in time with zeros in the multiples of the sampling period $T$, condition that satisfies the ISI constraint. The main inconvenience of this filter is that its temporal response is infinite and the initial lobes have considerable weight.

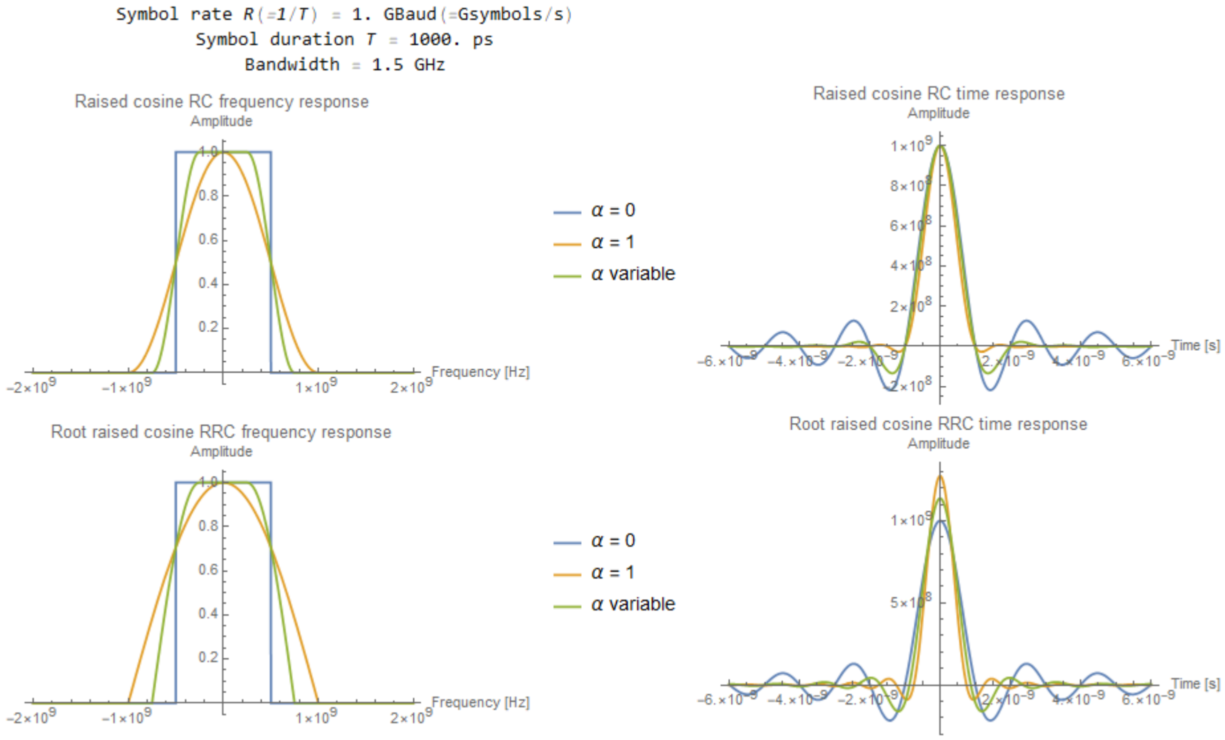
It is possible to modify slightly the *sinc* response to obtain a very flexible filter that is called raised cosine (RC) and has frequency response

$H_{\mathrm{RC}}(f)$ and impulse response $h_{\mathrm{RC}}(t)$:

$$H_{\mathrm{RC}}(f) = \begin{cases} 1, & |f| \leq \frac{1-\beta}{2T} \\ \frac{1}{2}\left[1 + \cos\left(\frac{\pi T}{\beta}\left[|f| - \frac{1-\beta}{2T}\right]\right)\right], & \frac{1-\beta}{2T} < |f| \leq \frac{1+\beta}{2T} \\ 0, & \text{otherwise} \end{cases} \tag{3.13}$$

$$h_{\mathrm{RC}}(t) = \begin{cases} \frac{\pi}{4T}\,\mathrm{sinc}\left(\frac{1}{2\beta}\right), & t = \pm\frac{T}{2\beta} \\ \frac{1}{T}\,\mathrm{sinc}\left(\frac{t}{T}\right)\frac{\cos\left(\frac{\pi\beta t}{T}\right)}{1-\left(\frac{2\beta t}{T}\right)^2}, & \text{otherwise} \end{cases} \tag{3.14}$$

where the term $\beta$ = ROF is the roll-off factor and it serves to adapt the excess of bandwidth with respect to the original signal. If the input signal has a symbol rate $R$, the output of the RC filter occupies a bandwidth $B = (1 + \mathrm{ROF}) \cdot R$. If ROF = 0 we have a sinc filter and we maintain the bandwidth, but in practice it is more convenient to use a slightly higher ROF to increase the performance at the cost of some bandwidth. At ROF = 1 we would double the bandwidth but the temporal response would be very narrow. In the upper part of figure 3.8 we can see representations of the raised cosine filter in time and frequency for different values of ROF. Note that the values at the multiples of $T$ are zero.



```
Symbol rate R(=1/T) = 1. GBaud(=Gsymbols/s)
        Symbol duration T = 1000. ps
             Bandwidth = 1.5 GHz
```

**Figure 3.8:** Raised cosine and root raised cosine time and frequency representations.

Without other effect apart from the ISI it would be sufficient to apply the RC filter at the transmitter, but as we discussed earlier we will have a clock phase mismatch between Alice and Bob, meaning that we will not necessarily sample at the correct times at Bob's side. One way to solve this problem is to use some method to estimate the phase and apply a delay digitally at the receiver. A more complete approach consists in using an adaptive filter that solves the clock phase mismatch and other problems from the channel. This filter will be discussed in the next section, but one of its functions will be to complete the pulse shaping, meaning that it is practical to divide the pulse shaping between Alice and Bob.

Applying a RC in both entities would no longer sustain the anti-ISI property that we want, but $H_{\mathrm{RRC}}(f) = \sqrt{H_{\mathrm{RC}}(f)}$ would do. This filter is called root raised cosine (RRC) and its impulse response reads:

$$h_{\mathrm{RRC}}(t) = \begin{cases} \frac{1}{T_s}\left(1+\beta\left(\frac{4}{\pi}-1\right)\right), & t=0 \\ \frac{\beta}{T_s\sqrt{2}}\left[\left(1+\frac{2}{\pi}\right)\sin\left(\frac{\pi}{4\beta}\right)+\left(1-\frac{2}{\pi}\right)\cos\left(\frac{\pi}{4\beta}\right)\right], & t=\pm\frac{T_s}{4\beta} \\ \frac{1}{T_s}\frac{\sin\left[\pi\frac{t}{T_s}(1-\beta)\right]+4\beta\frac{t}{T_s}\cos\left[\pi\frac{t}{T_s}(1+\beta)\right]}{\pi\frac{t}{T_s}\left[1-\left(4\beta\frac{t}{T_s}\right)^2\right]}, & \text{otherwise} \end{cases} \tag{3.15}$$

After this separation of one RC into two RRC the process is the following:

- Alice does the pulse shaping with $h_{\mathrm{RRC}}[n]$ (the digital version of $h_{\mathrm{RRC}}(t)$ with a finite number of taps $N_A$ but sufficient to approximate the desired response).
- Bob initializes its adaptive filter with $h_{\mathrm{RRC}}[n]$, a filter of $N_B$ taps.

Note that the pulse shaping with RRC does not satisfy the ISI criterion, as can be seen in figure 3.8. It is only the combination of the pulse shaping at Alice and Bob that accomplishes the effect. In figure 3.9 we can see the effect of pulse shaping in a sequence of symbols represented in IQ. The information at each temporal point now depends on the contiguous symbols (the lower the ROF the higher the influence) and the discrete regular distribution of the symbols in the constellation is not so clear in the samples that are sent to the DAC.

### 3.5.3 Adaptive filter

When Bob receives a signal transmitted over a generic channel the phase and the polarization at the receiver will not be aligned to the ones transmitted. Also, the optimal sampling clock phase is not known by Bob's ADC. The purpose of the adaptive filter is to correct at least the clock phase recovery and the polarization recovery (in some occasions also the signal phase). This task is quite ambitious and typically the adaptive filter is the most complex element of the DSP.

In order to simplify the problem we will assume that we know some characteristic of the signal. For example we might know that the transmitted signal has constant modulus, or we might know the transmitted value for certain symbols (pilots). If we have this kind of knowledge

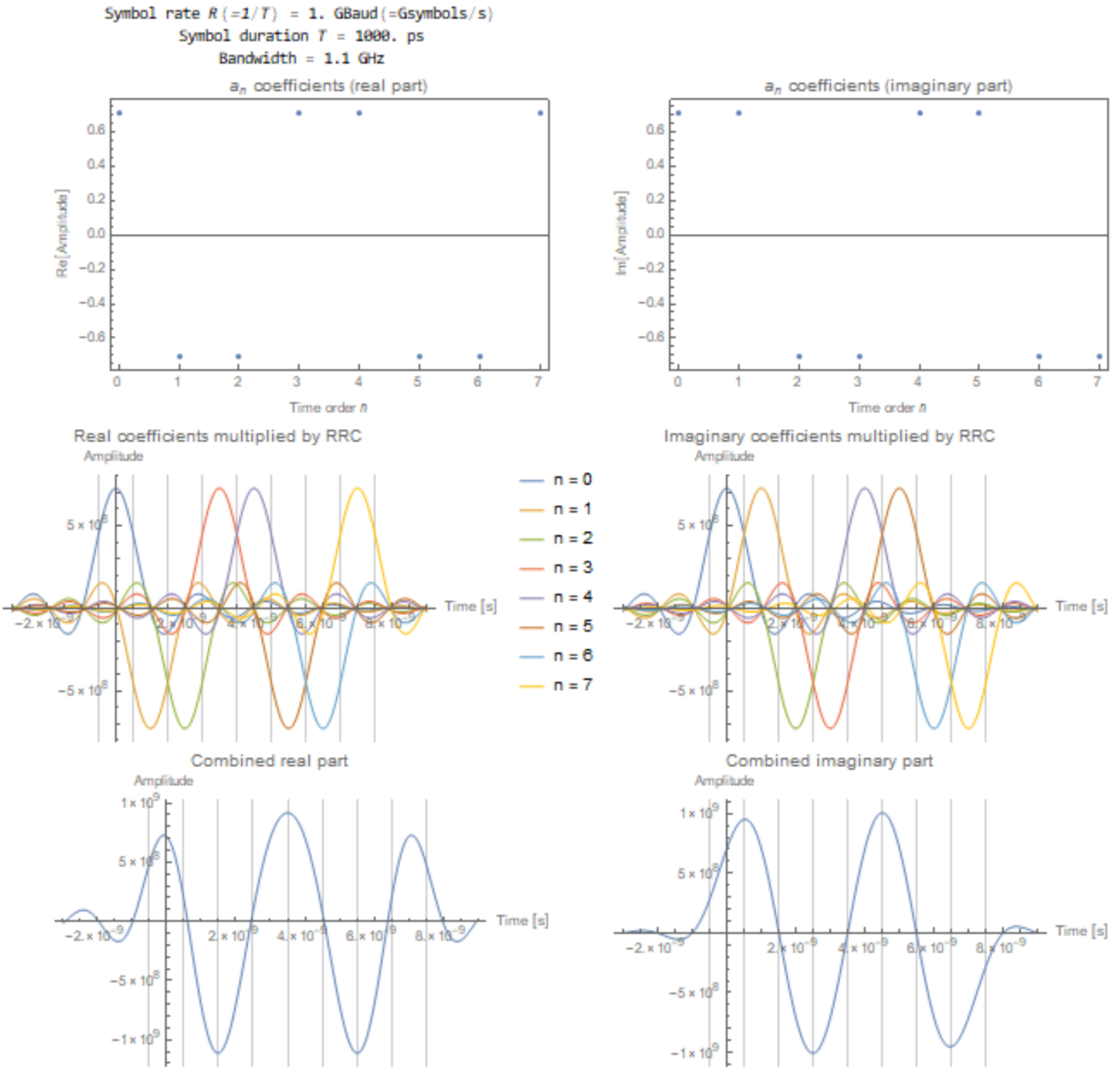


**Figure 3.9:** QPSK sequence after pulse shaping with RRC filter (ROF=0.1).

we can establish a training phase during which, using the known information, we adapt the coefficients of the filter in order to minimize some criteria.

An example for a double polarization set up is illustrated in figure 3.10. In this case we have two complex signals at the input, two complex signals at the output and four filters communicating them in a butterfly fashion. The coefficients of those filters are initialized in the training phase and can be continuously updated during the execution of the DSP.

The coefficients of the filters need to follow some criteria to be updated. Two of the most commonly used methods are CMA and DD-LMS. Constant modulus algorithm (CMA) assumes that all the symbols used in the training or updating have constant modulus and iteratively adapts the filters until this is achieved in the output. Decision-directed least-mean-square requires to know (or at least decide using a ML criterion) the symbol that has been transmitted. If the symbol is known also the phase can be corrected at this stage. These are iterative algorithms and they need to be tuned as a function of the stability of the channel and other parameters like the pilot rate.

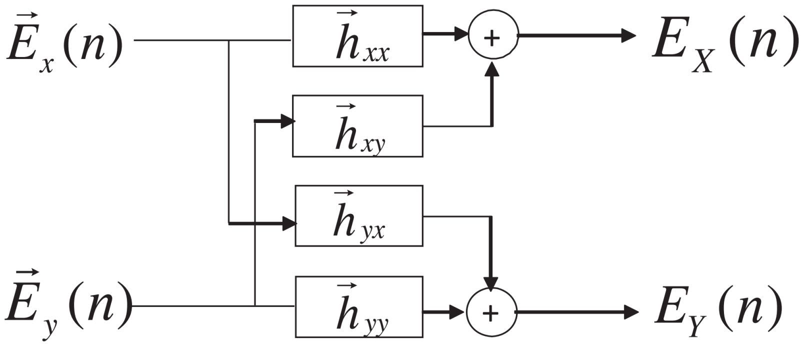


**Figure 3.10:** Butterfly structure of the adaptive filter [74].

### 3.5.4 Frequency and phase recovery

A frequency mismatch $\Delta f$ between the lasers of Alice and Bob will have an effect $h_{\Delta f}(t) = e^{i2\pi\Delta f t}$ on the received signal. This can be seen as a rotation of the constellation with time at constant angular velocity. This mismatch can happen due to a detuning between the two lasers and typically does not exceed 100 MHz. When the drift $\Delta f$ is slow, which is often the case, the effect can be compensated applying the opposite effect: $e^{-i2\pi\Delta f\, t}$.

The phase coherence of the lasers is inversely proportional to their linewidth and this characteristic is not so stable as the frequency. If the evolution of phase drift between the two lases is noted as $\phi(t)$ it is necessary to find and estimation $\hat{\phi}(t)$ and correct it multiplying by $e^{-i\hat{\phi}(t)}$.

There are several options to obtain a good estimation $\hat{\phi}(t)$. It is possible to agree on the value of certain symbols between Alice and Bob and use them as reference (pilots). The channel characteristics can be estimated from the difference in amplitude and phase between the received and the expected symbols. This method reduces the throughput as additional symbols need to be inserted only for channel estimation purposes, but it provides robustness to the communication.

Another option is to use the information symbols to estimate the channel. They are typically based on the estimation after a decision and the comparison with the received symbol. They tend to be particularly efficient with low density constellations and their main advantage is that they do not add symbol overhead.

Many methods exist, the most extended being Viterbi-Viterbi, blind phase search and Kalman filtering.

### 3.5.5 Synchronization

At the beginning of the communication Alice and Bob might not know at which point the message has started, so a synchronization mechanism is necessary. The most extended way to achieve synchronization is to send a sequence of symbols repeated regularly. The desirable feature of the sequence is that its autocorrelation is zero except at the origin (i.e. when the signal matches itself). Those sequences are called CAZAC (constant amplitude zero autocorrelation) and one of the most commonly used is the Frank–Zadoff–Chu (FZC) which has expressions of the form

$$x_u(n) = \exp\left(-j\frac{\pi un\left(n + c_{\mathrm{f}} + 2q\right)}{N_{\mathrm{FZC}}}\right) \tag{3.16}$$

with $N_{\mathrm{FZC}}$ the length of the sequence, $0 \leq n < N_{\mathrm{ZC}}$, $0 < u < N_{\mathrm{ZC}}$, $\gcd\left(N_{ZC}, u\right) = 1$, $c_{\mathrm{f}} = N_{\mathrm{ZC}} \mod 2$ and $q \in \mathbb{Z}$.

The first thing that the receiver does is to calculate the cross-correlation between the received signal and the CAZAC sequence. Peaks will be obtained at the origin of the sequence and the location of the rest of the symbols can be inferred if a known pattern was used.

The cross-correlation also serves to detect which is the right combination of ADC outputs to reconstruct the IQ signal, as only the right combination will give a strong positive peak. Also, some of the previous algorithms can only be applied at Bob's if we know the pattern of symbols (which are reference, information...) that we are processing. For example, during phase correction with references it is necessary to know if a symbol is a reference or information.

### 3.5.6 DSP scheme

The receiver will take the most heavy load of all the previously described techniques, especially when the regime of operation pushes the limits near what is theoretically possible. Both Alice and Bob need to agree on a pattern for the symbols (synchronization, references, information...) and a modulation format for each kind of symbol. With the ideas described previously, the DSP at the transmitter for a double polarization coherent system would look as in figure 3.11, performing mainly the pulse shaping. The receiver will need to perform the most complex operations in order to recover as much information as possible from the received symbols. Its DSP is sketched in figure 3.12.

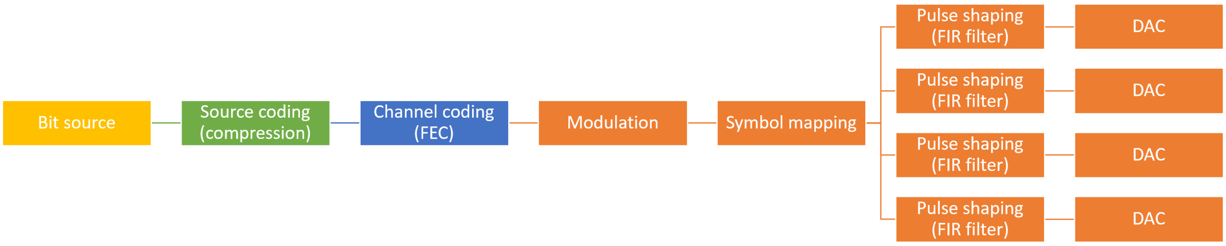

Bit source
Source coding (compression)
Channel coding (FEC)
Modulation
Symbol mapping
Pulse shaping (FIR filter)
Pulse shaping (FIR filter)
Pulse shaping (FIR filter)
Pulse shaping (FIR filter)
DAC
DAC
DAC
DAC

**Figure 3.11:** Scheme of the DSP at the transmitter.

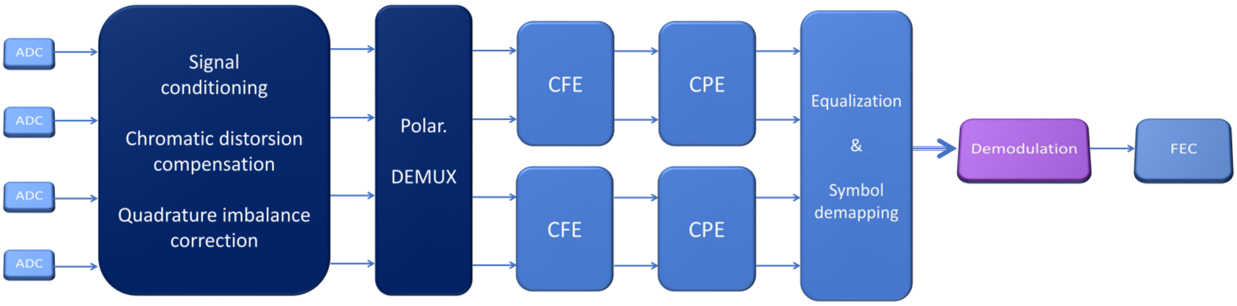

ADC
ADC
ADC
ADC
Signal conditioning
Chromatic distorsion compensation
Quadrature imbalance correction
Polar. DEMUX
CFE
CPE
CFE
CPE
Equalization & Symbol demapping
Demodulation
FEC

**Figure 3.12:** Scheme of the DSP at the receiver. CFE: Carrier Frequency Estimation; CPE: Carrier Phase Estimation.

## 3.6 Coherent communications and CV-QKD

The underlying principles of classical coherent communications and CV-QKD are the same. Early classical communications had a considerable amount of electronic noise, but modern systems can achieve 10 dB of clearance (ratio between the shot noise and the electronic noise), which makes shot noise the main source of noise in practice. This can create synergies in the development of technologies for both applications.

Classical communications are mainly focussed on the optimization of the mutual information, a parameter that does not depend on the nature of the noise. CV-QKD on the other side needs to the determine the fraction of the noise that corresponds to the fundamental shot noise (and possibly also the fraction of electronic noise if this parameter is assumed trusted), which changes the way of approaching the problem, since certain noise parameters need to be parametrized before hand and/or during the execution of the protocol.

For CV-QKD it is also important to have an accurate estimation of what is happening in the channel. In classical applications it is the same, but some of the algorithms might mask some of the effects. It is important that the DSP does not perform operations that might hide the presence of an eavesdropper from the parameters used in the estimation.

Another difference is the implementation of the error correcting code, that is used directly on the transmitted data in classical communication while in CV-QKD is applied after the symbol exchange.

In the rest of the section we will explore the possibilities of implementing a CV-QKD system using the techniques of classical coherent communications presented in this chapter. We will start building the system and the DSP from scratch in chapter 4 while chapter 5 will follow the opposite approach, studying the possibility of implementing CV-QKD over a high rate classical coherent communications system with a fully operational DSP.

# Continuous Wave CV-QKD 4

This chapter will study the possibility of building a CV-QKD system using classical coherent communications techniques. We examine its possible advantages and the consequences for security before proposing a proof-of-principle experiment to test the concept. The implementation of the main DSP algorithms is discussed and the initial results evaluated.

4.1 Motivation . . . . . . . . . . 57
4.2 CV-QKD using pulse shaping . . . . . . . . . . . . . . . . . 58
4.3 Is it secure? . . . . . . . . . . 59
4.4 Proposed proof-of-principle experiment . . . . . . . . . . . . . . 61
Hardware description . . . . 61
DSP description . . . . . . . 62
Preliminary results . . . . . 65
4.5 Comments and possible improvements . . . . . . . . . . . . 66

## 4.1 Motivation

Early communication systems like the electric telegraph used electromagnetic pulses well defined in time in order to be able to discern the different symbols. An analogous idea is used in the first CV-QKD implementations. Typically a laser is pulsed (directly or by an external intensity modulator) to produce a train of light impulsions with regular repetition rate $R$ and certain average power, and each of them is modulated by Alice and detected by Bob (interfering with a pulsed or continuous wave LO). The separation between the pulses is such that each of them can be considered independent from the others in the sense that an effect in one of the pulses will not influence the state of the others.

The main advantage of this strategy is to provide a simple system where the distinction between symbols is straightforward and direct detection can be applied (if $\omega_{\mathrm{IF}} = 0$), but if we calculate the Fourier transform of a train of pulses, the bandwidth $B$ of the spectrum would be much wider than the symbol rate ($B \gg R$). This has two main drawbacks: (a) the available bandwidth in the channel is not used efficiently; (b) the electronics involved in the system are required to operate at higher bandwidths $B > R$. Another disadvantage might be the need of chopping a continuous wave (CW) laser in order to work with pulses.[23] If the set up has side mechanisms to compensate the effects in the channel (polarization controller, time synchronization...) the operations in the digital domain could be done directly in symbols and the sampling done at rate $R$.

As discussed in the previous section, classical coherent communication systems solve the problem of bandwidth efficiency applying a particular filter to the symbols before the transmission over the channel (pulse shaping). The use of (root) raised cosine filters allows the reliable transmission occupying bandwidths in the order of the symbol rate, adjustable by the roll-off factor (ROF) $B = (1 + \mathrm{ROF})\, R$. For an intradyne detection system, the minimum bandwidth of the electronics should be slightly higher than $B/2$ to take into account the detuning, but the sampling rate should be at least $2R$. This configuration is in general more practical since DACs and ADCs with high sampling

[23] 23: In LLO CV-QKD systems it is necessary to have relatively long coherence times between Alice's and Bob's lasers, so it is convenient to use CW lasers.

rate are generally accessible, but they do not always provide the high analogue bandwidths that would be required in a pulsed scheme.

## 4.2 CV-QKD using pulse shaping

The efficiency in terms of bandwidth of using pulse shaping translates as symbols overlapping in time, meaning that the value of the signal at any given time is a function of all the symbols in the sequence (in practice only the ones in the vicinity are relevant). It is only at a particular moment that the value of the signal corresponds to the value of the symbol.

The general course of action for a communication at symbol rate $R$ can be described as follows:

1. Alice generates at rate $R$ the symbols $x[n]$ to transmit. The sequence $x[n]$ includes the subsequences interleaved in a previously agreed order:
   - $x_{\text{sync}}[n]$: deterministic CAZAC sequence for synchronization.
   - $x_{\text{ref}}[n]$: deterministic values for channel reference (mainly phase).
   - $x_{\text{secret}}[n]$: random values that will be used in the generation of the secret key.
2. Alice converts the symbols $x[n]$ to samples at rate $s_A R$ and filters them using a RRC filter before sending them to the DAC. The bandwidth of the optical signal is $B = (1 + \text{ROF})\, R$ and each IQ electronic signal occupies a bandwidth $B/2$. Optionally it is possible to apply a pre-distorsion filter before sending the signal to the DAC in order to correct some predictable imperfections of the hardware, like the spectral response of the amplifiers for example.
3. Alice's CW laser is modulated by the IQ signals and transmitted through the channel. The received signal interferes with Bob's CW LO and is converted using balanced photodetectors to 2 (SP) or 4 (DP) electronic signals which are amplified by transimpedance amplifiers (TIA).
4. Bob recovers the signals from the ADC at rate $s_B R$ and processes the information:
   - The cross-correlation with the CAZAC sequence allows the synchronization between Alice and Bob. With the agreed pattern Bob knows how to identify each symbol.
   - The adaptive filter recovers the polarization, the phase clock and other channel effects. The pulse shaping is completed in this step and it is possible to convert the samples to symbols $y[n]$ at rate $R$.
   - $y_{\text{ref}}[n]$ can be used to better estimate the channel and recover the frequency and phase mismatch.

5. Alice and Bob use the symbols $x_{\text{secret}}[n]$ and $y_{\text{secret}}[n]$ to continue the CV-QKD protocol. One part will be used for parameter estimation, then error correction and privacy amplification of the rest.

The system described is simply a classical coherent scheme, used not to transmit information directly, but to exchange quantum states between Alice and Bob. We already know that coherent systems work in the classical world, so the most important question now is whether this is secure for CV-QKD.

## 4.3 Is it secure?

As it was indicated in chapter 2, the security proofs are constructed based on the laws of quantum mechanics and a model of the system. We will study the key aspects of the pulsed shaping paradigm and see if they affect the assumptions for the model used in CV-QKD for Gaussian modulated states under collective attacks (see chapter 2).

**Detector noise.** In order to comfortably use the CV-QKD protocols, the predominant source of noise in the detector should be the shot noise. There are many commercial devices that can provide in the order of 10 dB of clearance which is sufficient for CV-QKD under trusted detector assumptions. It is important to characterize well the spectrum of the electronic noise and the shot noise[24] , and integrate them over the bandwidth of interest. In the intradyne detection that we are considering, the detuning between the two lasers also needs to be considered in the integration bandwidth.

**Variances.** The eavesdropping on the states should be recognizable by the trusted parties in the form of excess noise, so the typical modulation variances for the signal are typically much lower than in classical communications, in the order of a few shot noise units. This is a problem for LLO CV-QKD systems that need to recover the mode of the transmitted signal from the received one and if it is too weak it might be practically impossible. A typical solution is to send stronger agreed signals multiplexed in time, frequency and/or polarization, to act as references. This solution can be implemented with pulsed or CW schemes in a similar manner, and in both cases it is necessary to pay attention to the dynamic range of the components, particularly to the effective resolution of the DAC/ADC and the extinction ratio of the modulators. The peculiarity of pulse shaping is that the temporal values depend on the neighbouring symbols so if there is a sequence {secret, reference, secret} the shape would be mainly governed by the reference but the influence of the secret symbols would still be there and it can be recovered after DSP.

[24] The theoretical shot noise spectrum is flat, but the electronic response might introduce effects that need to be accounted for.

**DSP.** It is the most complex novelty of the CW scheme and it should be linear, conserve the signal bandwidth, conserve the energy and able to work in different modes.

**Linearity.** To maintain the linear properties of quantum mechanics it is necessary to avoid non-linear operations in the DSP. Filters will be linear and time-invariant (LTI) in general, so unless other effects like erasures or copies are introduced the typical DSP operations will not introduce non-linear effects. Note that there will be border effects due to the finite size of the filters, but those can be arbitrarily reduced extending their number of taps.

**Bandwidth.** All the signal information needs to be taken into consideration, so parts of the signal cannot be filtered out.

**Energy conservation.** The DSP can process the $d$ complex signals ($d = 1$ for SP and $d = 2$ for DP) from the ADC to form $d$ new signals with the correct polarizations and sampling phase. It is important that the factor $E$ between the sum of energy of the input and output signals $\sum_d \sum_n |s_{d,\text{in}}[n]|^2 = E \sum_d \sum_n |s_{d,\text{out}}[n]|^2$ is constant and taken into account in further steps[25] . This can be translated to a weighting factor in the coefficients of each filter.

**Calibration mode.** In order to avoid the conversion of units it is convenient to calibrate the shot noise and the electronic noise in the units used by the DSP. In the absence of signal the adaptive algorithms can diverge falsifying the results, so it is convenient to have a calibration or *dummy* mode where the adaptive filters are initialized to the Dirac delta filter $\delta[n]$ and not updated. In this calibration mode the process is the following: (1) the electronic noise $\sigma_{\text{el}}^2$ is measured without light, (2) the LO is injected at the $P_{\text{LO}}$ of interest measuring $\sigma_{\text{el}}^2 + N_0$, (3) $N_0$, the clearance and the electronic noise in SNU $V_{\text{el}}$ can be obtained from the two previous quantities.

**Signal mode.** When the signal is on, the adaptive filter can start working in order to correct the defects on the channel. After the complete sequence of symbols is recovered and the mode corrected using the reference symbols, the secret symbols will take part in the rest of the CV-QKD protocol.

If all these conditions are satisfied, then all the transformations due to the DSP can be considered linear and the validity of the security proofs described in chapter 2 should still hold. It can be argued that some of the process might be imperfect, so a confidence margin $\epsilon_{DSP}$ could be added to the estimated parameters, but the quantification of those imperfections on the final parameters could be matter of a more profound analysis. The first thing to evaluate is the noise that the DSP can add to the parameters, and for this we propose a proof-of-principle experiment implementing the most relevant features.

[25] Ideally $E$ should be one for simplicity, but sometimes it is interesting to normalize the energy of the constellation to one. If variance comparisons need to be made as in the case of CV-QKD the factor $E$ needs to be carried over in this case.

## 4.4 Proposed proof-of-principle experiment

We propose a proof-of-principle experiment to integrate the concepts of the previous chapters. Its performance will depend on the adopted hardware and the algorithms implemented by the DSP.

### 4.4.1 Hardware description

A fundamental part of the proof-of-principle experiment is the DSP, and the intention is to construct a system that can execute the DSP on real time[26] , processing the data continuously.

Several options were studied for the logical electronics. The use of benchtop oscilloscopes was discarded due to the difficulty of communicating between the DAC/ADC and the software continuously for relatively long times (longer than the memory of the oscilloscope). FPGAs could be a good candidate, but the time required to develop the DSP routings would be high.

The final solution was to use a PXI (PCI eXtensions for Instrumentation) chassis with one controller and modules for the DAC and ADC. The equipment is produced by Keysight and the key component is the M3302A PXIe AWG and Digitizer Combo module. In order to simplify the development experiment and reduce costs, the DSPs of Alice and Bob are running on the same machine, but there is no fundamental reason that would prevent the separation[27] (only additional classical communication task would need to be implemented).

The M3302A has 4 outputs and 8 inputs. The output sampling rate is 500 MSPS with 16 bits of resolution and an analogue bandwidth of 200 MHz. The input sampling rate is 100 MSPS using 14 bits per sample and allowing 100 MHz of bandwidth. If we would only consider the bandwidth of the electronics we could approach a symbol rate of 100 MBd (remember that the signals seen by the DAC/ADC occupy one half of the optical bandwidth), but the requirement of using 2 samples per symbol limits the symbol rate to 50 MBd, since the ADC can only sample at 100 MSPS.

The electronic bandwidth is given by $B/2 = (1 + \mathrm{ROF})R/2$, with ROF between zero and one, so knowing that the maximum available symbol rate is 50 MBd the maximum bandwidth that should be managed by the electronics will be 100 MHz (in practice ROF values tend to be low, so 60 MHz is a more realistic value). In the spirit of using readily available commercial devices we used the Koheron PD100B balanced detectors with TIA amplifiers, which can achieve 10 dB of clearance in the bandwidth of interest. More advanced home-made equipment is also been developed to improve the performance of the system. Given the expected 10 dB of clearance we will use the trusted detector version of the security proof, assuming that the electronic noise can be calibrated and trusted.

The initial channel medium will be fibre (although it could be extended to free space as discussed in section 4), so changes in the polarization

[26] The experiment is focussed on the signal processing part novelties, and this is the part targeted as real time, at least for the exchange of states involved in the formation of one key. More computing demanding tasks like CV-QKD post-processing are not considered to be on real time for the moment.

[27] The only technical aspect that could be different is the clock frequency alignment, but in practice it is not an issue at the frequencies of interest for the experiment.

are expected. A possibility for correction is to use a polarization controller, but as in most of the classical communication systems we decide to implement diversity in polarization at the receiver, so a double polarization 90° hybrid mixes Bob's LO with the signal arriving from the channel. Its eight optical outputs are measured using four balanced detectors connected to the ADC inputs of the M3302A.

As the electronic bandwidth of the detectors is not particularly large and the repetition rate is relatively low it is convenient to use frequency locked narrow linewidth lasers as sources of light. The narrow linewidth allows longer coherence times in phase, which could be recovered at rates of MHz using reference symbols. The fact of locking the frequency of the laser reduces the effect of the detuning between the lasers of Alice and Bob, which could displace the signal out of the band of the detectors. A pair of Pure Photonics PPCL590 laser is used with nominal linewidth of 10 kHz and where the frequency locking is achieved locking the wavelength of the laser to the resonance bands obtained from an acetylene gas chamber. Note that this locking system does not involve communication between Alice and Bob, but some trial and error to find the best channel to use in order to have a good locking in the two lasers.

The modulation of the optical signal at Alice is accomplished by lithium niobate modulators. Their linewidth exceeds 10 GHz and they need a driver, as the DAC in the M3302A is not able provide enough power for their operation. Having polarization diversity at the detector we can choose to use one or two polarizations at the transmitter. In this case we decided to use only one for simplicity, but the system can be extended to two. It is possible to use either one IQ modulator or a combination of amplitude and phase modulators, and several models from iXblue and EOspace have been tested. The amplifiers are iXblue DR-AN-10-HO.

The point of operation of modulators can drift in time, so it is important to correct it dynamically during the execution of the protocol. In order to achieve this a modulation controller can be placed after the IQ or the amplitude modulator. The controller acts over the DC port in order to adjust the bias, which is estimated introducing a dither signal (a small modulation in amplitude at a low frequency) also in the DC port. The equipment used is iXblue MBC-DG-LAB for the amplitude modulator and iXblue MBC-IQ-LAB for the IQ modulator.

A combination of variable optical attenuator (VOA), beam splitter and power meter is placed before Alice's output in order to measure the optical power injected to the channel. The channel can be a back-to-back (B2B) link, a VOA to simulate certain attenuation or a spool of fibre to create more realistic conditions.

### 4.4.2 DSP description

Keysight provides access to its libraries in many programming languages (C/C++, C#, Matlab, Python, LabView). We decided to implement the software in Python, creating three different libraries:

- Keysight with functions dedicated to the communication with the hardware.
- DSP, containing the signal processing algorithms.
- CVQKD for the functions related to parameter estimation and key generation.

Python scripts can be created in order to call the previous functionalities in the desired way depending on the case.

Given the available hardware it is interesting to choose symbol rates that are factors of the sampling frequencies (500 MSPS for Alice and 100 MSPS for Bob), so that we have an integer number of samples per symbol. The system will then be able to operate at 50, 25, 20, 10, 5 and 1 MBd.

The nominal resolution on the DAC is 16 bits, which is sufficient to approximate a Gaussian distribution without security concerns [90]. The 14 bit resolution in the ADC is also sufficient to distinguish a wide range of amplitudes in reception. Considering this, we decided to use a Gaussian distribution for the secret symbols, hence we are able to profit from all the results for this kind of modulation. The selected constellation for the phase reference symbols is QPSK due to the robustness and simplicity of the phase recovery methods available. The average energy of the phase reference symbols will be higher with respect to the secret symbols. The synchronization sequence is a Frank-Zadoff-Chu sequence of configurable length. The ratio of secret symbols per reference symbols is also be configurable.

Part of the DSP will run on Alice's side and well denote it by DSPtx, while the most complex algorithms will be carried out by DSPrx at Bob's side.

### DSPtx

We will assume that there is a file with a sufficient number of Gaussian samples for the duration of the protocol. It will be the source of the secret symbols, while the synchronization and reference symbols are deterministic and can be generated once and repeated with a given pattern. The steps to generate samples at Bob are the following:

1. The reference symbols are disposed according to the configured frame. The secret symbols are added and a complex vector is generated. A synchronization sequence is inserted at the configured times. One complex vector with secret, reference and synchronization symbols is available.
2. The sequence is upsampled (zeros are inserted between the symbols) and convoluted with a RRC filter at rate 500 MSPS.
3. The result of the filtering is transmitted to the PXI module. Optionally a pre-distortion filter can be applied.

### DSPrx

The reception will have two modes of operation: the calibration mode and the signal mode. The sampling rate is 100 MSPS in both modes.

In the calibration mode the optical signal is disconnected and the DSP is only collecting the power spectral densities (PSD) of the input when the LO is absent $S_{\mathrm{el}}[k]$ and when the LO is present $S_{\mathrm{el+N_0}}[k]$. The shot noise PSD $S_{\mathrm{N_0}}[k]$ and the clearance $S_{\mathrm{C}}[k]$ can be obtained from the previous two[28] . The PSD is calculated using Welch method [95] and the sample length is configurable.

The PSD of the shot noise and the electronic noise calculated this way contain the effects of the lasers, the balanced detectors and the ADC for each input channel (four in our case, equivalent to two complex signals). They are stored in memory and assumed to be stable during the execution of the protocol, so that they can be used later in the parameter estimation, integrated along the required bandwidth.

The signal mode consists in the following steps (all the applied filters are stored in memory):

1. The spectrum of the signal is calculated. The detuning $\Delta f_1$ is estimated assuming that the optical signal is symmetrical and centred at zero. The correction is done digitally multiplying the received signal by $e^{-i\Delta f_1 n}$.
2. A conditioning low pass filter is applied. The objective is to digitally filter the noise outside the band of interest.
3. The adaptive filter signal is passed through the adaptive filter:
   - The four filters are initialized with RRC filter coefficients.
   - The synchronization sequence is used to train the filters using DD-LMS algorithm.
   - The four real sequences are filtered, the samples are converted to symbols in the process.
   - After the filtering, two of the four real outputs will correspond to the signal while the other two should be zero and are discarded.
4. The remaining frequency $\Delta f_2$ and phase offset $\phi$ are estimated using the reference symbols and corrected multiplying by $e^{-i(\Delta f_2 n - \phi[n])}$. Several methods can be used.

At this point we have symbols that we can compare to those transmitted by Alice, but in order to calculate the variances and covariances correctly for CV-QKD some adjustments are still required:

- The reference spectra for the electronic and shot noise need to be transformed in the same way as the received signal, so the filters that have been stored during the previous steps are applied to them.
- There is a conversion factor $\gamma_A$ between the arbitrary units of the Alice's software and SNU.
- The trusted detection efficiency $\eta$ would need to have been estimated beforehand.

[28] The PSD is calculated in the digital domain, so $k$ is the digital frequency corresponding to the expression of the digital Fourier transform (DFT) $X[k] = \sum_{n=0}^{N-1} x_n \cdot e^{-\frac{i2\pi}{N}kn}$. The difference in natural units ($V^2/Hz$) gives the shot noise $S_{\mathrm{N_0}} = S_{\mathrm{el+N_0}} - S_{\mathrm{el}}$ and the difference in $dBm/Hz$ gives the clearance $S_{\mathrm{C}} = S_{\mathrm{el+N_0}}/S_{\mathrm{el}}$.

- The reconciliation efficiency $\beta$ is supposed to be fixed and realistic.

At this point, and with $N$ total secret symbols separated into $N_{\text{key}}$ and $N_{\text{PE}}$[29] , it is possible to calculate the variances and covariances correctly and from that estimate $V_A$, $N_0$, $V_{\text{el}}$, $T$ and $\xi$, and along with $\beta$ calculate the expected secret key size.

### 4.4.3 Preliminary results

Different configurations of the set up have been tested in order to develop the system. Ordered by complexity we can distinguish:

- The samples generated by DSPtx can be fed directly by software to DSPrx (only a resampling to adapt the sampling rate is necessary). This is the basic step to ensure that the logical structure of the DSP works. Artificial noise or phase changes can be simulated at this and other stages.
- The samples generated by the DAC are introduced directly in RF to the ADC. This allows the inclusion of the effects of the converters in the previous step.
- The samples act on a simplified version of the optical system, using the same laser for Alice and Bob. This avoids the detuning and simplifies the last stages of the protocol (frequency and phase recovery), but already includes the effects of the polarization and all the components of the set up.
- The complete system is tested, where the main challenge with respect to the previous step is the recovery of the frequency and phase of the carrier.

The first two stages are a characteristic of the system useful for debugging, so we will treat directly the results containing the optical part. The testing of the system is still in progress and at this stage it is possible to transmit information between Alice and Bob, but the calibration of the excess noise is still not resolved. The main problem seems to be the characterization of the detector response. As can be seen in figure 5.5 the response of the detector to an incoming signal has certain undesirable components (peaks in the signal part of the spectrum) that complicate the characterization of the relation of this response with the shot noise and the electronic noise. The effects seen take into account the responses of the modulator, the channel, the detector and the ADC electronics. New test are under progress with new home-made detectors and commercial integrated coherent receivers (ICR) in order to improve this characteristic.

[29] The selection is done randomly as a function of the configured percentage of symbols used for parameter estimation (PE). The value of $N_{\text{PE}}$ needs to be sufficiently high to avoid impairment from the finite size effects in the parameter estimation. The position in the frame is indicated to Alice and she reveals the values in an authenticated manner.

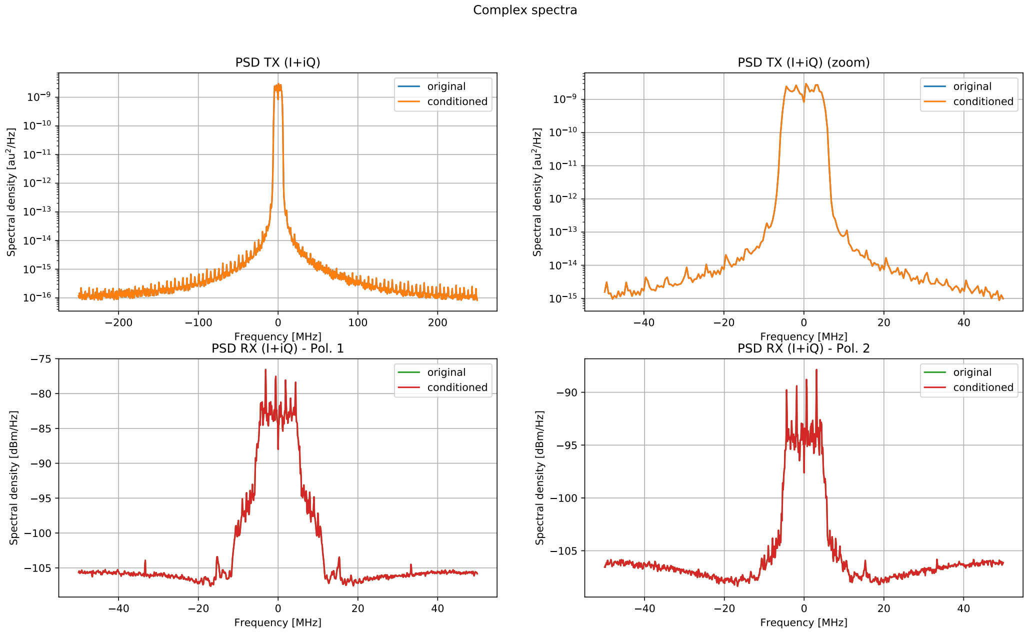


**Figure 4.1:** Power spectral densities at Alice's output and Bob's input. The complex spectrum corresponding to the I and Q components entering Alice's DAC is represented in the upper part of the figure (note that at this point the vertical units are arbitrary). The polarization diverse complex signals corresponding to the four inputs of Bob (I and Q for 2 polarizations) are displayed in the bottom part of the figure. They comprise the effects of transmitter, channel, detector (with TIA) and ADC. Note the clear spectral peaks observable in the detector response. Signal conditioning is off (original and conditioned are equal).

## 4.5 Comments and possible improvements

The system is intended as a proof-of-principle and its functionality can be extended in many ways. Probably the most interesting one would be to physically separate Alice and Bob. An additional PXI chassis and module would need to be added, but the software would still be functional with only minimal changes.

If a new module is added, it would be desirable that it extends the 100 MSPS of the current ADC. That would allow to increase the symbol rates above 50 MBd. The current system would be able to accommodate a double polarization transmission scheme if a DP modulator is installed, since the diversity in polarization already exists for the detection.

As long as the electronic noise is tolerable and the components support the bandwidth, it is interesting to extend the same ideas to higher symbol rates. In practice systems above the GBd are difficult to test in real time, so a different approach will be covered in the next chapter.

# High rate CV-QKD | 5

An implementation of CV-QKD using high rate (> 1 GBd) classical communication systems is discussed. The main characteristics are described and the structure of the system is presented, both in terms of hardware and software, including the interesting modulation schemes. The estimation of parameters for CV-QKD is illustrated for this particular case and the results are exposed and discussed before presenting possible improvements and evolutions.

This work is the fruit of the collaboration with the Research Department of Nokia Bell Labs at Nozay (France) and will be further developed in the PhD thesis of François Roumestan.

5.1 CV-QKD using high rate optical coherent communications systems . . . . . . . . . . . . . . . . 67
Hardware set up . . . . . . . 68
DSP . . . . . . . . . . . . . . . 69
5.2 Parameter estimation . . . . 71
Mutual information . . . . . 71
Estimation of detection efficiency: $\eta$ . . . . . . . . . . . . . . 72
Estimation electronic and shot noise: $N_0$, $\sigma_{\text{el}}^2$ . . . . . . . . . . . 73
Estimation of correlation: $\rho$ 74
Estimation of $V_A$ . . . . . . . 74
Estimation of $V_B$ and $\xi_{\text{Bob}}$ . 76
Estimation of $T$ and $\xi$ . . . . 76
5.3 Results . . . . . . . . . . . . . 76
QPSK modulation . . . . . . 77
PCS-QAM modulation . . . 77
Expected key rates . . . . . . 77
5.4 Possible improvements . . . 78

## 5.1 CV-QKD using high rate optical coherent communications systems

The approach followed in the previous chapter could be extended to higher bandwidths, but in the current state of technology it becomes impractical since the cost of the electronic equipment is much higher, and with more sampling rate more processing power is needed in order to keep up with real time processing. In order to overcome this inconvenience in research and development phases, it is typical to run the tests using a functioning hardware system, but most or all the processing is done off-line. The sequence would be as follows:

1. A sufficiently long sequence of samples is generated by DSPtx.
2. The sequence is loaded in an arbitrary waveform generator (AWGN) that controls the modulation.
3. While the system is running, a digitizer (oscilloscope) accumulates a sufficiently long sequence of received samples.
4. DSPrx processes the received samples off-line.

CV-QKD requires long sequences of symbols to reliably estimate the state of the channel, much longer than the memories of most digitizers. In this case the system should have the ability of working with different blocks of symbol that are not contiguous.

When the research phase is advanced and the system consolidated, the typical approach is to create a real-time implementation of the system. Field-programmable gate arrays (FPGA) are suitable systems for up to certain GHz using current technology. For higher rates an application-specific integrated circuit (ASIC) is usually required. The cost of implementation of these technologies is orders of magnitude higher than an off-line DSP that can run in desktop computer, but it is important to keep in mind that they would be the final target of this approach so the proposed algorithms should be cost-effectively implementable.

We will assume the availability of classical coherent communications equipment and standard DSP algorithms providing different modulation schemes and configurations. The most promising combinations for CV-QKD will be tested using the same procedure for each configuration $C$:

1. DSPtx generates samples for configuration $C$.
2. The physical system runs for certain time with the given transmission samples. Reception samples are collected and stored by the digitizer.
3. DSPrx processes the stored samples off-line giving the most relevant parameters for classical communications.
4. The parameter estimation is performed taking into account: (a) parameters measured outside the influence of the DSP; (b) parameters directly related to the DSP.
5. With the given parameters the SKR for configuration $C$ is estimated.

The objective is to identify configurations that can operate CV-QKD, but at the same time are as close as possible to current state of the art classical coherent communications. If substantial changes in the algorithms can be avoided, that would simplify the commercial implementation of CV-QKD devices based on classical coherent communications technology.

Figure 5.1 shows the basic scheme of the set up. Hardware and software elements are described in the following subsections.

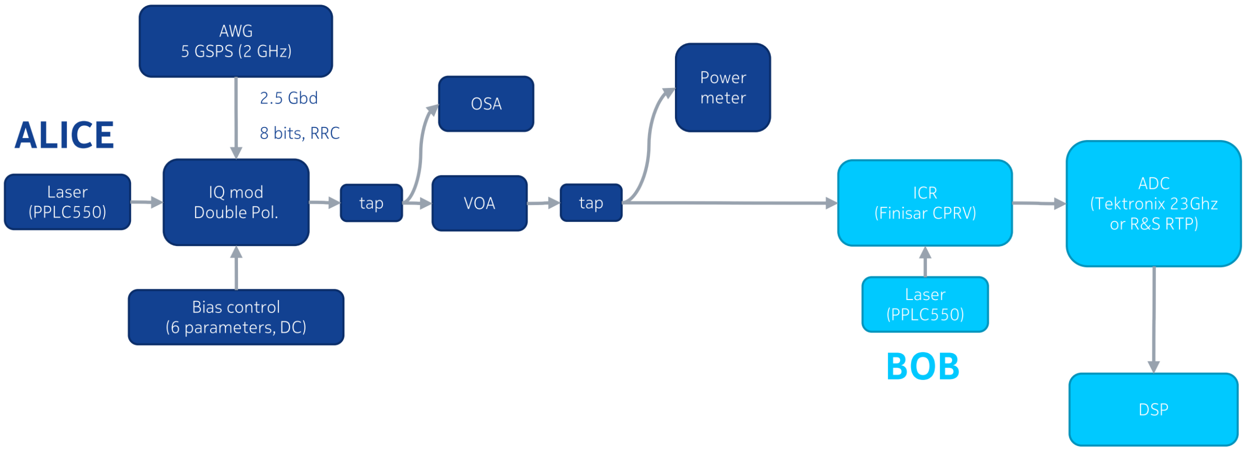


**Figure 5.1:** Scheme of the coherent communications set up.

### 5.1.1 Hardware set up

A double polarization diversity scheme in transmission and reception is presented. The light is generated by two Pure Photonics PPCL550 lasers with 10 kHz of nominal linewidth capable of providing 18 dBm of optical power. Bob's acts as LO and it is typically operated at 15 dBm. Alice's can be operated at lower output power.

The light from Alice's laser is modulated by a double polarization Fujitsu lithium niobate IQ modulator with 20 GHz of bandwidth. Six bias parameters need to be settled in order to work in the correct operation point. This setting is regulated manually with the help of an optical spectrum analyser (OSA) and the results of the DSP, and can be considered stable during several hours under normal operating conditions.

The digital signal generated by DSPtx is converted to an analogue electronic signal by a Tektronix AWG5200 generator and its four outputs amplified by four drivers that feed the DP IQ modulator. The AWG can generate samples at 5 GSPS with a nominal resolution of 16 bits and the bandwidth is 2 GHz. The memory depth per channel is 2 Gsamples, an important parameter that limits the length of the transmitted sequence without reloading a new sequence.

A software controllable variable optical attenuator (VOA) regulates Alice's output power extrapolating the measurements indicated by a power meter in the 90 arm of a 90/10 beam splitter.

Bob's hardware comprises three elements: the detector, the digitizer and the LO laser. The detector used in the tests is a commercial integrated coherent receiver (ICR) model Finisar CPRV. An ICR is a standard component in classical communication set ups that allows the integration of many optical and electronic features of the detector, as can be seen in figure 5.2. An ICR has two optical inputs: one SMF for the signal and one PM fibre for the LO. The interference, detection and amplification of the electronic signal are done inside the device, that provides four outputs in differential mode.

The four signals are directed to an oscilloscope that digitizes the signal at high sample rate. Different oscilloscope models have been used: (a) Tektronix DSO, 50 GSPS, 23 GHz, 8 bits; (b) Tektronix MSO64, 8 GHz, 25 GSPS, 12 bits. A photograph of the system in B2B configuration can be seen in figure 5.3.

Digitally, the rate limiting factor comes from the 5 GSPS of the AWGN that will allow symbol rates up to 2.5 GBd, occupying between 1.25 GHz (ROF=0) and 2.5 GHz (ROF=1) in each electronic path. This range fits widely in the regimes of the rest of the electronics.

### 5.1.2 DSP

The DSP used in the tests was developed by Nokia Bell Labs with coherent communications in mind, i.e. to maximize the mutual information between Alice and Bob, so it does not have adapted functions for CV-QKD as we did in the previous chapter. Is is proprietary and very flexible, so its full capabilities will be out of the scope of this document and only the most relevant characteristics for our purpose will be mentioned.

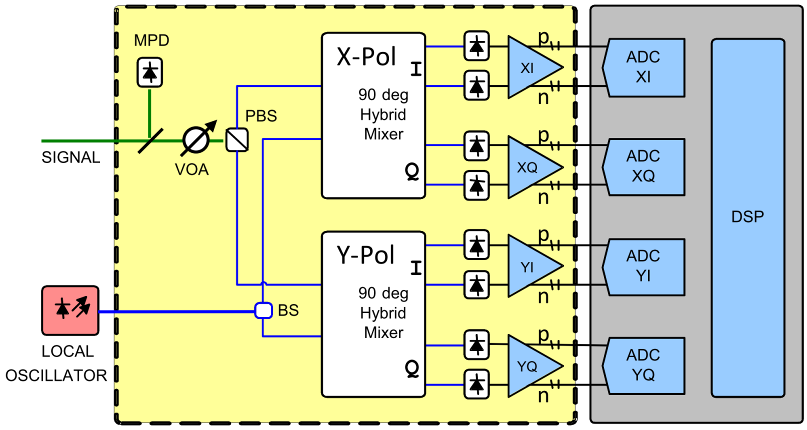


**Figure 5.2:** Integrated coherent receiver (ICR) scheme [Source: OIF DPC RX-01.2].

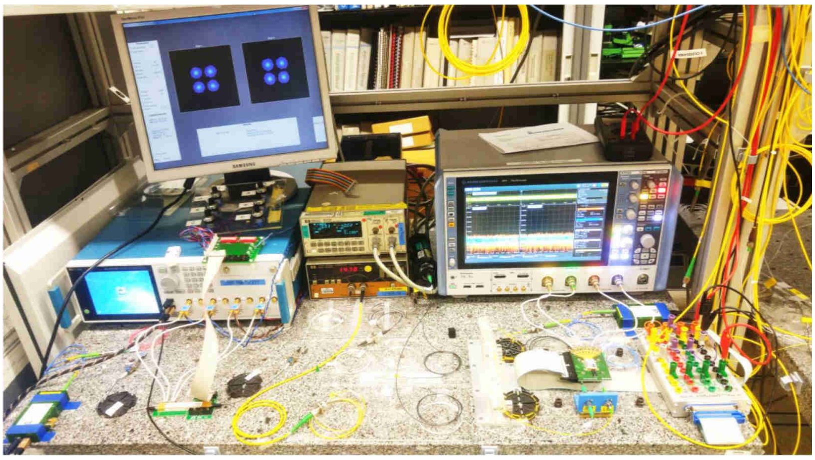


**Figure 5.3:** Photo of the coherent communications set up. Image courtesy of François Roumestan.

The DSP is equipped with the capability to generate and treat many digital modulation schemes, but the most interesting for us will be QPSK, 16-QAM, 64-QAM and PCS-64-QAM. Probability shaped constellations (PCS) are interesting for CV-QKD since they approach the distribution of a Gaussian modulation, which has many desirable qualities for the security proofs. The good characteristic of the chosen AWG, despite of its relatively low sample rate, is the nominal resolution of 16 bits. This allows the accurate representation of high density constellations in the electronic domain.

The most elaborated algorithms run in DSPrx which follows a scheme directly comparable to figure 3.12. As the typical SNR in CV-QKD will be typically lower than in classical communications, it is interesting to explore different configurations of reference symbols (pilots) in order to support the DSPrx algorithms. Pilots are reference symbols with agreed information and location, and will help the DSP, but not form part of the secret key generation. Phase recovery algorithms of different kind (Viterbi-Viterbi, blind phase search, Kalman filtering...) are available and configurable.

The input of DSPrx are the four sample sequences from the ADC (equivalently two complex sequences) and the natural output are two complex sequences with the resulting symbols and the associated SNR per polarization.

## 5.2 Parameter estimation

The estimation of parameters for one and two dimension systems (one polarization and one or two projections) has been already treated in chapter 2 and appendix C. Here we will need to extend it to two polarizations, taking into account that the polarization recovery will be done by software, mixing the signals from the different inputs according to certain algorithms.

We will treat the communication in both polarizations as CV-QKD. The main reason to do this is to guarantee that all the excess noise present at Bob's input is also taken into account at the output of Bob's DSP. If only part of the processed signal would be used for CV-QKD it would be harder to certify that part of the excess noise was not transferred to the non-CV-QKD service[31] . We will also assume that when one symbol is randomly revealed for parameter estimation both polarizations are revealed.

The detector will be the factor influencing most of the parameters. Four sequences of values will be read by the ADC and treated by the DSP as a function of the effect suffered in the channel. As the signals are mixed digitally the same happens with the noise parameters at each input. For simplicity we will assume that the electronic and shot noise in each input channel $c$ are sufficiently similar to be approximated accurately as

$$N_0 = \frac{1}{4}\sum_{c=0}^{3} N_{0,c} \qquad N_0\, V_{\mathrm{el}} = \frac{1}{4}\sum_{c=0}^{3} \sigma^2_{\mathrm{el},c} \tag{5.1}$$

Under these conditions the relations of the measured values and the parameters involved in the Holevo bound calculation still hold:

$$\langle x^2 \rangle = \sigma_A^2 = V_A/\gamma_A^2 \tag{5.2}$$

$$\langle y^2 \rangle = \sigma_B^2 = N_0(2 + 2V_{\mathrm{el}} + \eta T \xi_{\mathrm{Alice}}) \tag{5.3}$$

$$\langle xy \rangle = \sqrt{\eta T} V_A \tag{5.4}$$

In this section we will see how to estimate each of the parameters, as well as the mutual information.

### 5.2.1 Mutual information

The main output value of the DSP is the SNR per polarization obtained after the processing. In CV-QKD the communication is not direct, so in order to have the value of the mutual information we need to complete the error correction phase, but a reliable way to obtain an estimation of the mutual information is to rely on the efficiency of the protocol $\beta$.

[31] It might still be possible if the parameter estimation is also run on the symbols of the other service, but not very practical. CV-QKD could coexist with classical communications in the same set up, multiplexed in time or frequency for example.

The expected mutual information per polarization $P$ is calculated in bits per symbol as:

$$I_{\mathrm{AB,p}} = \beta\left(\mathrm{SNR}_p\right)\log_2\left(1+\mathrm{SNR}_p\right) = \beta\log_2\left(1+\mathrm{SNR}_p\right) \tag{5.5}$$

where in the last equality we assumed that we can obtain the desirable efficiency $\beta$ independently of the SNR using methods similar to [96]. Using two polarizations for CV-QKD the total mutual information will be the sum of the contributions by both polarizations:

$$I_{\mathrm{AB}} = \sum_{p=1,2} I_{\mathrm{AB,p}} = \beta\sum_{p=1,2}\log_2\left(1+\mathrm{SNR}_p\right) \tag{5.6}$$

### 5.2.2 Estimation of detection efficiency: $\eta$

The eight photodiodes of the detectors used in the set up can be polarized independently, so it is possible to measure each of the photocurrents independently, and from that calculate the efficiency of each photodiode as described in chapter 2. We will assume that the LO and the signal path have different losses and measure them independently. Taking into account that in this case the natural losses are $\mathcal{L}_{\mathrm{N,LO}} = 1/8$ for the LO and $\mathcal{L}_{\mathrm{N,S}} = 1/4$ for the signal, we can alternate the insertion of light between the LO input with power $P_{\mathrm{LO}}$ and the signal input with power $P_{\mathrm{S}}$ to obtain the corresponding efficiencies:

$$\eta_{\mathrm{LO,i}} = \frac{I_{\mathrm{LO,i}}}{P_{\mathrm{LO}}\mathcal{L}_{\mathrm{N,LO}}\mathcal{R}_{\mathrm{opt}}} \qquad \eta_{\mathrm{S,i}} = \frac{I_{\mathrm{S,i}}}{P_{\mathrm{S}}\mathcal{L}_{\mathrm{N,S}}\mathcal{R}_{\mathrm{opt}}} \tag{5.7}$$

The measurements in the LO input is stable, since it uses a polarization maintaining fibre, but in the signal input it is more delicate since it involves a SMF and a polarization controller is required to maximize the results in the photodiodes corresponding to one polarization alternatively.

The measured values are shown in figure 5.4 and we can see that they cover a range between 0.5 and 0.6. The lower efficiency in the signal input can be explained by the tap included in the signal path. The ICR introduces an additional component (a polarization rotator) in one of the polarization paths, so one of the polarizations is less efficient than the other. The interest of separating the losses between a trusted part $\eta$ and an untrusted part $T$ is to use trusted models for the detector in the security proof. For this reason, in order to maintain security we need to choose the lowest value which in this case is $\eta = 0.5$. The concerned values are those of the signal input, which in this case coincide with the minimum.

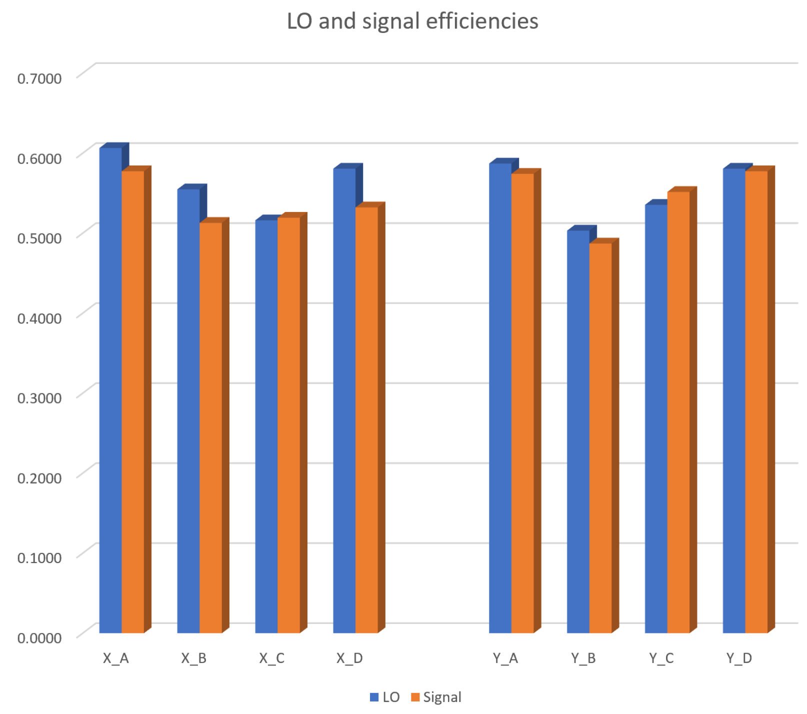


**Figure 5.4:** ICR photodiode efficiency. The photocurrents or each photodiode are measured independently with an ampere-meter and compared to the optical responsivity $\mathcal{R}_{\text{opt}}$ once the natural losses $\mathcal{L}_N$ for a double polarization detector are taken into account.

### 5.2.3 Estimation electronic and shot noise: $N_0$, $\sigma^2_{\text{el}}$

The electronic and shot noise are estimated before the execution of the protocol. The power spectral density is calculated from long acquisitions of signal by the oscilloscope:

1. For the spectrum of $\sigma^2_{\text{el}}$ no light input is applied to the signal.
2. For the spectrum of $N_0 + \sigma^2_{\text{el}}$ light is injected in the LO input.
3. The spectrum of $N_0$ is calculated from the natural difference of the two previous ones.
4. The spectrum of the clearance is calculated from the logarithmic difference of the first two ones.
5. A band pass filter is applied to the band of interest as a function of the symbol rate: (1) the high cut frequency point is set to $(1 + \text{ROF})\,R$; (2) the low cut frequency is set to 200 MHz in order to eliminate the effects of the AC coupling in the oscilloscope.

The typical spectral results are not flat in all the bandwidth of the detector (around 25 GHz), as can be seen in figure 5.5. The high bandwidth TIAs are able to achieve more clearance in the lower part of the spectrum, obtaining more than 8 dB of clearance for bandwidths lower than 4 GHz, up to 10 dB around 1 GHz. This corresponds to values of $V_{\text{el}}$ between 0.1 and 0.18 SNU. The final value will depend on the integrated bandwidth and the average described in equation 5.1.

It is necessary to ensure that the detector operates in the linear regime at a given LO power $P_{\text{LO}}$, in which case the integrated noise should be linear as a function of $P_{\text{LO}}$. Multiple power spectrum densities have been calculated at different values of $P_{\text{LO}}$ in order to calculated the integrated noise between certain frequencies and verify the linearity. Figure 5.6 shows the behaviour for the bandwidth between 1 and 5

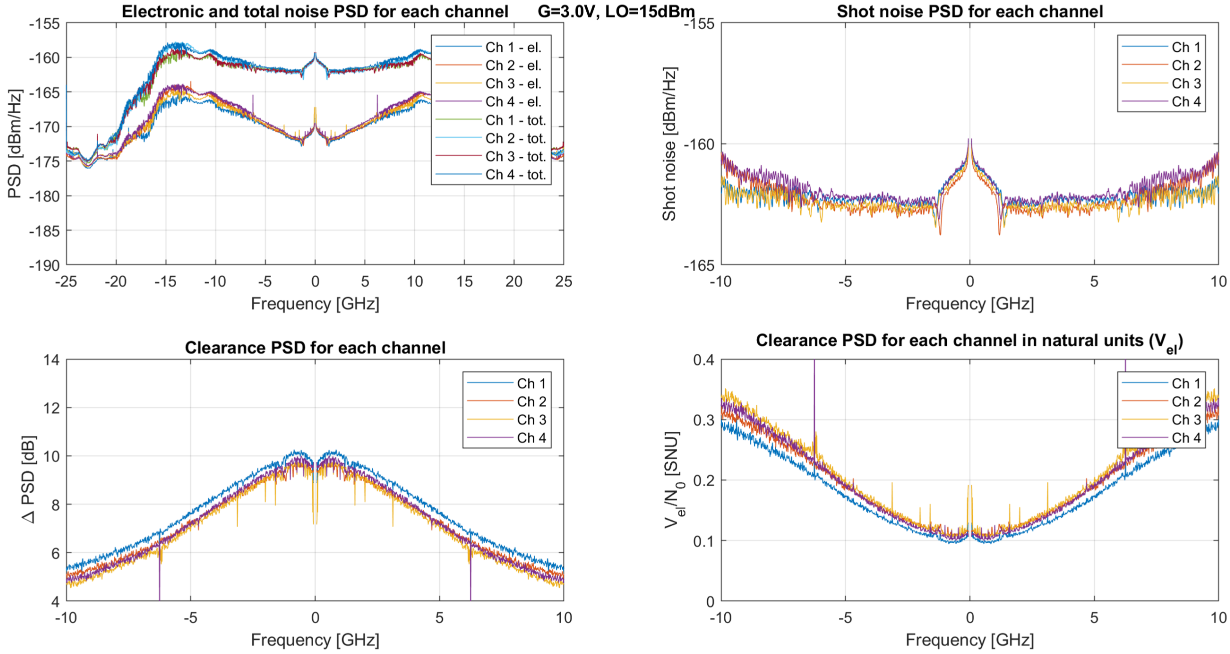


**Figure 5.5:** Measured power spectrum densities of ICR electronic and shot noise. The electronic and total PSD are shown for each channel along the entire bandwidth of the scope. The shot noise PSD and the clearance PSD are displayed for a narrower band. $P_{\mathrm{LO}}$ = 15 dBm = 31.6 mW.

GHz. It can be seen that the linearity holds only up to 40 mW (16 dBm) of LO power, which is the recommended limit for the device. It is a saturation effect, while another possible effect could be the tendency to an ascending quadratic curve, indicating the non-negligible presence of optical classical noise (e.g.: RIN). The used value in the following will be $P_{\mathrm{LO}}$ = 15 dBm = 31.6 mW, which corresponds also to the value illustrated in figure 5.5.

### 5.2.4 Estimation of correlation: $\rho$

The DSP is prepared to give directly the SNR as result, but there is a direct relation with the correlation $\rho$ and the SNR in natural units:

$$\mathrm{SNR} = \frac{\rho^2}{1-\rho^2} \qquad \rho^2 = \frac{\mathrm{SNR}}{1+\mathrm{SNR}} \tag{5.8}$$

We also know that the normalized correlation corresponds to the following expression

$$\rho = \frac{\langle x\, y\rangle}{\sqrt{\langle x^2\rangle\,\langle y^2\rangle}} = \frac{\langle x\, y\rangle}{\sqrt{V_A V_B}} \tag{5.9}$$

### 5.2.5 Estimation of $V_A$

**Estimation using the optical signal.** The estimate of $V_A$ can be calculated from the average photon number of the quantum fraction of

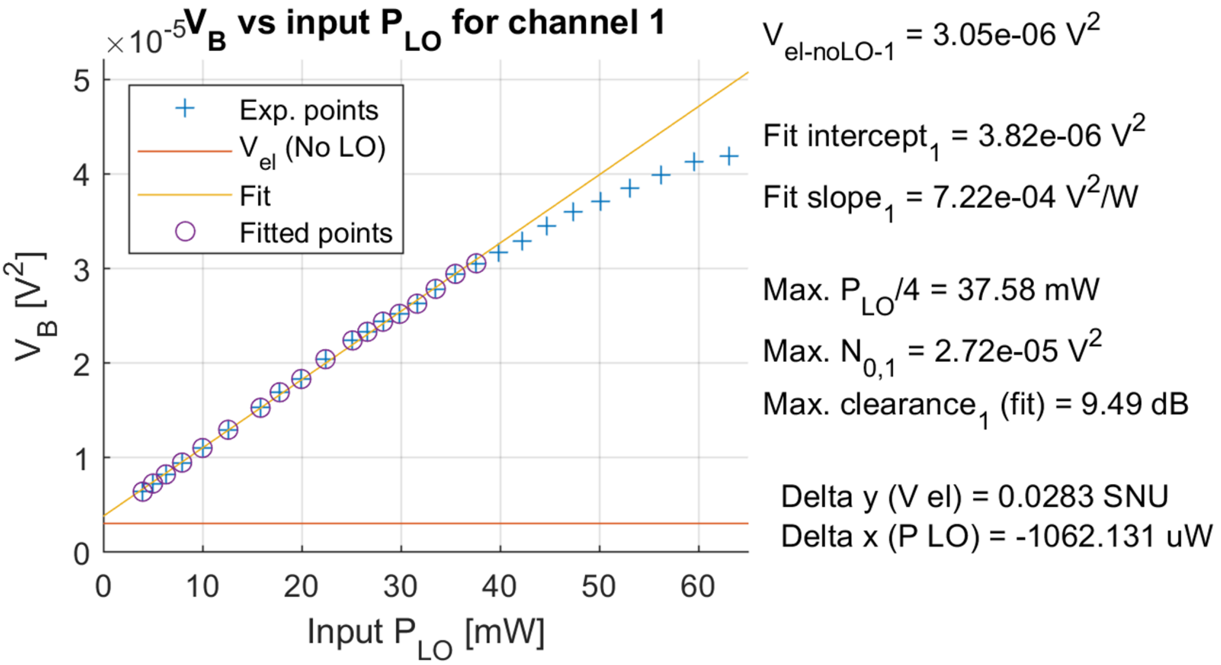


**Figure 5.6:** ICR integrated electronic and shot noise between 1-5 GHz. The calculations are done by channel and for the fit only the circled points are used. This is the result for one of the four input channels, the other three are similar. The intercept of the fit should coincide with the electronic noise (shown in red), the deviations are indicated.

the signal transmitted by Alice. For a distribution with only one modulation level (same power for signal and reference), $p$ polarizations, rate $R$, optical power $P_{\text{opt}}$, photon energy $E_{\text{ph}}$ Alice's variance can be calculated as

$$\hat{V}_A = 2\langle n_p \rangle = \frac{2}{p} \frac{P_{\text{opt}}}{E_{\text{ph}} R} \tag{5.10}$$

For a multilevel signal only the fraction involved in the quantum part of the signal should be taken into account. For this the power ratio between both needs to be known, as well as the fraction of symbols that are dedicated to each task.

**Estimation using the electronic signal.** The values $x_i$ in equation 5.2 represent the values in Alice's software, so it is necessary to use a factor $\gamma_A$ to obtain the relation between $V_A$ in shot noise units and $\sigma_A^2$ in arbitrary units. There are several ways to do that, but probably the simplest is to set up a distribution with variance $\sigma_A^2$ and measure the average optical power $\langle P_{\text{in}} \rangle$ at the input of the channel (Alice's output), that can be related to the symbol rate $R$, the energy per photon $E_{\text{ph}}$ and the average number of photons per symbol $\alpha^2$ as $\langle P_{\text{in}} \rangle = \alpha^2 E_{\text{ph}} R$. The variance in SNU is $V_A = 2\alpha^2$ and it is easy to calculate the factor that corresponds to $V_A = \gamma_A^2 \sigma_A^2$ as[32]

$$\gamma_A^2 = 2\frac{\langle P_{\text{in}} \rangle}{E_{\text{ph}} R} \tag{5.11}$$

[32] If $\sigma_A^2 = 1$ as it considered by the DSP then $\gamma_A^2$ is directly $V_A$.

### 5.2.6 Estimation of $V_B$ and $\xi_{\text{Bob}}$

At Bob's the spectrum of the received signal is integrated in the band of interest giving the value $\sigma_B^2$ in $V^2$. During the DSP the signal is normalized to one, and after the process is completed the normalized fraction of total noise $\bar{\sigma}_n^2$ in arbitrary units is available. As the total signal at the DSP is normalized to one, it can serve as factor to calculate the total noise in $V^2$ simply multiplying it by the original signal power:

$$\sigma_n^2 = \sigma_B^2 \times \bar{\sigma}_n^2 \tag{5.12}$$

We know from equation 5.3 that the noise is composed of shot, electronic and excess noise.

$$\sigma_n^2 = N_0 + \sigma_{\text{el}}^2 + N_0\xi_{\text{Bob}}/2 = N_0(1 + V_{\text{el}} + \xi_{\text{Bob}}/2) \tag{5.13}$$

Shot and electronic noise have been previously estimated, so we can deduce the excess noise from the previous estimations. The value as seen at Bob's can be calculated as:

$$\xi_{\text{Bob}} = 2\frac{\sigma_n^2 - N_0 - \sigma_{\text{el}}^2}{N_0} = \eta T \xi \tag{5.14}$$

### 5.2.7 Estimation of $T$ and $\xi$

To calculate the equivalent excess noise at the input of the channel $\xi$ it is necessary to know the transmission efficiency $T$. From equation 5.4 we can estimate the transmission efficiency $T$ (for the B2B the value should approach one):

$$T = \left(\frac{\langle x\, y\rangle}{V_A\sqrt{\eta}}\right)^2 \tag{5.15}$$

The excess noise at the input of the channel is then

$$\xi = \frac{\xi_{\text{Bob}}}{\eta T} \tag{5.16}$$

## 5.3 Results

Different modulation formats have been tested and the most interesting results were obtained with QPSK and PCS-64-QAM. The results have been proven very dependable on the symbol rate and the different parameters of the system. The main target is to obtain the parameters of interest for CV-QKD as a function of different conditions, the most sensible for the DSP being the SNR.

### 5.3.1 QPSK modulation

QPSK is an interesting modulation scheme due its simplicity and robustness, along with the variety of algorithms that can work efficiently with it (e.g.: Viterbi-Viterbi). There has been recently a series of articles on asymptotic security proofs for discrete modulations [86–88] that can be applied for QPSK. They join the security proof restricted to linear channels [85] that we will use as reference[33] .

One characteristic of QPSK modulation according to the security proofs above is the requirement of relatively low $V_A$. This will result in practice in very low SNR at the receiver side and the DSP will have difficulties to operate correctly. Preliminary measurements have been carried out by François Roumestan for values of $V_A$ between 0.5 and 3 SNU, giving values of $\xi_{\mathrm{Bob}}$ around 0.07 SNU, which in B2B configuration and with $\eta = 0.5$ gives $\xi \approx 0.14$ SNU. We will use these values to estimate the key rates in the next section.

### 5.3.2 PCS-QAM modulation

PCS modulation is interesting because the mutual information can potentially increase and, if the constellation density is sufficiently high, Gaussian approximations can be extrapolated. A first approach to a Gaussian modulation, reasonably valid for low $V_A$, is done with a PCS-64-QAM constellation. The estimated excess noise as a function of $V_A$ has been measured by François Roumestan and currently it is $\xi \approx 0.20$ SNU at the input of the channel for $V_A = 0.1$ SNU.

### 5.3.3 Expected key rates

The expected SKR as a function of $V_A$ at a distance of 100 m is represented in figure 5.7. The curves for different excess noise values are displayed and it can be seen that not all the values of $V_A$ can produce key in these circumstances. The trusted detector model is used to take into account the effect of an imperfect detector of efficiency $\eta = 0.5$ and electronic noise $V_{\mathrm{el}} = 0.10$ SNU.

In particular for QPSK with linear channel proof it is possible to work in a relatively narrow margin of values of $V_A$ and the excess noise should not exceed 0.045 SNU. This means that we should improve the obtained excess noise estimation of 0.14 SNU by a factor 3 in order to operate in this regime. The ranges of $V_A$ are already achievable using high power pilots. We can see that if we extend the distance to 20 km (figure 5.8) it is very challenging to work with QPSK since the required excess noise will be in the order of one percent.

Assuming Gaussian modulation the situation is very different, since the range of $V_A$ is much higher in this case, and also the tolerance to excess noise. In fact for these particular distances it is convenient to use high values of $V_A$. The problem with the obtained results is that $\xi$ tends to increase with $V_A$, so the use of PCS-64-QAM is not viable with the current performances.

[33] The linear proof, although more restrictive in the assumptions is easier to calculate than the other ones, which are based on semi-definite programming (SDP). It also seems to be a lower bound in many cases (not all of them), so it can be a good initial reference.

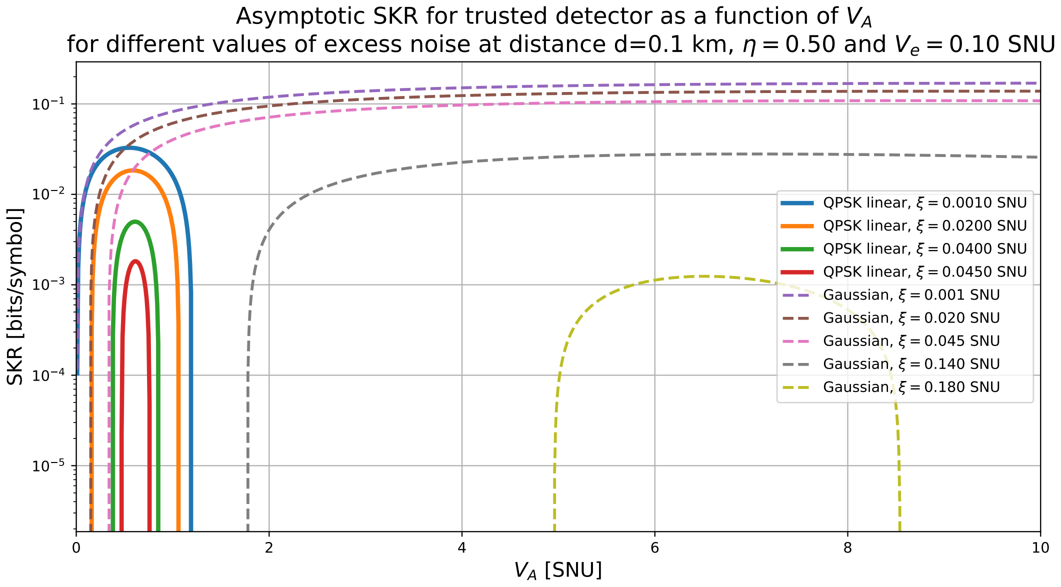


**Figure 5.7:** Expected SKR as a function of $V_A$ at 100 m for different values of excess noise. The margin of useful values of $V_A$ is bigger using Gaussian modulation than QPSK. Gaussian modulation is also more tolerant to the excess noise.

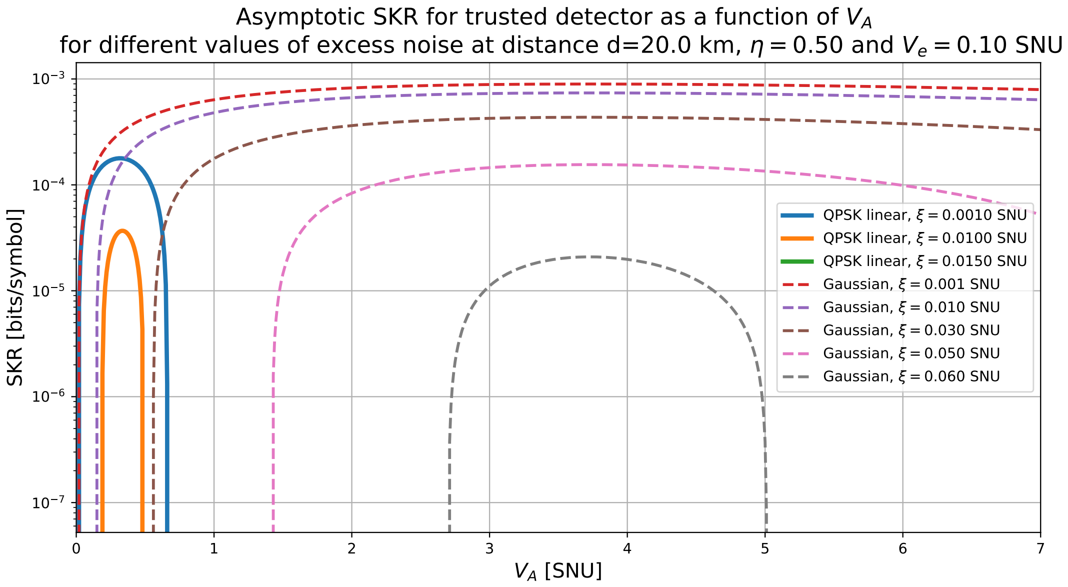


**Figure 5.8:** Expected SKR as a function of $V_A$ at 20 km for different values of excess noise. Using Gaussian modulation it is possible to achieve several km with excess noise estimates lower than 0.1 SNU. In order to achieve the same performance with QPSK at these distances an order of magnitude lower in $\xi$ is required.

## 5.4 Possible improvements

The obtained results need to be improved in order to successfully use CV-QKD on a system of that kind. The minimum required improvement would be to reduce the excess noise (at least by a factor 4 in the Gaussian case to operate comfortably at 20 km), but a more noticeable improvement would be desired. If the target is to achieve key exchange at a distance in the order of tens of kilometres, using a Gaussian-like modulation with a trusted detector the excess noise should be maintained below 10% for a wide range of $V_A$. With a QPSK modulation both excess noise and $V_A$ should be much lower than the Gaussian case.

The first thing to understand is the behaviour of each of the algorithms under the test conditions. Except for the adaptive filter, the elements of the DSP are applied sequentially so it is important to understand which is the algorithm that is not responding correctly and study the alternatives to improve it: increase the pilot rate or power, increase the repetition rate, change the algorithm... For this it is interesting to test the algorithm in a controlled scenario with software generated signals.

This process can be iterated and once the weakest algorithm of the DSP is improved, continue with the next bottleneck. But even following that procedure there will be a limit below which the DSP cannot go. Possible causes might be the quantization of the signal, the finite resolution in the operations, the finite time for the convergence of the algorithms, the fading of the channel... Once this limit is reached it will be necessary to study if the achieved performance is sufficient for the cases of interest, or if a dedicated *ad hoc* system based on similar premises is more convenient.

# ON-CHIP CV-QKD

# Integration of optical devices 6

6.1 Integrated circuits . . . . . . 83
6.2 PICs in CV-QKD . . . . . . . 84
Additional considerations . 85
6.3 Development of a PIC . . . 86

The objective of this chapter is to serve as a brief introduction to integrated photonics in order to understand the main concepts of the next chapter, where we will test a 180° hybrid on chip. More detailed views on this topic can be found in [97, 98] as well as the references provided in the text.

## 6.1 Integrated circuits

Photonic integrated circuits (PIC) are devices that combine multiple photonic functions in one chip. PICs have many points in common with the electronic integrated circuits (EIC or more commonly IC) since they can be fabricated using similar techniques (photolithography typically) and facilities. One important difference is that while EICs operate on electrons that follow Fermi-Dirac statistics, the operations on PICs are applied to photons obeying Bose-Einstein statistics. This characteristic will result in two different paradigms.

EICs are good devices for the storage of information, especially in binary format thanks to the use of transistors operated as on-off switches, which also simplifies the execution of digital operations. The transistor is the fundamental element of this paradigm, and concentrated attention on its improvement allowed the explosion of the performances of this kind of devices during the last fifty years, revolutionizing the digital information industry. The transistor density on an EIC is a typical performance indicator used in the industry and for many years it has followed the famous Moore's Law [99], doubling every two years although this might change as the size of the transistors approach atomic scales.

The bosonic nature of PICs implies that they will cover different functionalities than the EIC counterparts. One field where PICs excel is the communication and routing of high-speed data, in particular at infra-red wavelengths due to the compatibility with optical fibre transmission windows. This capacity made PICs a key player in the recent ICT (information and communication technologies) industry where their presence is expected to grow in the near future [100]. Nowadays it is possible to construct integrated devices that can generate, detect and guide light among other linear and non-linear operations. Each of these operations is performed by a specific device designed for that purpose. In a PIC there is no equivalent reference device like the transistor for digital EICs and the design methodology is more similar to radio-frequency analogue EIC. Having a more specific design approach can be beneficial in some situations. For example, using a PIC it is relatively easy to construct a wavelength multiplexer using an array waveguide grating (AWG) [101].

The undeniable leading technology in the EIC industry is silicon, with its different fabrication technologies, but based on the same material due to its interesting properties. The PIC industry in the first years was clearly dominated by III-V materials (especially indium phosphide, InP), but recently other technologies like silicon (silicon photonics/silicon nitride), ferroelectrics (lithium niobate), polymers, photonic crystal waveguides and metal optics have entered the scene.

III-V materials have a direct band gap that provides great flexibility in the design of optical components, allowing the integration of active and passive components on the same substrate. The similarities on their lattices also facilitate different combinations according to the requirements of the devices, e.g.: indium gallium arsenide (InGaAs) can be grown over InP. Silicon photonics is an indirect band gap material, so the creation of active devices like lasers is not practical.

The refractive index is one of the main factors that influence the confinement of the light inside the waveguides and devices. It depends a lot on the fabrication process and a good reference to calculate the expected value as a function of the wavelength is [102], a catalogue of many available fabrication technologies. Silicon has a high refractive index (in the order of n=3.5) which makes it a good candidate for the fabrication of long circuits where losses are important. It also allows the use of more abrupt bends in the design, reducing the size of the circuit (and hence the cost). The refractive index of InP is slightly lower than in silicon.

The main advantage of silicon with respect to other alternatives is the potential combination with the technologies used in the more mature EIC industry, mainly conventional CMOS (complementary metal-oxide semiconductor) and SOI (silicon on insulator). Detection of light at telecommunication wavelengths can be provided by germanium (Ge) photodiodes, but the generation of light should be provided by an external source (e.g.: an InP laser).

At this moment we do not know any material that can perform optimally all the interesting photonic operations. For this reason it is typical to combine different materials and technologies to obtain the desired results.

## 6.2 PICs in CV-QKD

Quantum communications use mainly photons to transmit information, so the use of PICs would improve the size, cost and consumption of the devices in comparison to the bulk counterparts. Different stages can be targeted. The first step would be the integration of some or all of the photonic operations in one chip, controlled by external electronic components. A second step, related to the similarities between PIC and analogue EIC, would be to include also analogue electronics (drivers and amplifiers) in the integration, maintaining the logical control external. A third and more ambitious step would be the integration of the logical control with the other functionalities, providing an application-specific integrated circuit (ASIC).

For a CV-QKD implementation using coherent states of light the following functionalities can be involved:

- Generation of coherent states. InP is one of the most suitable technologies for the construction of lasers [103]. Important parameters to take into account are power (especially for Bob's LO), linewidth, noise and stability.
- Modulation of coherent states. ICT industry has extensively used lithium niobate devices for high rate modulation systems, but they could be substituted by InP or silicon photonics.
- Attenuation. If we consider attenuation as a slow type of amplitude modulation it could be implemented with the same devices, but typically it is more practical to include simpler mechanisms like passive thermal actuators.
- Waveguides. The different elements are communicated by waveguides, sometimes requiring relatively abrupt turning angles to optimize space. Light will propagate along the waveguide, but at the same time have evanescent losses through the borders. It is important to have good confinement indices, even for small bending radii.
- Interference. Beam splitters and multi-mode interferometers are common devices to mix two or more light beams [104].
- Detection. The wavelength will play an important role in the selection of the technology [105]. Good candidates for 1550 nm are indium gallium arsenide (InGaAs) in InP and germanium (Ge) photodiodes in silicon photonics.
- Coupling between chip and fibre. A grating over or under a waveguide can allow specific wavelengths to couple the waveguide if it is injected with the correct angle. This allows the coupling of light from the top of chip. An alternative is to use edge coupling where the fibre is coupled in the same plane as the waveguide, usually with the help of V-grooves to approximate the fibre. Other methods are available, but they are mainly combinations of the two previous ones. It is an important choice, since it will affect the packaging of the chip.

Additionally, the generation of random strings of information is required, for which several integrated alternatives are already available [47–50], allowing the combination of CV-QKD devices and QRNG.

### 6.2.1 Additional considerations

When considering polarization, integrated devices tend to have different performances with transverse electric (TE) and transverse magnetic (TM) polarizations, and in general they are restricted to only one of the two (typically TE). For applications like CV-QKD where the polarization before the interference at the detector is not controlled, it is possible to use a coupler and splitter that admits TE/TM at the input and outputs two spatially separated TE modes after the rotation of the TM input[35] . The rest of the operations can be performed in TE mode.

The packaging [106] of the system is one of the most important steps of the process, since it will simplify the test of the device and it is fundamental towards the commercialization. The design can condition the possible package and vice versa. In the case of PICs that need to communicate light with the exterior the optical packaging is one of the more time consuming and costly parts.

## 6.3 Development of a PIC

A PIC can be produced in small scales in a clean room or at larger scales in a commercial foundry. Foundries usually have more advanced technological processes than research lab clean rooms and can sell a portion on the wafer for the implementation of the client's design. The typical life cycle of a chip is illustrated in figure 6.1, that corresponds to the steps and players involved in the development of the chips that we will describe in the next chapter.

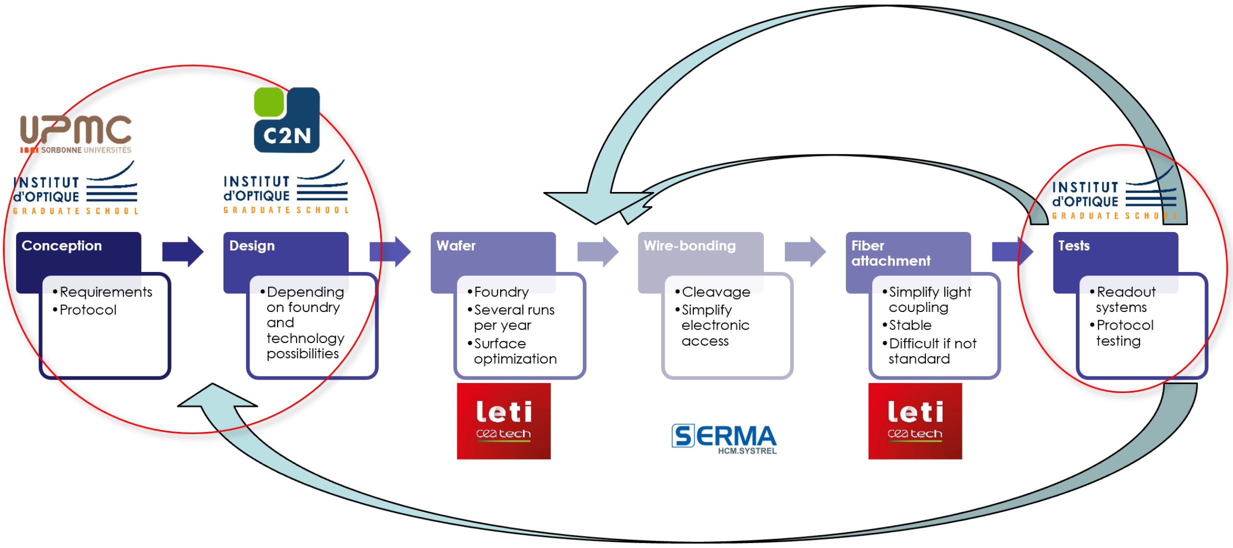

UPMC SORBONNE UNIVERSITÉS
INSTITUT d'OPTIQUE GRADUATE SCHOOL
C2N
INSTITUT d'OPTIQUE GRADUATE SCHOOL
INSTITUT d'OPTIQUE GRADUATE SCHOOL
Conception
• Requirements
• Protocol
Design
• Depending on foundry and technology possibilities
Wafer
• Foundry
• Several runs per year
• Surface optimization
Wire-bonding
• Cleavage
• Simplify electronic access
Fiber attachment
• Simplify light coupling
• Stable
• Difficult if not standard
Tests
• Readout systems
• Protocol testing
leti ceatech
SERMA HCM.SYSTREL
leti ceatech

**Figure 6.1:** Typical life cycle of a chip. Unsatisfactory results may lead to the repetition of some steps. In our case it happened after some defective packages (arrows on top). The worst case would be the requirement to redesign the chip (lower arrow).

The design can be done directly using the design tools that will determine the required shape for a particular function, or more practically using the process design kit (PDK) provided by the foundry. The PDK usually contains a list with the most commonly used elements and their characteristics. Based on the requirements and the previous experience, the designer can decide to use the elements in the PDK or develop new ones and link them in order to have a properly connected circuit fulfilling the desired function.

We will use the concepts described previously to evaluate the performance of CV-QKD protocols using a 180° hybrid on silicon in the next chapter.

[35] This is typical in ICR and implies that the efficiencies of the two input polarizations will not be homogeneous.

# Experimental evaluation of on-chip coherent detector 7

7.1 Description of the device under test . . . . . . . . . . . . . . . . . . 87
Development sequence . . . 87
Test types . . . . . . . . . . . 89
Alice . . . . . . . . . . . . . . 90
7.2 Description of the set up . . 92
Frame structure . . . . . . . . 96
Feedback control . . . . . . . 96
7.3 Results . . . . . . . . . . . . 100
Detection efficiency . . . . 100
Electronic noise . . . . . . . 101
Shot noise and clearance . 102
Estimating $V_A$ . . . . . . . . 104
Protocol performance . . . 105
Achievable secret key rates 110
7.4 Conclusions . . . . . . . . . 112

In this chapter we analyse a 180° hybrid with two photodiodes in a balanced configuration integrated in a silicon photonics chip. The characteristics of the device under test (DUT) are described, as well as the packaging process. We propose an experimental set up to test the performance of the DUT under CV-QKD conditions assuming Gaussian modulation of the states, for which the results are commented before finishing with the conclusions.

## 7.1 Description of the device under test

Bulk fibre 180° hybrids are composed of a 2 by 2 beam splitter and typically two photodiodes in balanced configuration. An amplification is required in order to bring the signal to practical readable values and variable optical attenuators (VOA) might be needed between the outputs of the beam splitters and the photodetectors. The VOAs can be used to balance the detection reducing one of the beam splitter outputs in order to improve the common mode rejection ratio (CMRR).

Bulk coherent detectors have been successfully used in CV-QKD systems and the original idea when designing an on-chip detector was to substitute the optical part of the bulk detector, i.e. the beam splitter, the VOAs and the photodetectors. The electronic amplifier is at this step external to the chip, but it could be potentially integrated on chip in future evolutions of the concept, since silicon photonics is compatible with CMOS technology. An even more ambitious target would be the integration of the logical control as well.

The DUT is a 180° hybrid that has been designed with the purpose of reducing the cost and size with respect to the components used in bulk detector systems. CV-QKD implementations like [76] where the signal and the LO operate at the same frequency $\omega_{\text{IL}} = 0$, were the first target. These implementations operate in pulsed regime, and can profit from the use of charge amplifiers, so the test concepts in this chapter were developed under these assumptions.

The layout of the device is illustrated in figure 7.1 alongside with a microscopic photo of one of the units before packaging.

### 7.1.1 Development sequence

The design of the 180° hybrid, along with other elements relevant for CV-QKD like a 90° hybrid and two alternative versions of Alice, have been done in collaboration with the silicon photonics group (MINAPHOT) at the Center for Nanoscience and Nanotechnology

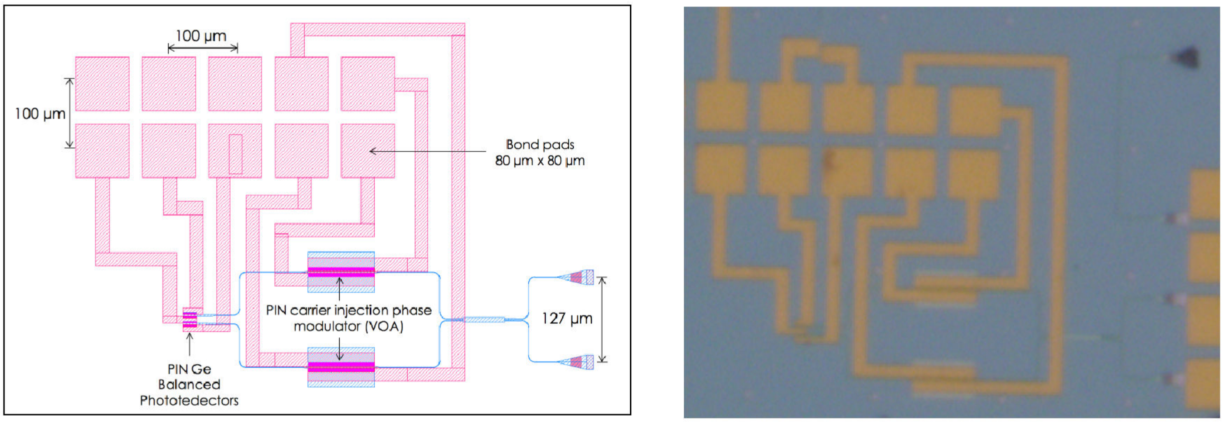


**Figure 7.1:** On-chip 180° hybrid detector layout and microscopic photo before packaging. The optical parts are indicated in blue in the layout of the left figure. The electronic contacts and tracks are clearly the elements occupying most of the surface.

(C2N). The layout of the different components was repeated over a section of the wafer that was fabricated at CEA LETI (Grenoble).

After several technically satisfactory but impractical initial tests using manual electronic probes and fibre couplers, a support using a mezzanine PCB (figure 7.2) was designed to hold one device and facilitate the testing procedure. A single mother board PCB (figure 7.3) acting as amplification chain was designed and constructed to be able to accept one mezzanine PCB. This provides a cost effective way to test multiple devices, since the only requirement is the construction of a small mezzanine PCB with passive components and the packaging of the PIC.

The electronic packaging of the chips (wire-bonding between the electronic pads on the PIC and the contacts of the mezzanine PCB) was performed at Serma Systrel (currently Serma Microelectronics). This is a well known process in the electronics industry and can be performed at competitive commercial cost if mass produced[37] .

The electronic packaging simplified the tests, but the light coupling was still manual, using precise micrometers to couple the signal and LO light arriving from a two channel fibre array into two grating couplers. In order to increase the repeatability of the results we packaged some units optically. The optical packaging consists in fixing fibres (typically a fibre array) to the PIC in a permanent position. It is desirable that the position maximizes the coupling of light between the fibre and the chip, and in the case of the detector the current of the photodiodes can be used as a reference. A known optical power is injected into one of the fibre inputs and following an iterative positioning method the coupling is maximized. In the optimal position a special glue is applied and after the drying process the chip is ready to be used, using the attached fibres as light interface and the mezzanine PCB connectors as electronic interface. At the time of writing the technology to perform the fibre attachment was more time consuming and costly than the electronic packaging, hence a potential bottleneck for the development of the PIC industry.

The electronic packaging has evolved during the project, but the results

[37] The particularity of PICs is that if light needs to enter or exit the chip a photonic access needs to be provided and the packaging cannot be completely closed as it is typical in electronics. This produced some problems in our case, since the fibre arrays needed to be custom made in order to access the reduced physical space available for the optical couplers.

in the following sections only relate to the final version, with complete electronic and optical packaging.

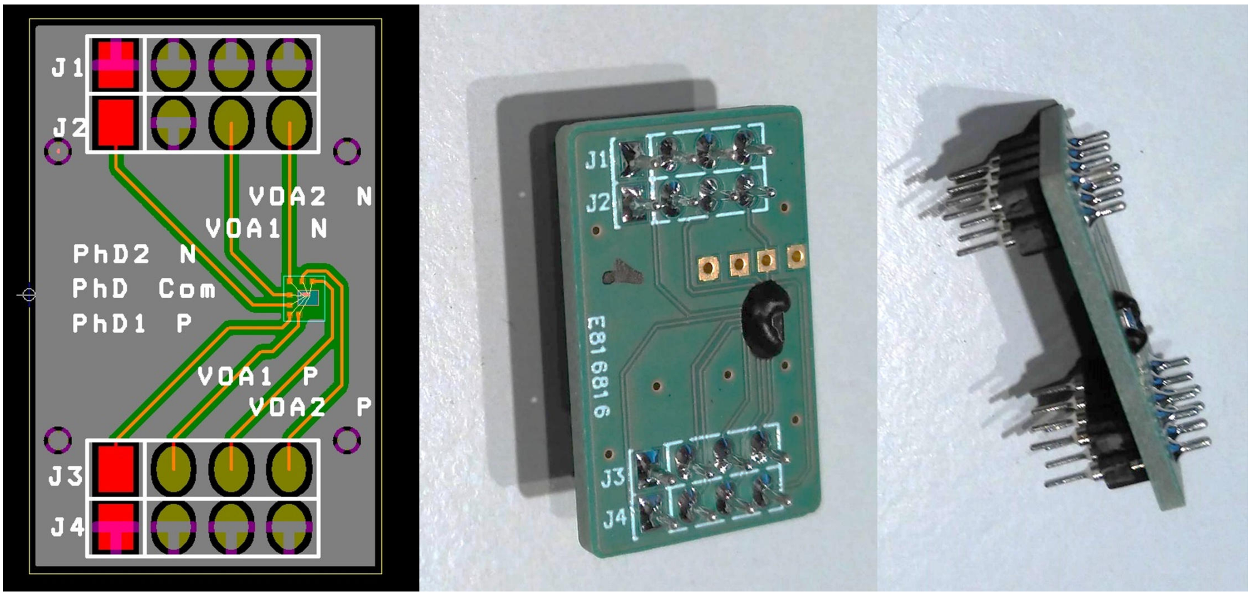


**Figure 7.2:** Mezzanine PCB layout and final result. The layout is represented on the left, with the labels of the seven signals of interest. The small blue rectangle indicates the position of the PIC. Two photographs of the mezzanine after wire-bonding with the chip barely visible under the black resin.

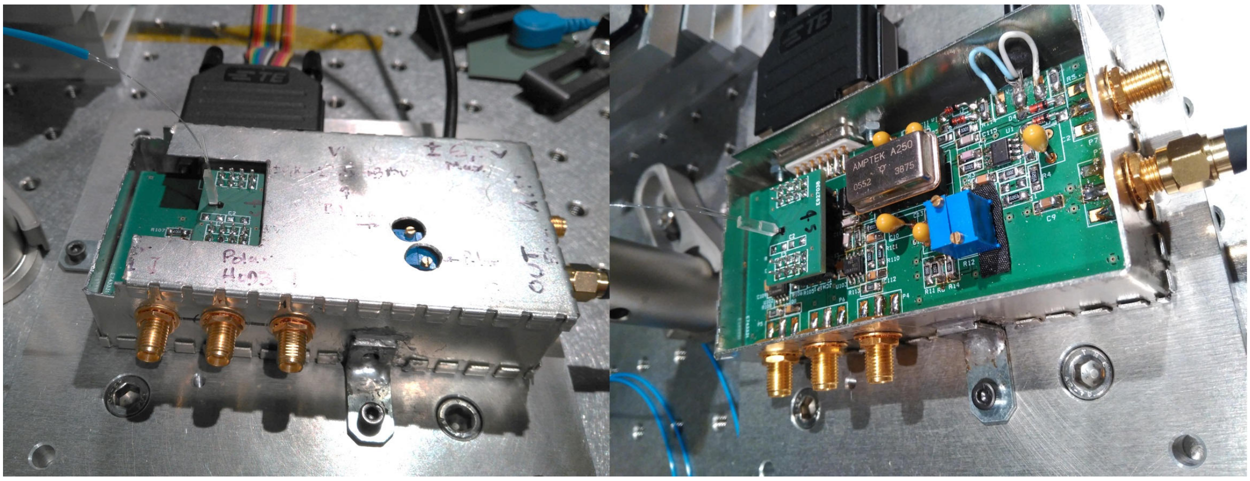


**Figure 7.3:** Mother board with inserted mezzanine board. A mezzanine PCB with the fibre attached is situated in the socket of the mother PCB. During operation the system is shielded due to the high sensitivity of the charge amplifier. In the right figure the charge amplifier is labelled as Amptek 250. The final output is the connected SMA port and the control of the VOAs is performed through the planar cable.

## 7.1.2 Test types

The DUT is a coherent detector with a 180° hybrid with two germanium photodiodes in balanced configuration. Different types of measurements can be performed in order to estimate the performance, but the final target is to be able to perform secret key exchange using the DUT. Some parameters cannot be determined practically during the execution of the protocol, and need to be estimated beforehand. We will name dynamic measurements those that are performed during the execution of the protocol and static measurements otherwise.

- ▶ **Static measurements** are those performed under special conditions. More details about the procedure will be given when discussing the results in section 7.3, but the most relevant parameters that can be determined independently of the protocol execution are:
  - The detection efficiency $\eta$.
  - The electronic noise $V_{\mathrm{el}}$.
  - The shot noise $N_0$.
- ▶ **Dynamic measurements** allow estimation of the statistics when Alice and Bob are communicating. The relevant parameters are:
  - Alice's variance $V_A$.
  - The channel transmittance $T$.
  - The channel excess noise $\xi$.

The conversion factor between Alice's and Bob's units $\gamma_A$ can be considered a special dynamic measurement since it is performed dynamically but not during the standard protocol operation. More details will be given in section 7.3.4.

The previous parameters, along with the reconciliation efficiency $\beta$, give all the information required to calculate the key. The possibility of executing the GG02 protocol until the parameter estimation and obtaining parameters compatible with the generation of key will be the main benchmark to evaluate the performance of the DUT. Bob's optical tasks are performed by the evaluated device, but an Alice is required in order to implement GG02 protocol. We discuss the alternatives and relevant points concerning Alice in the next subsection.

The simple characterization of the parameters relevant for CV-QKD might not be enough in order to improve the system in future iterations. Impairments on those parameters can have different sources, and it is important to identify the most relevant in order to improve the performance. The DUT is not tested under perfect environmental conditions (no temperature control is implemented) and the surrounding equipment (bulk Alice, amplifier...) might be imperfect. This leads to more realistic conditions if the generation of key is the benchmark, but to less strict conditions if the characterization of the device is the target. We are mainly interested in the application so we focused on the first approach but without losing sight of the second.

### 7.1.3 Alice

A system performing the functions of Alice needs to be implemented in order to test the detector dynamically. The selected option in this case was a set of bulk components performing the modulation, attenuation and splitting of the involved signals. An IQ modulator or an equivalent combination of amplitude and phase modulators could be used. We decided to implement it with amplitude and phase modulators in order to simplify the future tests of the PIC version of Alice, displayed in figure 7.4, that is designed using Mach-Zehnder interferometers in amplitude and phase configuration.

Since the integration of a laser inside the PIC is impractical in silicon photonic systems at the wavelengths of interest, the modulators are the most relevant component of the architecture of Alice. Modulators covering the whole phase space require the control of three bias parameters per polarization (we will only use one polarization in this chapter), and the environmental conditions might cause a drift on those values that needs to be compensated. This is true for high rate lithium niobate modulators, and for other Mach-Zehnder based architectures, where these parameters are typically controlled by a modulation controller that automates the process. Electro-optic modulators normally have two inputs depending on the applied frequency (RF and DC) and modulation controllers work in most cases applying a *dither* low frequency (in the order of kHz) amplitude modulation on the DC. The dither allows the characterization of modulation parameters and actuation on the bias, but it modulates the signal in amplitude. In high rate systems the dither at few kHz is negligible, but in lower rate systems it can be problematic and interfere with the proper functionality.

Commercial modulation controllers are prepared for bulk electro-optical modulators, where the devices do not suffer interference from other functionalities. The processes involved in the modulation of light in silicon photonics chips might not have the transfer functions as a function of the voltage expected by the commercial modulation controllers.

As the rates targeted in the set up are quite low (around 1 MBd), and anticipating the necessity of calibrating on-chip modulators in future tests, we have decided to implement a modulator controller mechanism.

- Inclusion of feedback mechanisms in Alice in order to calibrate her modulators. As phase is involved a coherent detection mechanism is required, a 180° hybrid being the simplest alternative. The LO can be obtained from the same laser source and $\omega_{\mathrm{IL}} = 0$ Hz, simplifying the analysis further. The amplitude can be more accurately tracked using a photodiode, since it measures directly the intensity. Note that in both cases security is not required since we are assuming that this calibration occurs inside Alice's lab, so the average number of photons in the calibration can be adapted to have an arbitrarily good precision in the estimations. Note also that the proposed schemes are present in the PIC version of Alice.
- Anticipation of the feedback mechanism in the structure of symbols of the protocol. Symbols destined to the control of the modulators will be inserted in order to characterize them via the results of the feedback mechanism. Those symbols will only affect the protocol introducing an overhead of symbols not used for secret key generation.

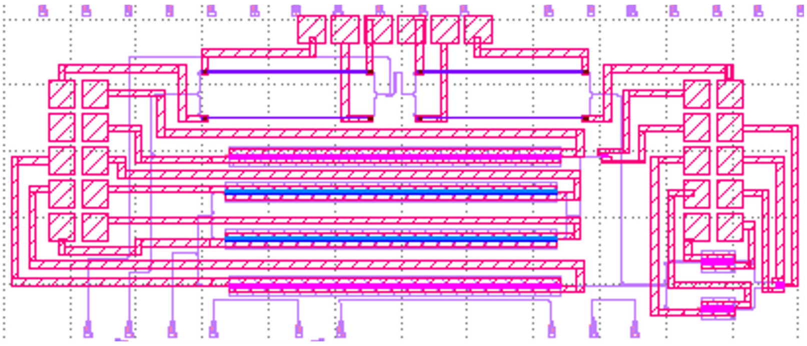


**Figure 7.4:** Layout for on-chip Alice with feedback system. The optical connections are located at the bottom, comprising input and outputs (final and control taps). The central part corresponds to the modulators while the right part is a coherent detector similar to the one in figure 7.1 that can be used for feedback.

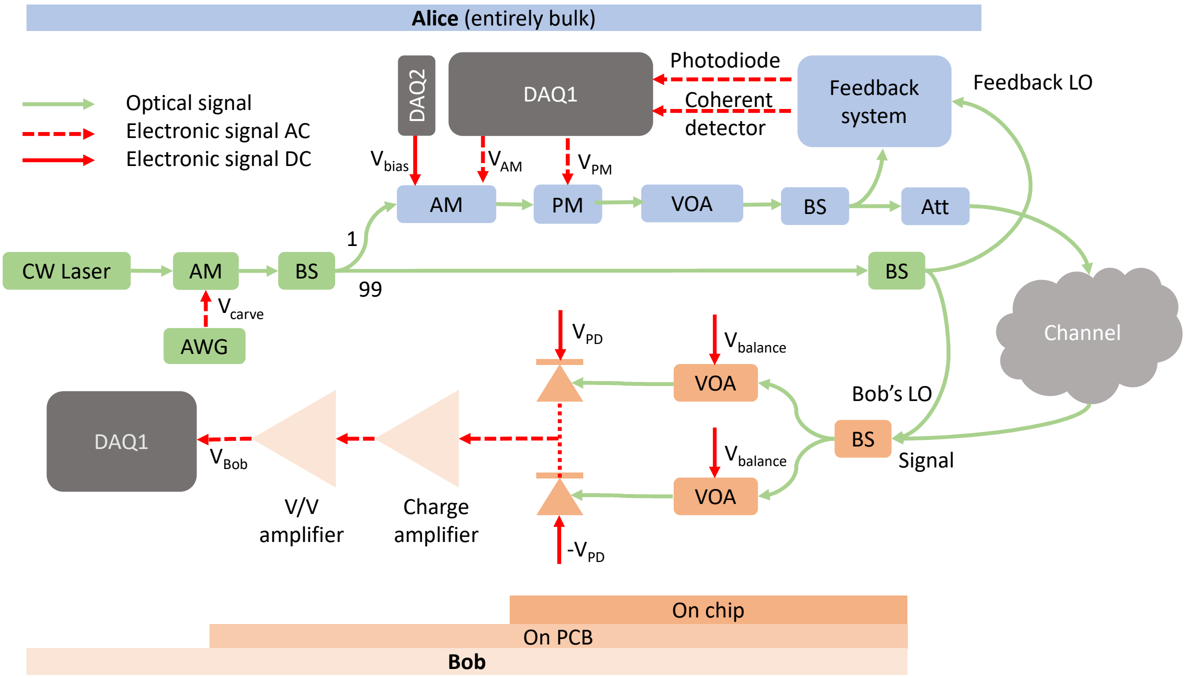


**Figure 7.5:** Scheme of the on-chip coherent detector set up. Alice is represented in blue and it is built using bulk components. Bob's components are painted in orange colors, the darker tones corresponding to the components inside the chip. The components shared by Alice and Bob in this set up are displayed in green.

## 7.2 Description of the set up

A scheme of the set up is illustrated in figure 7.5, representing all the elements required to run the protocol in dynamic mode. The static mode is a subset of the dynamic one disconnecting some of Bob's optical inputs. The individual components can be described as follows:

- **Light source.** Symbols are identified with separated pulses of constant repetition rate. Bob's LO uses the same source multiplexed in space using a beam splitter.
  - **Laser.** A Pure Photonics PPCL550 continuous wave (CW) laser is used as light source. The power is adapted so that

  it is sufficient for Alice's signal and feedback system and Bob's LO.
  - **Pulse carving.** The CW laser is carved into pulses by an iXblue MXER-LN-10 lithium niobate intensity modulator with 35 dB of extinction ratio. A voltage source controls the DC bias of the modulator.
  - **AWG.** The electronic signals to control the carving of the optical signal come from an arbitrary waveform generator (AWG) that generates a rectangular pulse. The repetition rate and pulse length is configurable but the results shown in this document are for 100 ns pulses separated by 1 $\mu$s. The AWG also generates the trigger pulse that synchronises the acquisition and generation of samples.
  - **BS.** An unbalanced beam splitter (99/1) separates the output of the intensity modulator between signal (1) and LO (99). The signal part will be modulated at Alice's and the LO part will be shared between Alice's feedback system and Bob.

- **Alice** is constructed using commercial bulk components. The acquisition and generation of signal is performed by specialized cards.
  - **Amplitude modulator (AM).** A lithium niobate EOSpace amplitude modulator changes the amplitude of each pulse according to the indications of the software. The DC input of the modulator is adjusted to operate at maximum extinction when no RF signal is applied.
  - **Phase modulator (PM).** A lithium niobate phase modulator changes the relative phase of each pulse according to the indications of the software.
  - **Variable optical attenuator (VOA).** A manual IDIL VOA is used to control the level of the output of Alice.
  - **Feedback mechanism.** Part of the signal at the output of the VOA is captured in order to obtain a feedback. The basic element is an unbalanced beam splitter that recovers most of the signal and can be used with two purposes: (1) estimate the optical power at the output of Alice, using the correct relation of factors between the measurements at this point and Alice's output, (2) use it as a reference signal for the calibration of the electro-optic modulators. Two types of calibration are performed:
    - A single photodiode is used to calibrate the amplitude modulator $V_\pi^{\text{AM}}$ and $V_{\text{bias}}^{\text{AM}}$.
    - A balanced detector is used to calibrate the $V_\pi^{\text{PM}}$ of the phase modulator. Part of the power needs to be used as LO in this case.
  - **Attenuator.** A fixed fibre attenuator is added to attenuate the signal to the quantum level.

- **Bob's** components are integrated in a PCB and the readout is performed with a digital acquisition card.
  - **PCB mother board** A home-made circuit board of approximately 12 x 5 cm is used to host the elements of the receiver.

    - **Photodiode polarization.** The voltage polarization of the PCB mother board is adjusted in order to provide a stable polarization voltage to the photodiodes (typically 2 V).
    - **PCB mezzanine for PIC**. The PIC is hosted by a 2 x 3 cm mezzanine PCB that handles the connection with the motherboard. Seven pins give access to the pads on the chip (three for the photodiodes in balanced configuration and two for each of the two VOAs).
    - **Charge amplifier.** The common point of the balanced detector is connected to the amplification chain. The first step consist in the accumulation of the charge in a capacitor during the duration of the pulse. The capacity is converted to voltage using an Amptek A250 charge amplifier.
    - **Voltage amplifier.** The output of the charge amplifier is conditioned to a readout voltage suitable for the acquisition system.

- **Control.** The acquisition and generation of data is performed with National Instruments (NI) digital acquisition cards (DAQ). Two units are used:
  - **DAQ1.** A NI PCI-6110 card is used as dynamic card. The DAC has a nominal resolution of 16 bits and a slew rate of 300 V/$\mu$s. The ADC has 12 bits of nominal resolution with a bandwidth of 4 MHz. The supported repetition rate combining inputs and outputs is 2.5 MSPS. The same card manages:
    - Alice's dynamic outputs controlling the amplitude and phase modulators. The electronic output power is sufficient to drive the electro-optic modulators without the use of an electronic amplifier.
    - Alice's dynamic inputs coming from the feedback system composed of a photodiode to calibrate the amplitude modulator and a balanced detector to calibrate the phase modulator.
    - Bob's measurement is acquired with a third input. This is enough for a 180° hybrid, but an additional input would be available if testing a 90° hybrid would be required.
  - **DAQ2.** The DC input of the AM is controlled by one analogue output of a NI USB-6363 card. The nominal DAC resolution is 16 bits with a sampling rate of 2.86 MSPS and a slew rate of 20 V/$\mu$s. The AM bias changes occur typically in the order of minutes, so this card is sufficient for the application. The reason to use an additional card is the insufficient number of outputs in the NI PCI-6110, limited to two.
  - **Synchronization.** The trigger to synchronize the system is distributed from the AWG to the trigger inputs of the acquisition cards. The electronic delay is set in order to optimize the readout of the detector, and due to the electronic delay

induced by the charge amplifier the same trigger can be used for the modulation outputs (see section 4.7 of [65] for more details).

- **Software.** The software runs in the same computer for practical purposes, but the functions of Alice and Bob are independent. The main functionalities related to the interaction with the hardware are the following:
  - **Alice's software.** For each symbol (pulse) two values of a two-dimensional Gaussian distribution are generated from a file of random uniform values. The values are converted to polar representation and adjusted to the properties of the modulators (see 7.2.2 for details) to obtain two values that are sent to the two DACs connected to the amplitude and phase modulator. The readings from the feedback components are measured in real time to maintain the modulators biased in optimal conditions.
  - **Bob's software.** At the reception of a triggering edge the acquisition system captures the value at the input and transfers it to the software. The symbols are stored until the sequence of symbols is completed.

The acquisition cards are controlled by a single computer and all the fibre components use polarization maintaining (PM) fibres. The limiting factor in the repetition rate is the bandwidth of the charge amplifier, which is able to work at rates between 0.5 and 2 MBd.

The set up is intended as a proof-of-principle experiment and some limitations need to be considered:

- The acquisition and generation of information is controlled by one computer for simplicity, but the processes are independent and could be separated in a commercial implementation.
- The unit under test does not have the phase modulation capabilities required to change the projection randomly as indicated by the GG02 protocol. This projection change is performed by Alice's phase modulator, introducing a $\pi/2$ shift in half of the symbols randomly. This method does not provide security for CV-QKD but allows the test of the detection capabilities in the same conditions. The DUT could be potentially used in a 180° hybrid heterodyne detection scheme that would not require the modulation of the phase.
- The same laser is used for Alice and Bob and the multiplexing is spacial using two different fibres. A more practical set up would require other multiplexing method.
- The polarization is manually controlled in the lab. An automatic mechanism would be required to operate autonomously under realistic channel conditions.

### 7.2.1 Frame structure

We group all the symbols required to obtain a string of secret key in an entity called frame. For practical reasons each frame is divided into $B$ blocks of equal number of symbols $N$. We have used three different types of blocks in the set up:

- Information blocks are the most numerous and contain:
  - Gaussian modulated symbols with variance $\sigma_G^2$. A configurable part of them will be randomly selected for parameter estimation.
  - Phase reference symbols with variance $\sigma_R^2$. The sequence is previously known by all entities and comprises values in a QPSK constellation. They will be used only to estimate the relative phase between Alice and Bob so it is interesting that $\sigma_R^2 > \sigma_G^2$ as they are not affected by security constrains, but they need to be kept within the dynamic range of the modulator and the detector.
  - Control symbols where the signal is completely attenuated can also be implemented but it is not used in the presented results[38] .
- AM calibration blocks, containing a range of voltage values applied only to the AM that will help to determine its instantaneous parameters.
- PM calibration blocks, that are similar to AM blocks but applied to the phase modulator. A voltage allowing the transmission of light needs to be applied in the AM as it is situated before the PM in the optical path.

The disposition of the block types is configurable and would depend mainly on the stability of the modulators. The ratio of information symbols to reference symbols can also be adapted to the channel conditions. The fraction of the symbols that will be revealed for parameter estimation is another configurable setting of the system.

A frame scheme is illustrated in figure 7.6 along with the typical information transmitted in each type of block. The block content is only schematic, since for practical reasons (to avoid the low frequency cut of the modulators mainly) the time indices inside the blocks are shuffled in order to obtain a signal without low frequencies.

### 7.2.2 Feedback control

The information blocks are stored at both Alice and Bob and processed after the end of the frame, only the feedback blocks are processed in real time[39] . As indicated earlier known symbols are transmitted by Alice in order to be read out by herself in the feedback detectors. The feedback involves the amplitude and phase modulators:

[38] It was implemented to calibrate $N_0$ dynamically under trusted conditions, but some excess noise might be present if the signal is not completely attenuated so its use was discarded.

[39] It would be also possible to do the processing of the information blocks in real time, but the available equipment was not able to perform this task sufficiently fast.

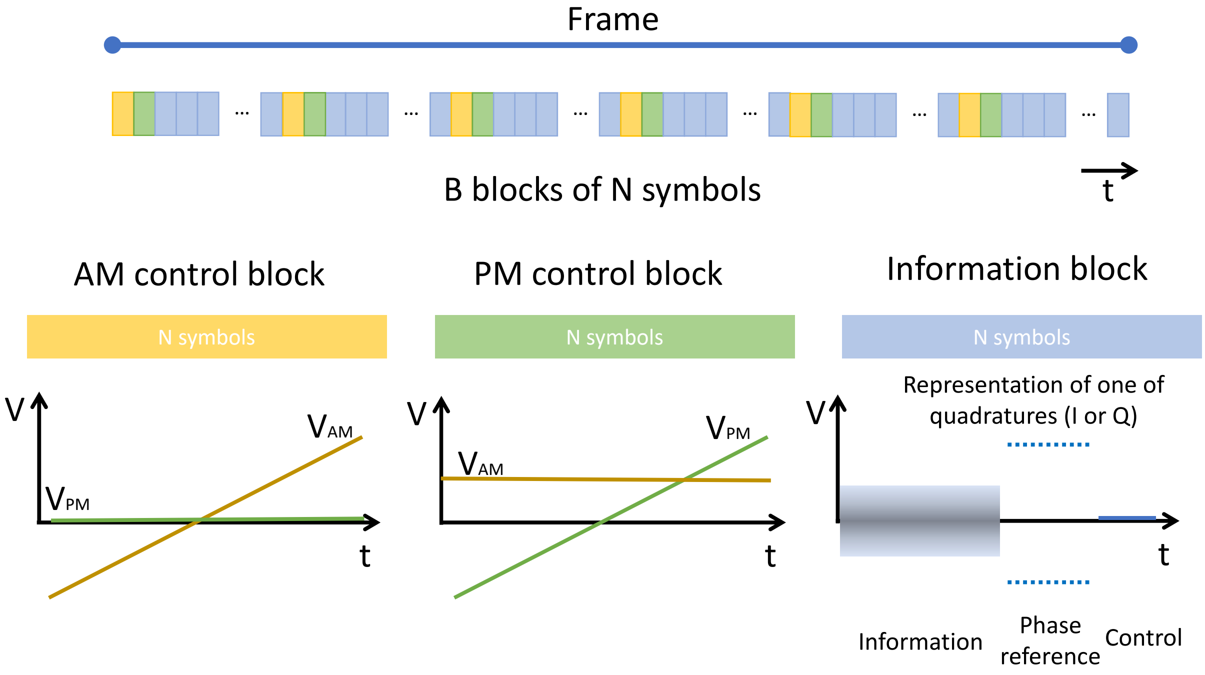


**Figure 7.6:** Frame structure: relation of frames, blocks and symbols. The symbols are represented in the block before the shuffling that would alter their time order. AM and PM blocks are represented directly in the output voltage while in the information block it is done in I (or Q) for clarity. The control sequence is not used in the results.

### Amplitude modulator

A uniform distribution of voltages in a range (a slope) is sent to the amplitude modulator conveniently shuffled in order to avoid too slow changes for the low frequency cut of the modulators (the repetition period is 1 $\mu$s and the low cut of lithium niobate modulators is in the order of kHz). The corresponding measures in the feedback photodiode of Alice are reordered and the typical sinusoidal transfer response of the Mach-Zehnder should appear, as can be seen in figure 7.7. The resulting points are fitted into a sinusoid whose frequency and phase can be related to $V^{AM}_{\pi,RF}$ and $V^{AM}_{\text{bias},RF}$ respectively. As the distribution is going to be Gaussian it is convenient to bias the AM to the maximum extinction point in order to modulate around this value. If a DC component $V^{AM}_{\text{bias},RF}$ would be introduced in the electronic modulation signal, the AC coupling would cancel its effect in the optical signal, so it needs to be applied in the DC port of the modulator. The bias voltage needed in the DC port is different than the corresponding one in the RF port, but an iterative approach can be followed increasing the DC voltage by the estimated $V^{AM}_{\text{bias},RF}$ as can be seen in the central plot of figure 7.9 where the purple squares represent the applied value in the DC port and the green circles the remaining offset in the RF port. It can be seen that after a short transition period the calibration of the AM becomes stable. As the estimates are inherently noisy it is convenient to perform a moving average of the result, as can be seen for $V_{\pi,\mathrm{RF}}^{\mathrm{AM}}$ in the uppermost trace of figure 7.9.

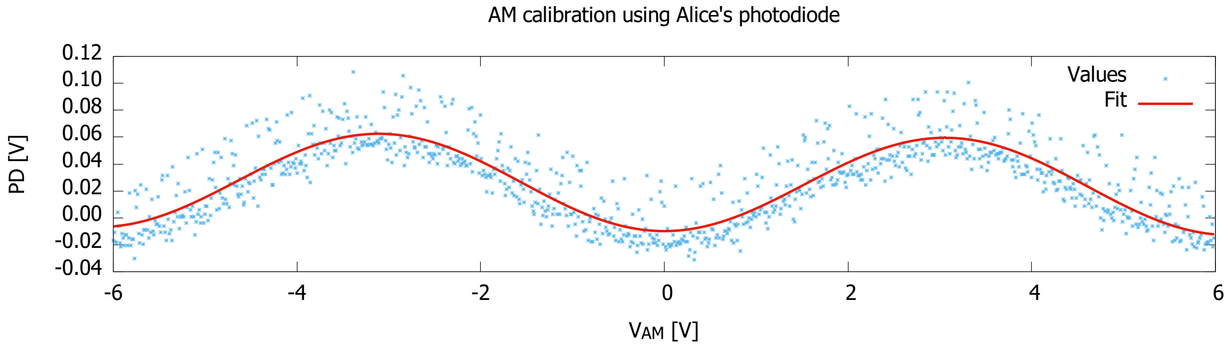


**Figure 7.7:** Calibration of amplitude modulator in one block. A uniform distribution of symbols is sent to the amplitude modulator and the results collected by the feedback photodiode. The results are fitted to four parameters (amplitude, frequency, phase and DC) in order to obtain $V_{\mathrm{bias,RF}}^{\mathrm{AM}}$ and $V_{\pi,\mathrm{RF}}^{\mathrm{AM}}$.

### Phase modulator

The phase modulator can also be parametrized by two values $V_{\pi,\mathrm{RF}}^{\mathrm{PM}}$ and $V_{\mathrm{bias,RF}}^{\mathrm{PM}}$, the second one being only a relative phase so we can omit it in the analysis as we have other mechanisms to estimate the relative phase at the receiver. $V_{\pi,\mathrm{RF}}^{\mathrm{PM}}$ will indicate the voltage that we need to apply in order to change the phase by $\pi$, so it is an important parameter to calibrate but it usually very stable, so a low number of PM blocks is required in practice. The AM located before the PM can also alter the phase so it needs to be taken into account. The AM is switched between two open positions at $\pm V_{\mathrm{open}}^{\mathrm{AM}}$ and a set of uniformly distributed voltages conveniently shuffled are applied to the PM with the results captured by the feedback coherent detector. The shuffled values can be inverted and the values categorized between $\pm V_{\mathrm{open}}$ to obtain results like the ones indicated in figure 7.8. An offset above the expected 180° can be observed and is taken into account on the PM voltage depending on the value of the AM voltage (if $V_{\mathrm{AM}}$ is positive an extra phase shift is applied). The evolution of the two obtained values (n and p) of $V_{\pi,\mathrm{RF}}^{\mathrm{PM}}$ is shown in the bottom plot of figure 7.9.

### Other considerations

The responses of the on-chip modulator of figure 7.4 could be completely different than the ones described for the lithium niobate modulators, but the same principles could be used. The basic idea is establishing a relation between the applied voltages and the corresponding optical response. The proposed feedback elements and the software are prepared to support other type of responses, which is not always the case for commercial modulator controllers based on signal dither.

An IQ modulator could be used instead of a set of amplitude and phase modulators. In this case also three values of interest would have been obtained, but the expected functions would have been different.

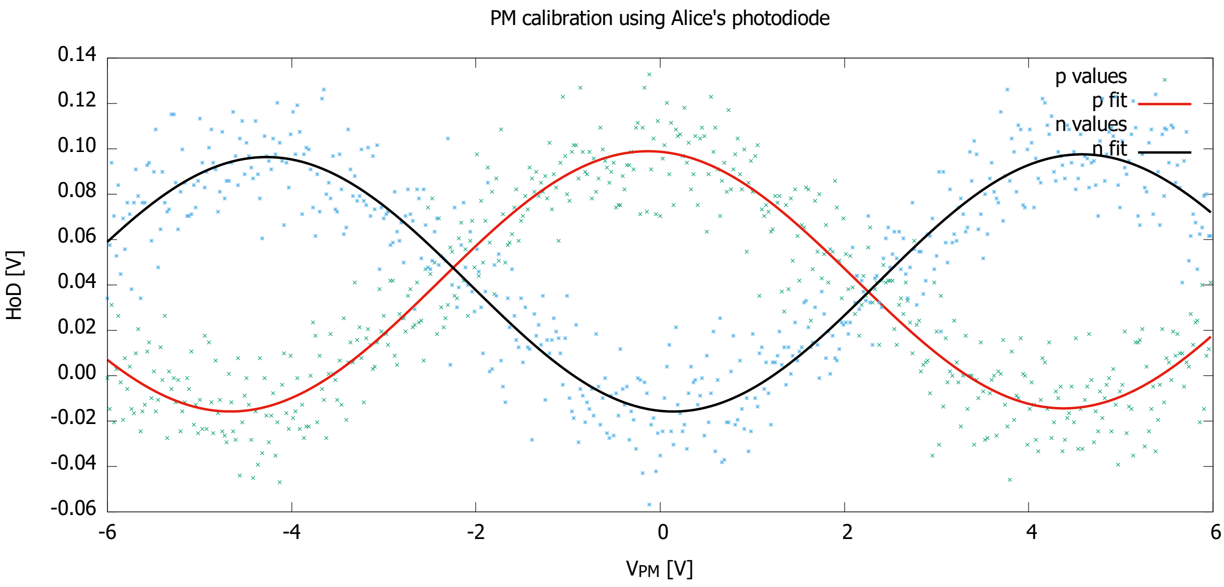


**Figure 7.8:** Calibration of phase modulator in one block. Two uniform distributions of symbols (n and p) are sent to the amplitude modulator and the results collected by the feedback coherent detector. The results are fitted to four parameters (amplitude, frequency, phase and DC) in order to obtain $V_{\mathrm{bias,RF}}^{\mathrm{PM}}$ and $V_{\pi,\mathrm{RF}}^{\mathrm{PM}}$ for each of the two distributions. Note that depending on the voltage point at which the detector is balanced the DC value might be different from zero.

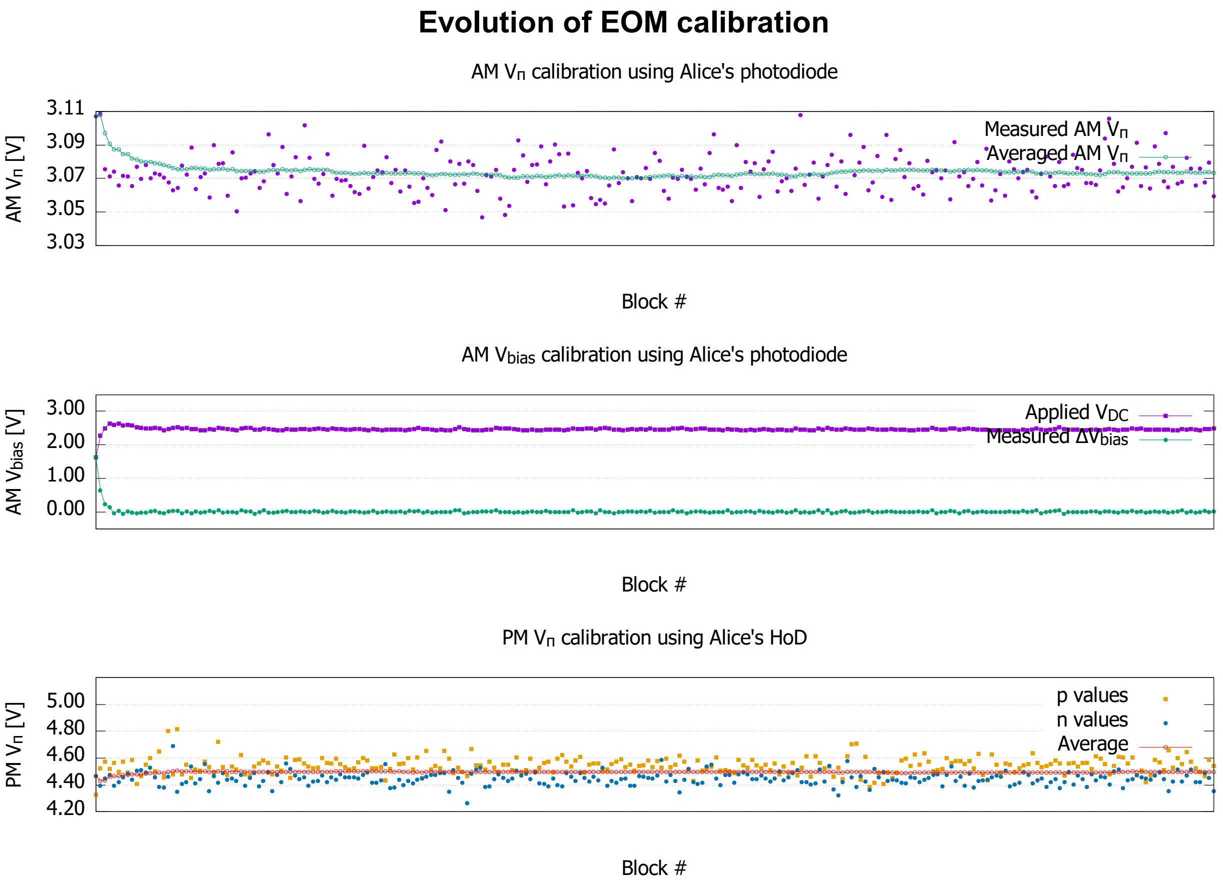


**Figure 7.9:** Evolution of the electro-optical modulator parameters during one frame. $V_{\pi,\mathrm{RF}}^{\mathrm{AM}}$ is displayed in the top, $V_{\mathrm{bias,RF}}^{\mathrm{AM}}$ in the center and $V_{\pi,\mathrm{RF}}^{\mathrm{PM}}$ in the bottom. The center also displays the applied voltage to the DC port of the AM. The results correspond to typical lithium niobate parameters.

## 7.3 Results

The current section comments the results obtained for one unit of 180° hybrid detector using an Alice composed of bulk components.

### 7.3.1 Detection efficiency

The most practical way to estimate the detection efficiency is to measure the photocurrent response to the input light in the photodiodes. The PCB with the charge amplifier is not well suited to this task, so the measurements have been performed during the fibre attachment process, since the same methodology is used in order to optimize the location of the fibre before the fixation. The coupling efficiency is highly dependent on the wavelength, so a sweep along a certain range is usually performed.

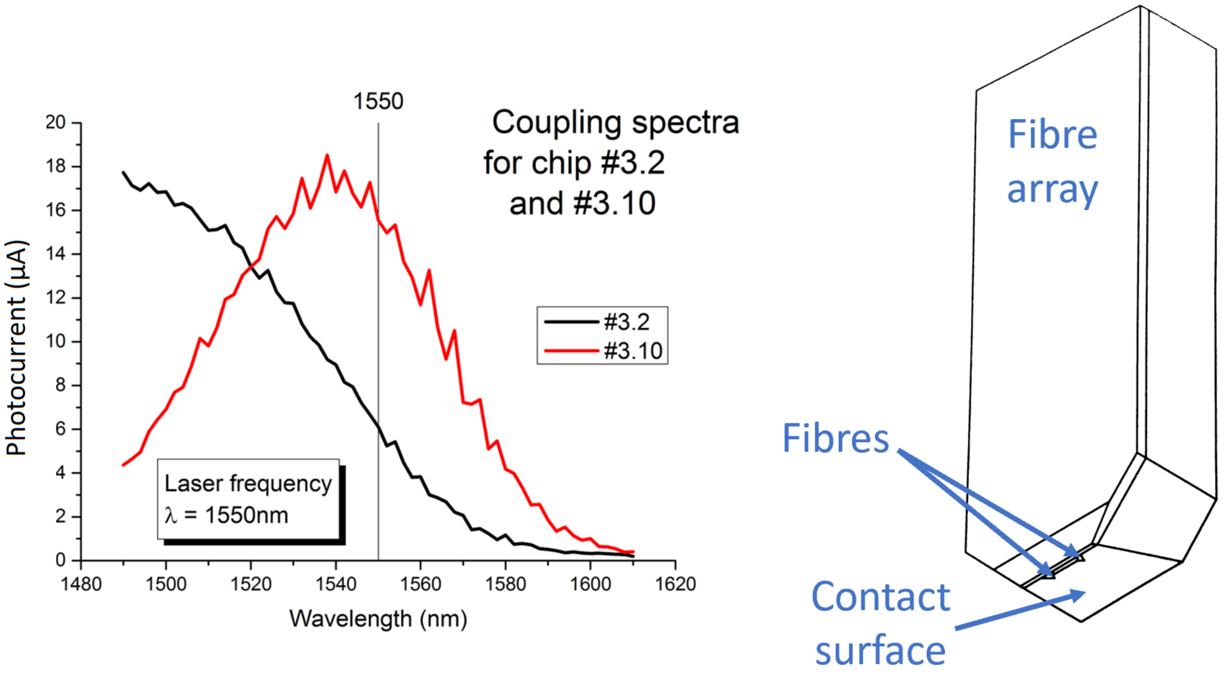


**Figure 7.10:** Efficiency as a function of the wavelength and fibre array scheme. Left: the aggregated measured photocurrent for two optically packaged chips as a function of the wavelength. Right: a scheme of the custom two channel fibre array and the indication of the contact surface.

The space available for the optical coupling after the wire-bonding is very reduced, and standard fibre arrays would not fit correctly in order to fix them to the chip during the fibre attachment. For this reason it was necessary to order custom fibre arrays with an adequate shape, as can be seen in the right part of figure 7.10, where the custom part corresponds to the edging on the sides. The angle of the fibres with the contact surface should be adapted to the design of the grating couplers. Even in standard arrays it is usually available in steps of 1° or less so it should have not posed any problem, but due to a misunderstanding at the time of ordering the fibre arrays, the angle did not match the optimal angle for the grating couplers (11° instead of 8°). This mismatch results in a lower efficiency than expected, as can be seen in the black trace of figure 7.10.

As the mistake was noticed new arrays were ordered and new packages were made, this time obtaining better efficiencies at the wavelengths of interest, as shown by the red curve of figure 7.10. The shown photocurrent values correspond to the added contribution of both diodes. If we separate the two photocurrents and we inject the light alternatively in the two fibre inputs we obtain the values of table 7.1, where *t* and *r* denote the transmission and reflection coefficients of the beam splitter.

| **Input A** | **Input B** | **Diode 1** | **Diode 2** | **t/r** |
|---|---|---|---|---|
| 460 $\mu$W | 0 $\mu$W | 5.3 $\mu$A | 4.0 $\mu$A | 56.6/43.4 |
| 0 $\mu$W | 460 $\mu$W | 4.0 $\mu$A | 5.2 $\mu$A | 56.5/43.5 |

**Table 7.1:** Measured current response for each photodiode as a function of input light in each of the ports.

The measurements give a best value for the global efficiency of 9.3/460 = 0.0202, but this does not count the fact that the system needs to be balanced, so after the action of the VOA in the higher beam splitter output a realistic value for the efficiency is 8/460 = 0.0174 (17.7 dB of attenuation). This efficiency value has improved with respect to the initial defective coupling angle but it is still very low.

The corresponding fibre coupling efficiency is studied in section 7.3.1.1 of [66] assuming typical parameters for the components of the system (1 dB of coupling loss into the beam splitter and photodiodes with a responsivity of 1 A/W) and the resulting losses due the coupling between the fibre array and the chip sum up to 15.7 dB (0.0272), much higher than the 3 to 8 dB of losses expected from a grating coupler.

A more careful analysis on unpackaged dice still available on the remaining wafer pointed out that some sections of the wafer provided responsivities much lower than the expected 1 A/W, probably due to an error in the fabrication. Unfortunately the packaged dice belong to the defective sections of the wafer. A new packaging process could have been started but it was discarded due to the high delay that it would imply[40] . We decided to continue testing the chips, since using the trusted detector assumptions the effects of a low efficiency detector could be mitigated. We will see in the next sections that even if in theory the efficiency has only a linear effect in the SKR, it will affect the estimation of other critical parameters.

### 7.3.2 Electronic noise

The main source of what we denote as electronic noise is the thermal noise due to finite temperature of the set up. This thermal noise is amplified through the gain chain and read out by the acquisition card, that digitizes the analogue signal introducing also quantization errors. These quantization errors, as well as the noise introduced in the amplification chain will compose the electronic noise.

A possible way to characterize the electronic noise is to switch on the device and, without applying any optical inputs, calculate the

[40] The electronic packaging could be relatively fast, since it only requires the fabrication of new mezzanine PCBs and its wire-bonding. The optical packaging would be more troublesome, since the provider of custom fibre arrays had long delay terms and the fibre attachment facilities were not easily available.

power spectral density (PSD) with a spectrum analyser. This is a valid way, but as we are going to work in a pulsed regime and with a charge amplifier it is more practical to estimate the integrated value directly, i.e. sample at the symbol rate and calculate the variance over a representative number of symbols. This is the method used in this chapter.

A subtle but important consideration that needs to be taken before proceeding to the electronic noise estimation relates to the detection balance. As discussed earlier, the beam splitter is not perfect and a VOA needs to be used to attenuate one of the photodiode inputs. The VOAs are implemented using thermal actuators that will consume certain electronic power, requiring the dissipation of this heat through the chip. In our case the typical values approach 15 mW of electronic power dissipated in the mezzanine PCB, which might produce some undesirable heating on a chip of such small size. We noted that the electronic noise increases right after the balancing adjustments to achieve a stable value after a few minutes. All the measurements were done after this transition regime.

A typical evolution of the estimated electronic noise during 10 seconds is illustrated in figure 7.11. In the trusted detector scenario, a lower bound of the estimator needs to be used in order to guarantee security, but in order to avoid the overestimation of the excess noise the lower bound on the electronic noise should be as tight as possible to the real value. In the results we can see margins of around 1% of the average value in the confidence intervals.

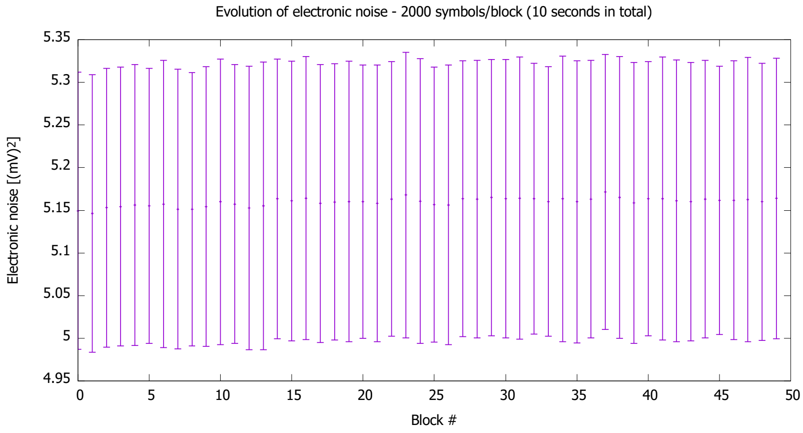


**Figure 7.11:** Evolution of the electronic noise during 10 seconds. The indicated error bars represent the standard deviations obtained for each individual block of 2000 symbols.

### 7.3.3 Shot noise and clearance

A similar procedure can be used to estimate the shot noise. In this case the measured value will correspond to the sum of electronic noise and shot noise, but assuming they are independent the shot noise can be calculated subtracting the previously estimated electronic noise to the recent estimation. Typical results can be observed in figure 7.12 and the confidence interval also fluctuates in the order of 1 to 2 percent of the average shot noise value.

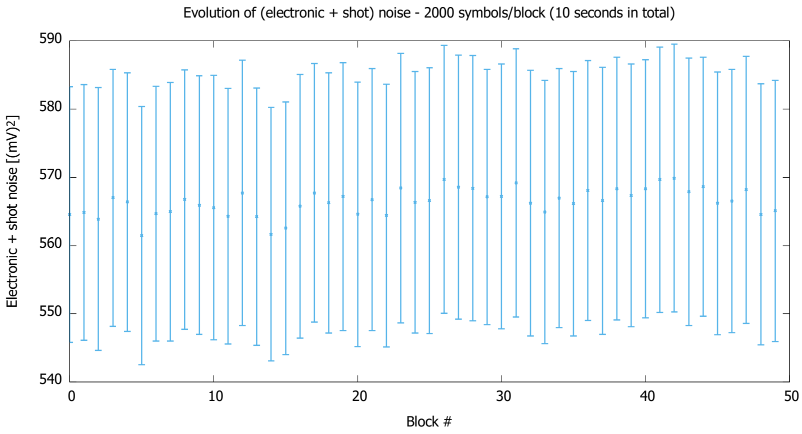


**Figure 7.12:** Evolution of the shot noise plus electronic noise during 10 seconds. The indicated error bars represent the standard deviations obtained for each individual block of 2000 symbols.

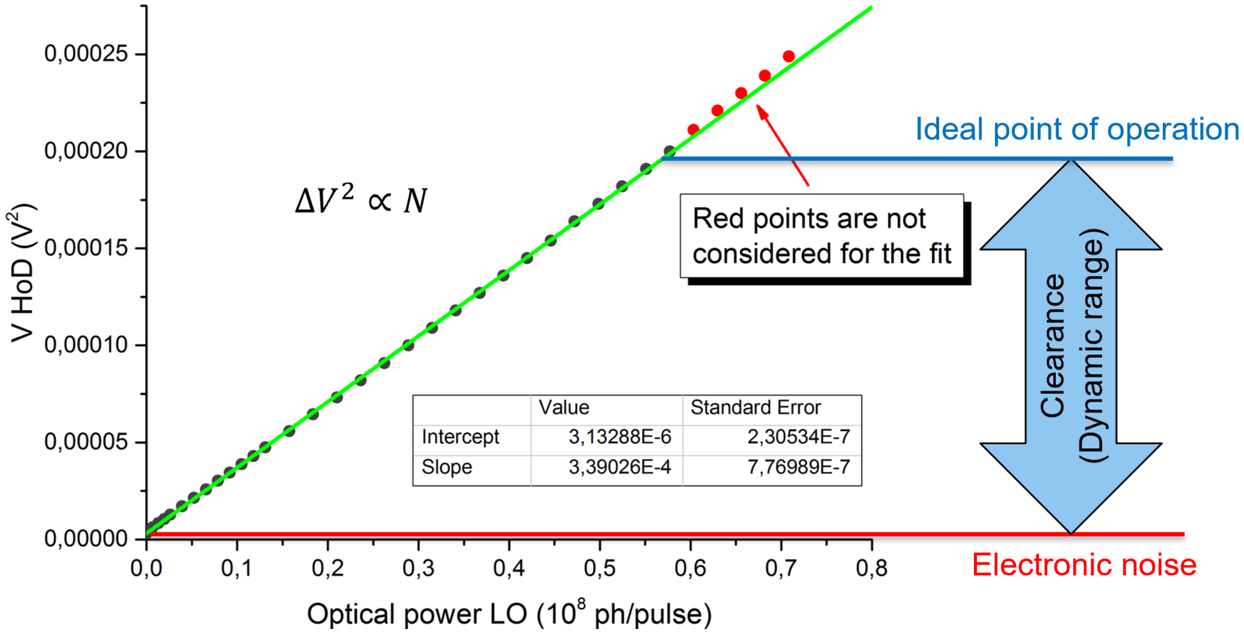
All the variances are normalized to shot noise units using the average value so the lack of a more precise estimation of the shot noise will also spread the confidence intervals of the other parameters. In particular it will lower bound the estimation of the excess noise, as the value estimated at the detector $\xi_{\text{Bob}}$ can be calculated from the expression

$$\xi_{\text{Bob}} = \sigma_B^2 - \eta T V_A + 1 + V_{\text{el}} \tag{7.1}$$

The shot noise estimation can be improved tracking more closely its evolution, similar to what is done in [76] as a countermeasure for side channel attacks. In that set up an amplitude modulator is used to randomly cut the incoming signal and estimate the shot noise during the protocol execution. In our case, if we assume that the LO fibre is not attacked we would not need to randomly switch off the signal and we could establish periods of shot noise calibration during the execution of the protocol to reduce the uncertainty of the average value. The on-chip device is not prepared to perform this operation so an external switch would be required. Switches, especially lithium niobate ones, introduce additional insertion loss reducing even further the overall detection efficiency, so a micro-electro-mechanical switch was selected for the task. The switching times for these devices are in the order of the ms, insufficient for symbol discrimination like in [76], but enough for regular calibration of blocks of symbols. For multiple not scientific related reasons the implementation could not be completed in time for this manuscript.

The results shown in the following sections are based on the estimations of the shot noise done seconds before the execution of the set up in protocol mode. The uncertainty of this method is higher, so the estimated parameters are more pessimistic that they would be with a more controlled set up. In any case, for the sake of providing a simple solution, we decided to venture on a system without temperature control or advanced calibration mechanisms.

The ratio between the shot noise and electronic noise is denominated clearance, and it is desirable that it is as high as possible. An increase in the LO power would improve the clearance, since the electronic noise is assumed to be independent of the LO power, but non linearity effects can occur if the LO power achieves certain values. The detectors might saturate or classical noise may appear as more relevant. For this reason it is important to plot the measured detector variance (without signal input) as a function of the LO power. The results are shown in figure 7.13 and it can be seen that for high LO powers the measured variance no longer fits a linear curve. The highest power that maintains a linear relation indicates the ideal point of operation.



| | Value | Standard Error |
|---|---|---|
| Intercept | 3,13288E-6 | 2,30534E-7 |
| Slope | 3,39026E-4 | 7,76989E-7 |

**Figure 7.13:** Shot noise as a function of the LO power and clearance. The bottom red line represents the electronic noise and the top red points represent the points discarded in the green linear fit.

### 7.3.4 Estimating $V_A$

The estimation of $V_A$ is performed in the electronic domain, comparing the results of Alice's variance in her units with the variance measured at Bob's in his units. As the units are not the same (typically a.u. for Alice and $V^2$ for Bob) a conversion factor $\gamma_A$ is required. It can be obtained tracing Bob's variance against Alice's variance and calculating the slope of the curve.

An alternative to the previous estimation method is the estimation of the average photon number at Alice's output. This can be done measuring the optical power at the input of the channel and relating it to the units used by the software of Alice. As the signal is pulsed and not all the symbols will be used in the protocol (reference symbols with have more average energy than the quantum ones), it would be necessary to relate the average measured power to the energy per quantum symbol. If $E_{\text{ref}}$ and $E_{\text{q}}$ are the average energies of the reference and quantum symbols respectively, and $N_{\text{ref}}$ and $N_{\text{q}}$ are the average number of reference and quantum symbols per time unit, then the average power corresponds to

$$P = E_{\mathrm{ref}} N_{\mathrm{ref}} + E_{\mathrm{q}} N_{\mathrm{q}} \tag{7.2}$$

$E_{\mathrm{q}}$ (and consequently $V_A$) can be estimated from the measurement of $P$ and the known relations $E_{\mathrm{ref}}/E_{\mathrm{q}}$ and $N_{\mathrm{ref}}/N_{\mathrm{q}}$.

### 7.3.5 Protocol performance

Once the parameters $N_0$, $V_{\mathrm{el}}$ and $\gamma_A$ are estimated it is possible to run the protocol. The results for a typical frame in a back-to-back (B2B) set up are displayed in this section, all the figures corresponding to the same realization, in this case dividing the frame in 5000 blocks of 2000 symbols each. The length of the frame has been reduced to 10 s ($10^7$ symbols) in order to simplify the figures, but typically $10^9$ symbols are required in the parameter estimation part in order to neglect the finite key effects.

The symbols composing the frame are modulated by Alice and received by Alice's feedback and Bob's receiver on chip. The feedback symbols belonging to a control block are processed in real time by Alice, calibrating the modulators accordingly. The rest of the symbols are labelled and stored by Alice and Bob until the transmission of the frame is finished. The labelling includes information of the type of symbol (information or reference) and the randomly chosen projection (I or Q).

Once the frame is completed, Bob estimates the phase difference with Alice using reference symbols corresponding to a QPSK constellation. The rotation of the symbols at the detection will be used to estimate the phase drift but those values will be strongly affected by the shot noise. Two examples are shown in figure 7.14 depending on the level of reference signal arriving to the coherent detector. A phase estimate is obtained for each block, obtaining a raw phase estimation that evolves randomly in a similar way as illustrated in figure 7.15. Further processing can be applied to the estimation, the most straightforward being the low pass filtering of the estimation to smooth the results and obtain a more realistic phase evolution. An interpolation of this filtered phase at the level of symbol would also increase the precision, but in our case the drift is slow enough to be almost negligible at the level of a block. The estimated phase can then be used to shift the phase of Alice's symbols[41] and maintain the projection measured by Bob.

A configurable fraction of the information symbols is randomly assigned to parameter estimation purposes. The variance of these symbols is calculated both at Alice's and Bob's, giving $\sigma_G^2$ and $\sigma_B^2$ respectively. The normalized correlation $\rho$ between the symbols of Alice and Bob is calculated per block giving the results in pale blue in figure 7.16. The results are very noisy as expected from the fact of operating close to the shot noise level regime, but if we accumulate the results over the blocks along the frame (note that the first 200 blocks are discarded to avoid convergence issues during the calibration of the modulators) we

[41] It is easier to shift Alice's symbols, for which both quadratures are known, than Bob's, for which we know only one projection.

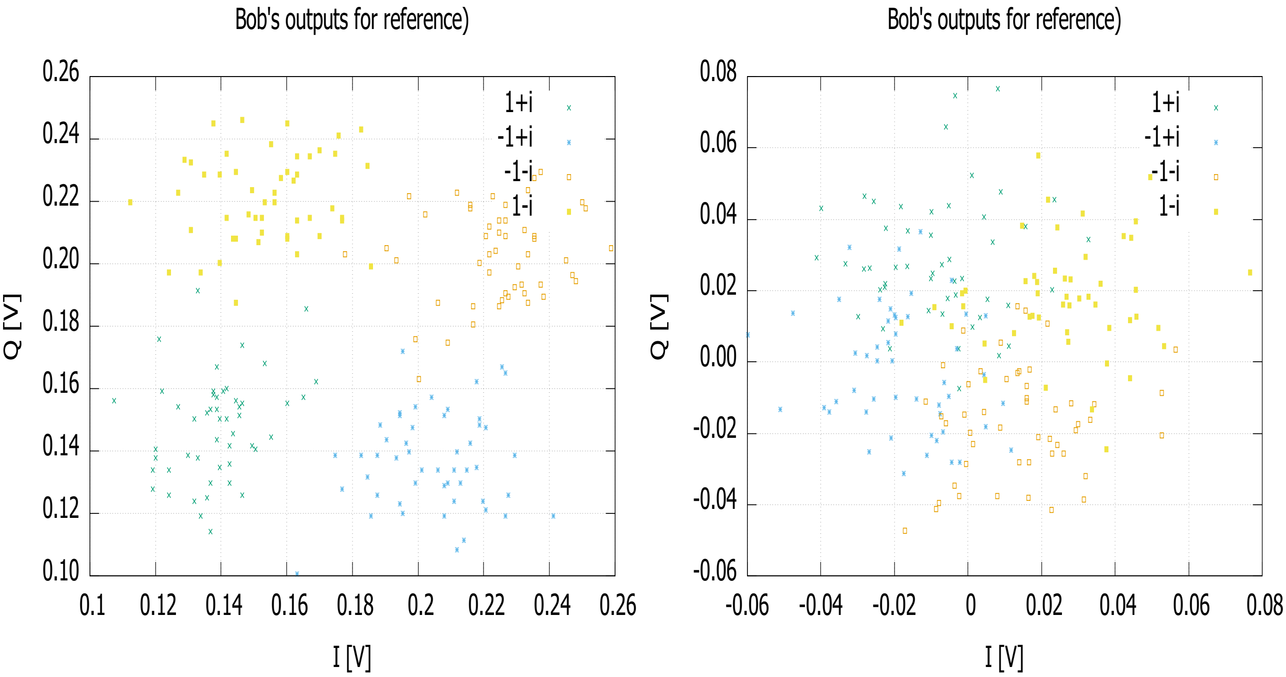


**Figure 7.14:** Reference symbols after detection. Each point of the QPSK constellation is represented by a different color. The rotation of each centroid represents the phase shift with respect to the values at Alice's. The figure on the left represents a high SNR situation while the left one is more typical on the chip. The coordinates of the centroid will depend on the balancing of the detector.

obtain a much more stable value. In 7.16, as well as in the subsequent figures, the continuous traces represent accumulated estimations, so the parameter that will be used in the SKR estimation is only the last one in the accumulated trace (it corresponds to the average of the entire frame except for the discarded initial blocks).

From table 2.2 we can derive the following relation between the estimated correlation and the original variance:

$$\langle xy \rangle^2 = \eta T V_A^2 \tag{7.3}$$

$$\rho^2 = \eta T \frac{V_A}{V_B} = \eta T \frac{\gamma_A^2 \sigma_G^2}{\sigma_B^2} \tag{7.4}$$

We assume that the detection efficiency $\eta$ is known and the channel transmittance can be estimated as

$$T = \frac{\rho^2 \sigma_B^2}{\eta \gamma_A^2 \sigma_G^2} \tag{7.5}$$

The results per block as well as the accumulated values are displayed in figure 7.17. The results approach 1 as expected in a B2B configuration with certain insertion loss due to the optical contacts.

Once the channel transmittance is estimated, it is possible to calculate the contribution of the signal to Bob's variance as $\sigma_A^2 = \eta T \gamma_A^2 \sigma_G^2$, where $\sigma_G^2$ is the variance calculated in Alice's units and $\gamma_A$ is the conversion

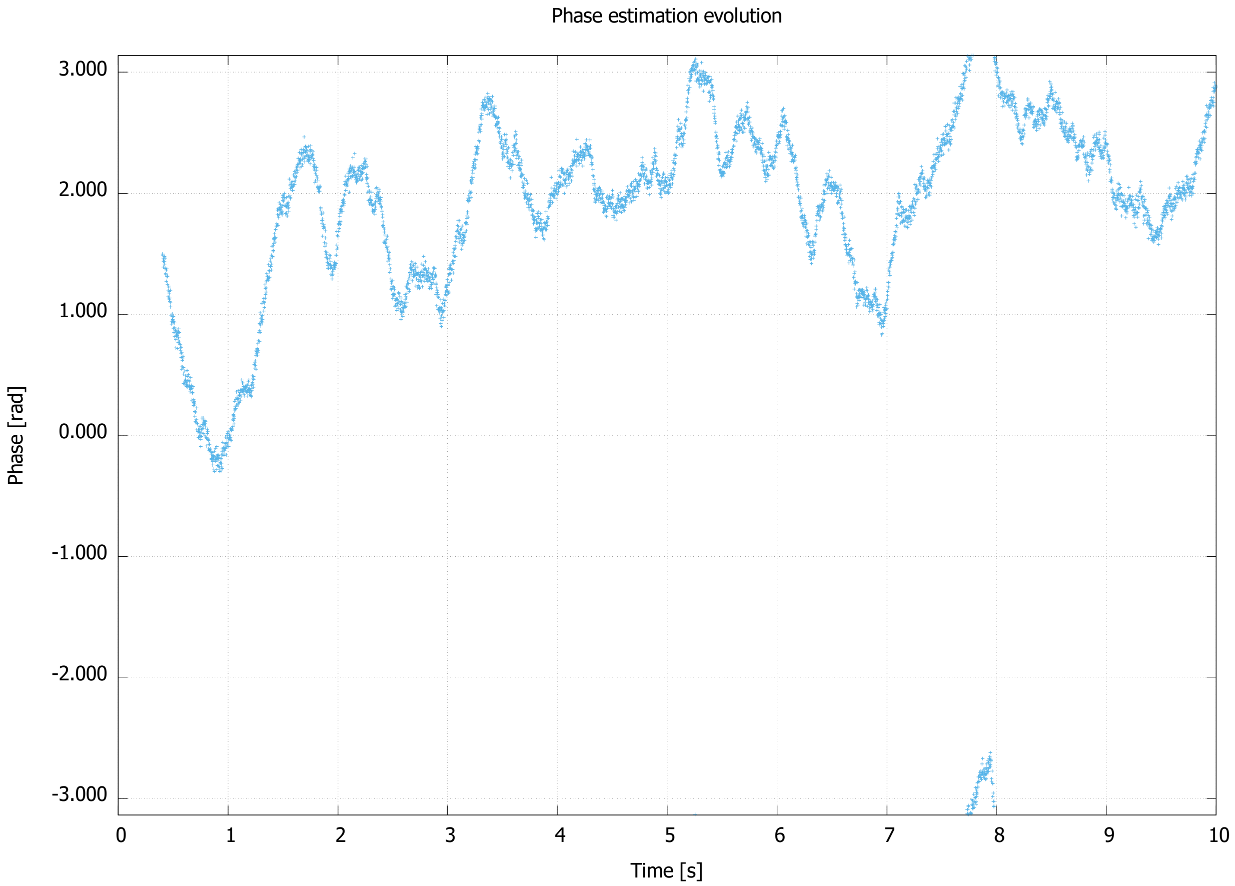


**Figure 7.15:** Estimated evolution of phase in on-chip coherent detector. The shape of these curves can be very diverse and correspond to possible fluctuations in the fibres of the system.

factor to Bob's units, estimated as indicated in the previous section. The contributions of each of the different sources of noise can be added up to approach the total variance at Bob's $\sigma_B^2$, the difference corresponding to the excess noise measured at Bob's. An illustration of these variances is given in figure 7.18, where the vertical scale has been kept linear to give a sense of the scale of the involved values and the discrimination that needs to be made in order to calculate the excess noise (blue and yellow traces are almost indistinguishable in this scale).

It is more practical to separate the different contributions and represent them in logarithmic scales to appreciate their evolution, as illustrated in figure 7.19. The shot noise $N_0$ corresponds to 1 and the rest of the values are normalized to $N_0$. The highest variance value corresponds to the reference signals that are not relevant for security (they were not represented in 7.18 to maintain the linear scale), and the level of $\eta T V_A$ in this case is slightly lower than 1 SNU. The excess noise is represented as measured by Bob (in black) and translated to the input of the channel (in red), after the division of Bob's estimation by $\eta T$. It can be seen that the values at the input of the channel are above 10% of the shot noise, mainly due to the 17.7 dB losses in the detector.

In order to put in context the performance of figure 7.19 we can compare it to figure 7.20 that represents the same process under similar

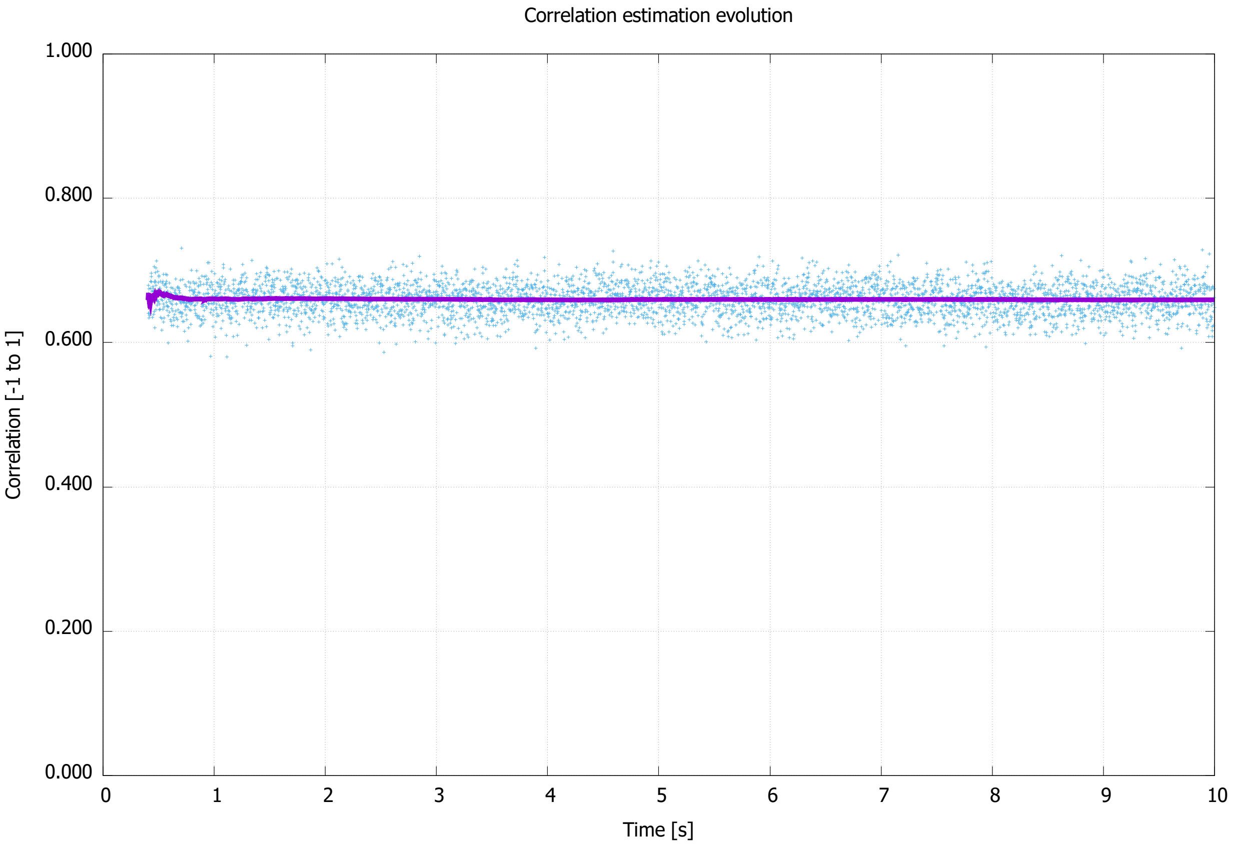


**Figure 7.16:** Estimated evolution of correlation in on-chip coherent detector. The estimated values obtained for a block (pale blue) can be very noisy, but performing a moving average (solid purple) provides a stable value.

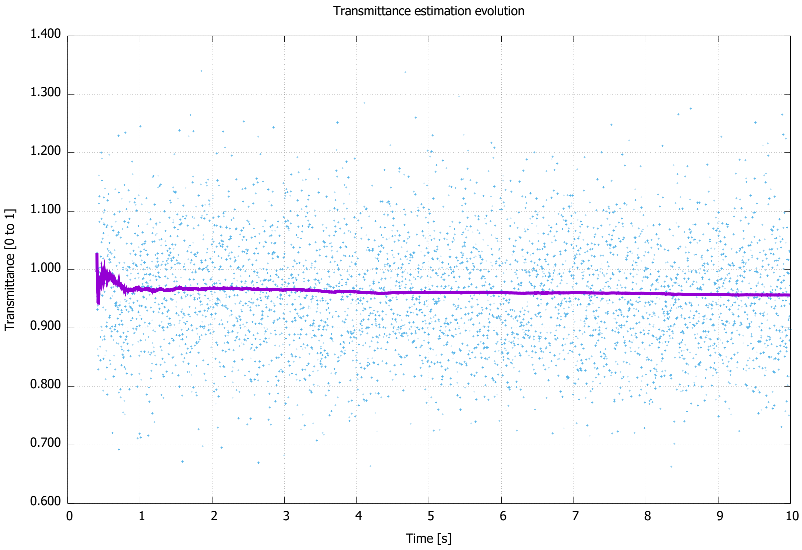


**Figure 7.17:** Estimated evolution of channel transmittance in on-chip coherent detector. As in figure 7.16, pale blue represents the noisy block estimations and the solid purple line the accumulated average values. Estimations for one block might be above 1, which is expected for a noisy detector, but the average remains below.

conditions but for a coherent bulk detector with the same type of amplifier and efficiency 0.6. If we pay attention to the red curve in 7.20, it is much lower than the one in 7.19, but this is not true for the black one, corresponding to the excess noise estimation at Bob's. We can infer from this that the estimation performed in the on-chip detector is comparable to the one achievable in a comparable bulk detector. We can predict also that coupling losses will separate the black and red

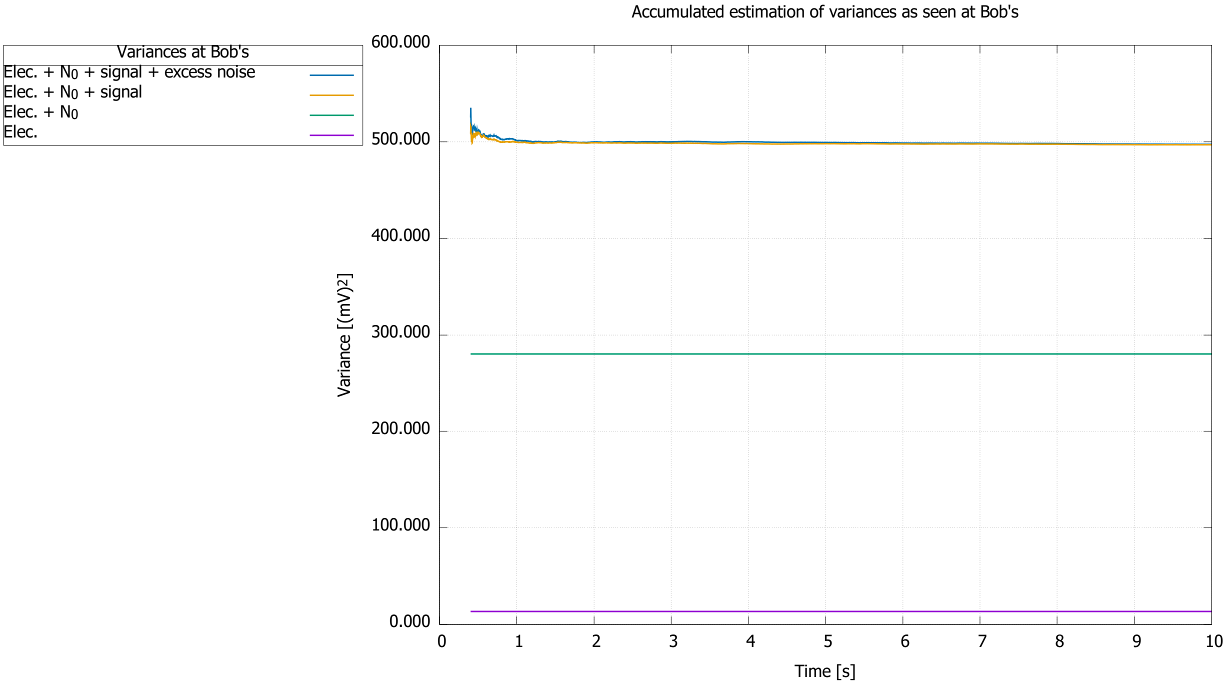


**Figure 7.18:** Estimated evolution of variances in on-chip coherent detector. Different sources of variance are accumulated (see legend) before attaining the total measured variance. The margin is the excess noise measured at Bob's $\xi_{\text{Bob}}$. Phase reference variance is not represented as it would be much higher than any of the others.

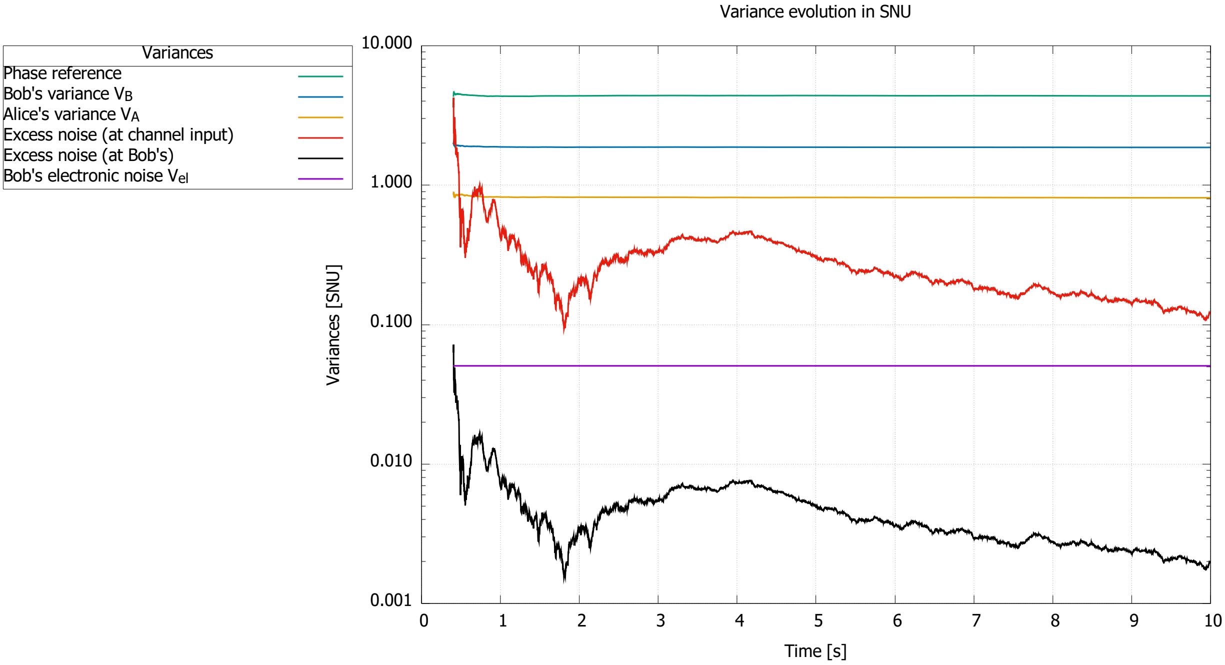


**Figure 7.19:** Evolution of estimated variances in on-chip coherent detector using logarithmic scale and SNU. The estimated discriminated variances are represented in shot noise units. Note the big margin between the excess noise at Bob's (black) and at the input of the channel (red). This is due mainly to the low efficiency of the detector and implies that in order to have a low value at the input of the channel the estimation at Bob's needs to be much lower. This uncertainty also produces oscillations of relatively high amplitude in the accumulated average, which stabilize as the window increases.

curves, requiring lower estimates of the excess noise at Bob's. This demands higher precision in the rest of the estimates, mainly $N_0$ and $V_{\text{el}}$, and it is probably the most disadvantageous effect of having low detection efficiencies.

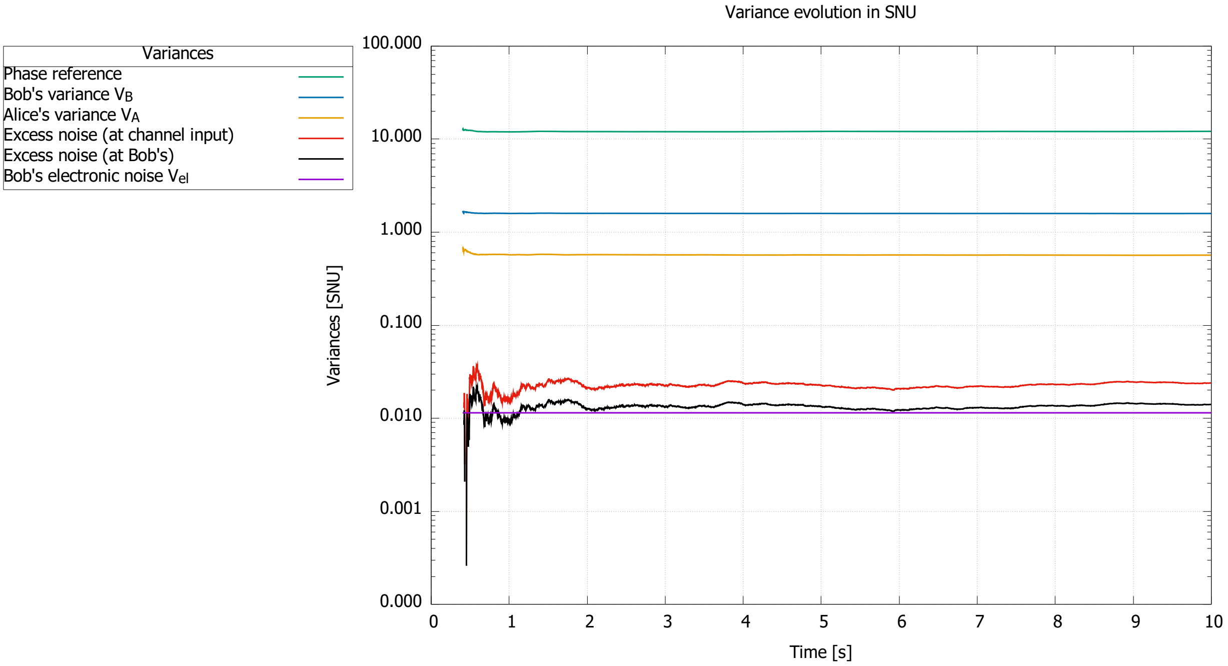


**Figure 7.20:** Evolution of estimated variances in bulk coherent detector using logarithmic scale. The same as figure 7.19 but for a comparable bulk detector with efficiency $\eta = 0.6$. In this case the separation between the excess noise at Bob's and at the input of the channel is much lower, allowing less incertitude in the rest of the parameters.

### 7.3.6 Achievable secret key rates

The previous results present two faces: a pessimistic one accounting for the 17.7 dB loss and the inconvenience of tightly following the oscillations in the shot noise, and a more optimistic one if we pay attention to the estimated excess noise at Bob's, providing values that would allow estimations at the input of the channel in the order of a few percent of SNU if the losses would be only 10 dB (a conservative value, since coupling losses could in theory approach 3-8 dB).

Figure 7.21 presents the expected SKR for a margin of parameters for the on-chip coherent detector compatible with the previous two interpretations. In the pessimistic case an excess noise between 0.12 and 0.2 SNU would only allow the exchange of secret key at short distances (between green and red curves). If we assume that $\eta$ can increase (or that we have a more elaborate method to calibrate the shot noise during the execution) and the estimation of the excess noise at Bob's remains constant, the excess noise at the input of the channel would improve, allowing longer communication distances (an estimate is shown in dashed orange in the same figure).

Note that an ideal parametrization of $\eta$ does not influence the achievable distance, as can be seen in figure 7.22, but as mentioned before it restrains the margin of error in the other estimations, increasing the excess noise.

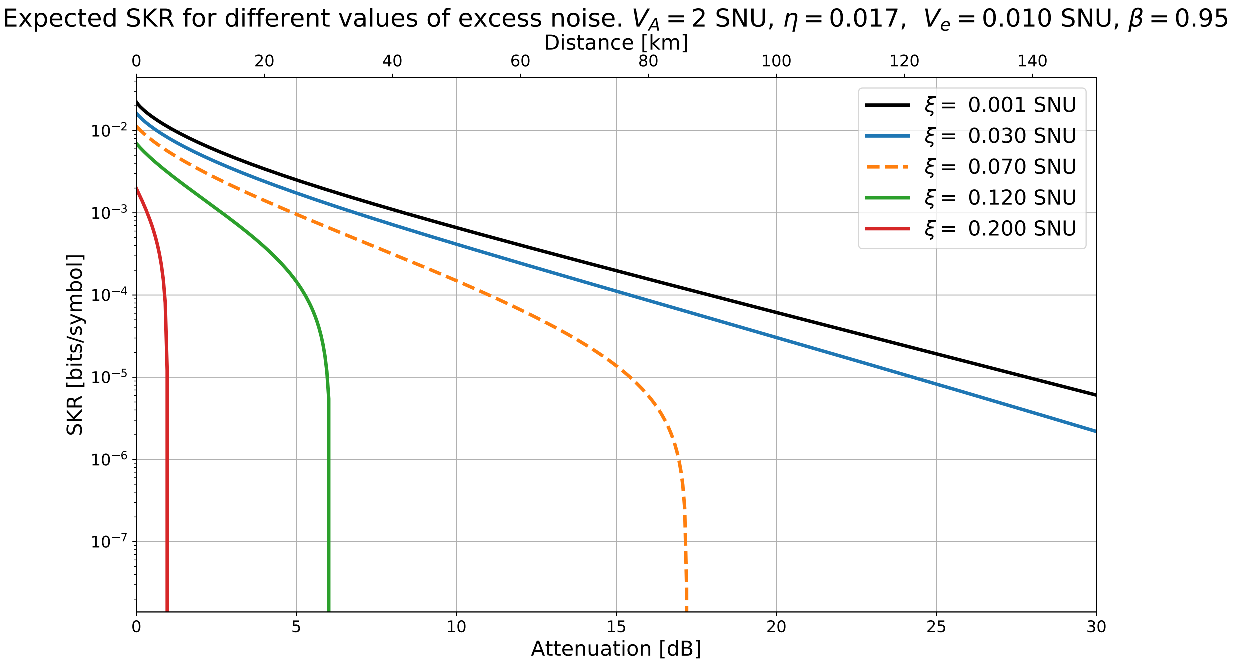


**Figure 7.21:** Expected SKR for on-chip detector for different values of excess noise. The detection efficiency is fixed to $\eta = 0.017$ and the expected SKR for different values of excess noise $\xi$ (at the input of the channel) are shown. An almost ideal curve is plotted in black for reference. We can see that high values of $\xi$ decrease the achievable distance in CV-QKD. The results obtained for the set up lay in the interval between the red and the green curves, but better results could be achieved with a more refined calibration method of the shot noise (the dashed orange curve is the expected bound considering the results with the bulk detector applied to the chip).

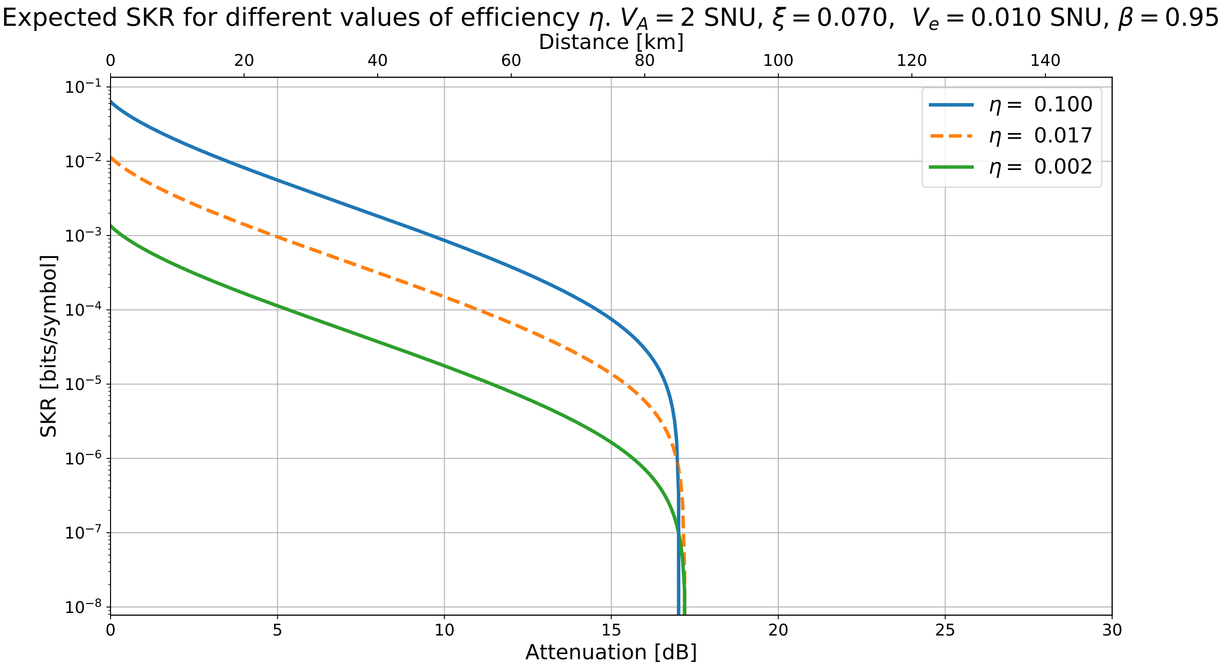


**Figure 7.22:** Expected SKR for on-chip detector for different values of detection efficiency. The excess noise is fixed to $\xi = 0.07$ SNU using the arguments explained in figure 7.21. Alice's variance is also fixed to $V_A = 2$ SNU. We see the theoretical effect of the efficiency $\eta$ as a function of the attenuation. The achievable distance changes due to the fact of using a fixed value of $V_A$ (detectors with higher $\eta$ can achieve longer distances if the optimal $V_A$ is used). For shorter distances the effect of the detection efficiency is a direct impairment on the SKR. In practice low $\eta$ will also imply higher $\xi$ since the estimates will have more associated uncertainty.

## 7.4 Conclusions

The results using an on-chip detector show parameters compatible with the generation of key, in principle restricted to short distances due to fabrication errors that led to efficiency losses in the detector of 17.7 dB. Comparisons with a bulk detector under similar conditions show that the situation would potentially improve if the coupling efficiency would be in the expected range of 5 to 8 dB losses and/or if a more complex shot noise tracking mechanism would be implemented.

The actions currently in progress to solve these problems are the packaging of new non-defective dice and the implementation of a shot noise calibration mechanism using an external switch. Due to the slow cycles involved in the fabrication and packaging of integrated devices the new units could not be completed before the closing of this document.

Additional conceptual developments are also being introduced, mainly transitioning from charge amplifiers (useful for pulsed set ups) to transimpedance amplifiers (TIA). This should provide more bandwidth and flexibility to the system, since CW LO and signal could be used allowing the compatibility with the systems described in section 2. Also, there would be no need of operating at $\omega_{\mathrm{IL}} = 0$ and a 180° hybrid heterodyne scheme could be implemented. This would solve the problem of requiring a phase modulator to implement CV-QKD on the current detector.

With the purpose of reducing the time to obtain a testable device we are also redesigning part of the electronics in order to work with standardized components. This should also reduce the potential mistakes in the process with respect to the use of home-made components.

# Free-space CV-QKD. Satellite feasibility study

# CV-QKD in free-space 8

8.1 Comparison fibre and free space . . . . . . . . . . . . . . . . 115
Losses . . . . . . . . . . . . 115
Channel fluctuations . . . . 117
8.2 Secret key over a fading channel . . . . . . . . . . . . . . . . . 117
Holevo bound . . . . . . . 118
Mutual information . . . . 119
Secret key rate . . . . . . . . 121
8.3 Secret key subdividing the fading channel . . . . . . . . . . . 122
Classification of symbols in bins . . . . . . . . . . . . . . . . 122
Methodology . . . . . . . . 124
Example . . . . . . . . . . . 125
8.4 Experimental proposal . . 130
Suitable schemes . . . . . 130
Emulation of a free-space link . . . . . . . . . . . . . . . . 130
Proposal for a proof-of-principle free-space CV-QKD experiment . . . . . . . . . . . . 131
8.5 Conclusion . . . . . . . . . 132

In this chapter we analyse the consequences of using free-space optical (FSO) links in CV-QKD and evaluate the expected secret key rate performance. We show that in the general case the fluctuations of the fading channel will prevent the generation of secret key, but this could be circumvented subdividing the channel. The methodology to perform this subdivision is explained and some examples illustrate the process. We finish with a brief description of a proof-of-principle implementation that we are currently developing. This chapter is limited to fixed emitter and receiver entities, but the same methodology will be extended to entities in relative motion in the subsequent chapter, studying the special case of satellite links.

## 8.1 Comparison fibre and free space

Optical fibre is a very interesting support for optical communications due to its guided nature, but it has two major drawbacks: (1) it requires deployment (and field infrastructure in some cases); (2) the losses are exponential in nature. An alternative to guided communications is to use free-space links. They do not require field infrastructure, but in the optical case a direct field of vision is necessary and the node infrastructure can be complex. As discussed below, the signal losses in the channel are quadratic, which can be competitive with respect to fibre in certain scenarios. This is especially interesting for QKD, where the losses of the channel are one of the main obstacles to achieve long key exchange distances.

With current technology it is more practical to generate and measure the states used in CV-QKD with fibre components (especially at 1550 nm due to the high availability of telecom components), so in most cases it is convenient to use the same basic hardware for Alice and Bob and introduce lenses to couple with the free-space channel. Other options are the use of the visible range or other wavelengths common in free-space communications.

### 8.1.1 Losses

The attenuation experimented by the free-space link can be divided into three main factors: (1) the geometry of the system, (2) the molecules in the atmospheric path and (3) the system losses.

The attenuation due to the geometry of the link can be calculated as a function of the diameters of the transmitting $d_t$ and receiving $d_r$ lenses, the range (slant distance) $L$ between the lenses and the divergence angle of the beam $\theta_d$ (which is in general a function of $d_t$.

If the distances are in meters and the angles in radians the expression in dB holds as:

$$L_{\text{geometric}} = 10\log\left[\frac{d_r^2}{(d_t + (L\cdot\theta_d))^2}\right] \tag{8.1}$$

The geometrical losses can be reduced increasing the size of the receiving lens or decreasing the divergence of the beam[43] , which are parameters that have practical technological limits. Bigger optics are not always feasible, and they typically increase the cost.

The molecules in the optical path can interact with the photons. In certain occasions a fraction of the photons will be absorbed, causing a fixed amount of losses. In other cases the interactions are more complex and will affect the stability of the channel. The amount of absorbed photons will depend on their wavelength and the weather conditions and it is convenient to calculate it empirically. These losses will be relevant for long horizontal links, where the communication takes place in the atmosphere. For satellite links, the trajectory in the atmosphere can be considered limited to around 15 km and the transmission windows are well studied for observation purposes. Figure 8.1 shows the transmission considering the complete atmosphere at mount Mauna Kea under certain conditions. It can be seen that the C and O bands (1530-1560 nm and 1260-1360 nm) suffer low attenuation in the atmosphere.

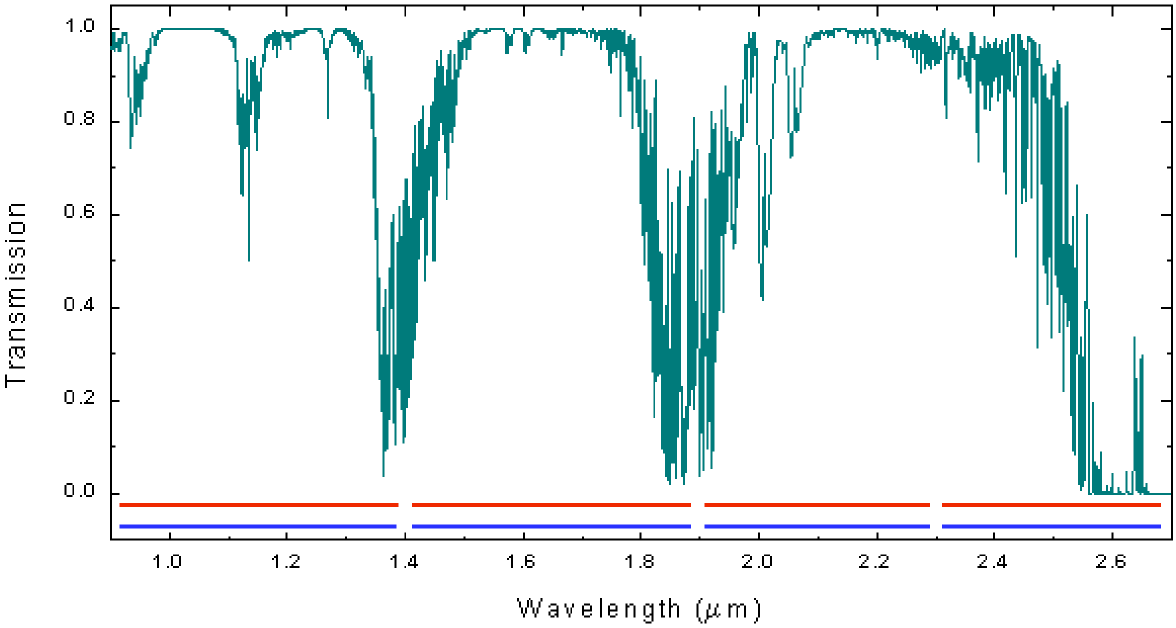


**Figure 8.1:** Transmission windows in the near infra-red regime at Mauna Kea. Source: https://www.gemini.edu/sciops/telescopes-and-sites/observing-condition-constraints/ir-transmission-spectra.

The system losses comprise the technological limits of the set up. The nature of interferometric and detection losses is the same as in fibre set ups. A particularly challenging technological aspect that free-space

[43] The reduction of the divergence can be obtained increasing the size of the lens at the transmitter or decreasing the wavelength.

communications face is the coupling of light from the medium to the detection system. This is so because the atmosphere will introduce unpredictable changes in the wave front of the beam. If they are not corrected there would be a mismatching of modes in the interferometric process that will affect the efficiency of the process. Fortunately there are techniques to partially compensate the effects of the atmosphere on the detection. The most prominent one comes from the field of observational astronomy and is generally designated as adaptive optics. The main idea is to correct the affected wave front beam passing it through a deformable mirror that corrects the aberrations up to a certain order[44] . The position of the deformable mirror is controlled by a software that analyses the wave front at the detector. Although its implementation is far from trivial in practice, in this work we will assume that we could implement those techniques with a cost of 3 dB in attenuation.

### 8.1.2 Channel fluctuations

Effects of different nature can introduce fluctuations in the received power that are not predicted by the previously discussed losses. They are generally referred to as fading and can be of slow or fast nature. Slow fading relates to events that are orders of magnitude slower than the symbol time and will not be considered in principle. Fast fading follows processes in a rate slower but comparable to the symbol rate and it will be the focus of our analysis. The study of fading can be considered a field on its own and we remit to the appendix D for a brief introduction and to reference [107] for more details. As in the references, we will consider that fading is composed of turbulent effects in the atmosphere and beam wandering (the fluctuation of the centroid of the beam with respect to the center of the receiving lens).

For this chapter we will assume that the transmission coefficient $\tau = \sqrt{T}$ of the channel can be modelled by a statistical process of density distribution $\mathcal{P}(\tau)$ that we will call probability density distribution of the transmission coefficient (PDTC). In most cases the predominant factor in the PDTC will be the beam wandering and in other cases the turbulence effects will be predominant.

## 8.2 Secret key over a fading channel

The estimation of the secret key rate over a fading channel with PDTC $\mathcal{P}(\tau)$ is analogous to the fixed channel case, but we will see that the variability in the transmission will have detrimental effects on the excess noise. We estimate the expected Holevo bound and the mutual information to evaluate the secret key rate.

[44] Zernike polynomials are typically used in the correction.

### 8.2.1 Holevo bound

As indicated in chapter 2 the covariance matrix before the measurement can be described using equation 2.8, where all the parameters are considered fixed, including $\eta$ and $T$. For a set of fixed transmission efficiencies $\{T_i\}$, $T_i \in [0,1]$, keeping the rest of the parameters[45] constant and the notation in figure 2.5 we can adapt equation 2.8 to each of the values as:

$$\gamma_{AB_1}^{T_i} = \begin{pmatrix} V \cdot \mathbb{1}_2 & \sqrt{T_i\left(V^2-1\right)} \cdot \sigma_z \\ \sqrt{T_i\left(V^2-1\right)} \cdot \sigma_z & \left(1 + T_i\left(V_{\mathrm{A}} + \xi\right)\right) \cdot \mathbb{1}_2 \end{pmatrix} \tag{8.2}$$

If we generalize the set $\{T_i\}$ to a distribution of transmission efficiency $\mathcal{T} = \tau^2$, the convex sum over $\mathcal{T}$ for all the possible covariance matrices $\gamma_{AB_1}^{\mathcal{T}}$ gives [108]

$$\langle\gamma_{AB_1}^{\mathcal{T}}\rangle_{\mathcal{T}} = \begin{pmatrix} V \cdot \mathbb{1}_2 & \sqrt{\langle\sqrt{\mathcal{T}}\rangle^2\left(V^2-1\right)} \cdot \sigma_z \\ \sqrt{\langle\sqrt{\mathcal{T}}\rangle^2\left(V^2-1\right)} \cdot \sigma_z & \left(1 + \langle\mathcal{T}\rangle\left(V_{\mathrm{A}} + \xi\right)\right) \cdot \mathbb{1}_2 \end{pmatrix} \tag{8.3}$$

Comparing 8.2 and 8.3 it is easy to rewrite the matrix in the following form

$$\langle\gamma_{AB_1}^{\mathcal{T}}\rangle_{\mathcal{T}} = \begin{pmatrix} V \cdot \mathbb{1}_2 & \sqrt{T_{\mathrm{eff}}\left(V^2-1\right)} \cdot \sigma_z \\ \sqrt{T_{\mathrm{eff}}\left(V^2-1\right)} \cdot \sigma_z & \left(1 + T_{\mathrm{eff}}\left(V_{\mathrm{A}} + \xi_{\mathrm{eff}}\right)\right) \cdot \mathbb{1}_2 \end{pmatrix} \tag{8.4}$$

where the transmission efficiency and the excess noise are substituted by equivalent constant factors $T_{\mathrm{eff}}$ and $\xi_{\mathrm{eff}}$ that follow the expressions:

$$T_{\mathrm{eff}} = \langle\sqrt{\mathcal{T}}\rangle^2 = \left\langle\tau^2\right\rangle - \mathrm{Var}(\tau) \tag{8.5}$$

$$\xi_{\mathrm{eff}} = \frac{\left\langle\tau^2\right\rangle}{T_{\mathrm{eff}}}\xi + \left(\frac{\left\langle\tau^2\right\rangle}{T_{\mathrm{eff}}} - 1\right)V_A \tag{8.6}$$

If we want to calculate the effects of the fading on the excess noise we can express them as

$$\begin{aligned} \xi_{\mathrm{fad}} = \xi_{\mathrm{eff}} - \xi &= \left(\frac{\left\langle\tau^2\right\rangle}{T_{\mathrm{eff}}} - 1\right)\left(V_{\mathrm{A}} + \xi\right) \\ &= \frac{\mathrm{Var}(\tau)}{T_{\mathrm{eff}}}\left(V_{\mathrm{A}} + \xi\right) \approx \frac{\mathrm{Var}(\tau)}{\mathcal{T}_{\mathrm{eff}}}V_{\mathrm{A}} \end{aligned} \tag{8.7}$$

The approximation holds for a noiseless channel and for the practical cases where $V_{\mathrm{A}} \gg \xi$ and it matches the results in [108] [46] . From the previous results we make the following observations:

[45] $V_A$ is Alice's modulation variance in SNU; $V = V_A + 1$; $\xi$ is the excess noise in SNU as seen at the input of the channel.

[46] Note that in [108] the excess noise is referred to the output of the channel, so the term $\mathcal{T}_{\mathrm{eff}}$ in the denominator does not appear.

- The effective overall efficiency is smaller than the average, independently of the distribution: $T_{\text{eff}} = \left\langle \tau^2 \right\rangle - \text{Var}(\tau) \leq \left\langle \tau^2 \right\rangle$. To keep $T_{\text{eff}}$ positive, $\text{Var}(\tau)$ cannot exceed $\langle \tau^2 \rangle$, as can be seen in figure 8.2.
- The excess noise due to fading $\xi_{\text{fad}}$ is linear with respect to Alice's modulation and the excess noise due to the channel $\xi$, which should play in favour of the quantum case (weak signals suffer less excess noise from fading), but it can become very high when the ratio $\text{Var}(\tau)$ over $T_{\text{eff}}$ is high (see figure 8.3), which makes it relevant in high loss scenarios.

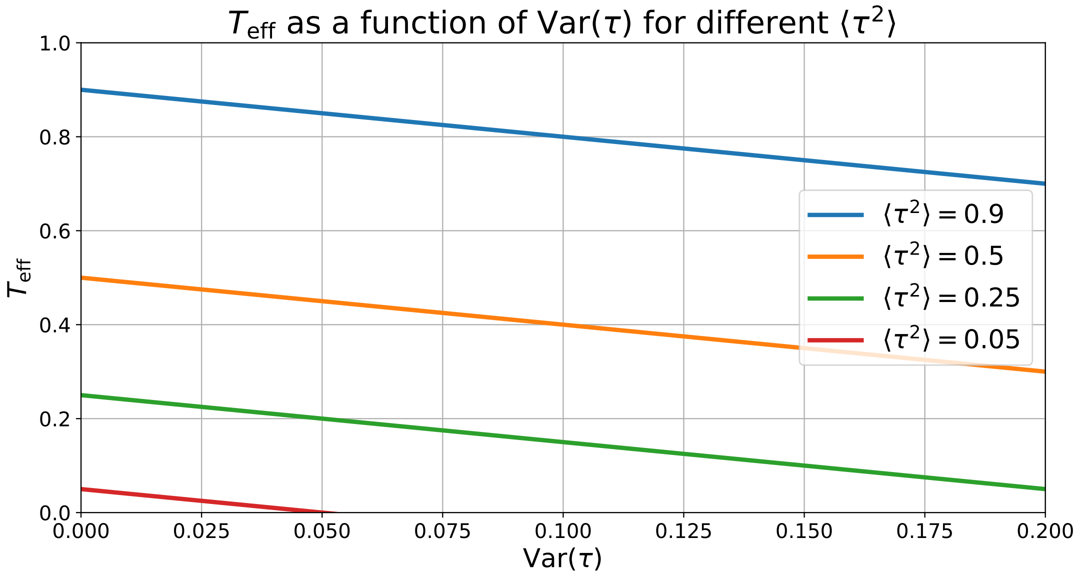


**Figure 8.2:** Effective overall transmittance $T_{\text{eff}}$ as a function of the variance $\text{Var}(\tau)$ for different average transmittances $\langle \tau^2 \rangle$. $T_{\text{eff}}$ is a decreasing function that can become negative if $\text{Var}(\tau) > \langle \tau^2 \rangle$.

In order to proceed with the calculation of the Holevo bound, the matrix 8.4 can be projected into a certain basis following the methods in appendix C resulting in a matrix $\gamma_{AB_1|b}$ or $\gamma_{\text{AFG}}^{m_{\text{B}}}$ depending on the quadratures measured, with eigenvalues $\nu_k$. Along with the eigenvalues $\lambda_k$ of $\langle \gamma_{AB_1}^{\mathcal{T}} \rangle_{\mathcal{T}}$ the Holevo bound can be calculated as:

$$\chi_{BE}^{\mathcal{T}} = \sum_{k=1,2} g(\nu_k) - \sum_{k>2} g(\nu_k) \tag{8.8}$$

where the Von Neumann entropy is calculated as

$$g(z) = \frac{z+1}{2} \log_2 \left( \frac{z+1}{2} \right) - \frac{z-1}{2} \log_2 \left( \frac{z-1}{2} \right) \tag{8.9}$$

### 8.2.2 Mutual information

As seen in appendix C, for a point to point communication over a noisy Gaussian channel of transmittance $T$, with a detector capable of two shot noise limited projections with detection efficiency $\eta$ and electronic

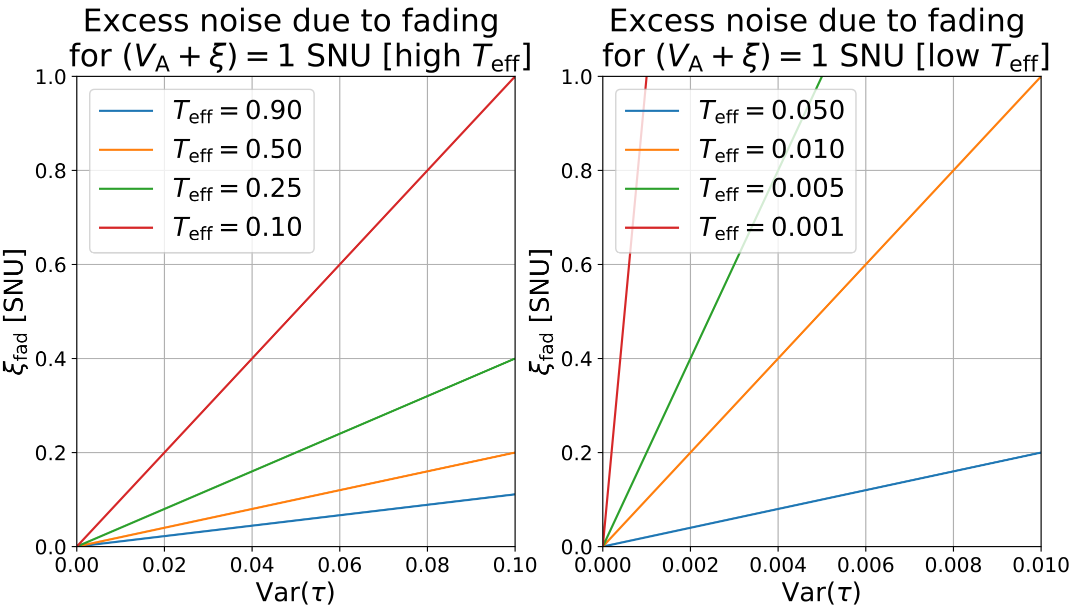


**Figure 8.3:** Excess noise due to fading $\xi_{\text{fad}}$ as a function of fading variance Var($\tau$) for different overall transmission efficiencies $T_{\text{eff}}$. As $T_{\text{eff}}$ decreases, the contribution of fading to the excess noise becomes more important. Curves are directly proportional to other values of $V_A + \xi$.

noise $V_{\text{el}}$, the mutual information can be written as a function of the SNR $s$ as

$$I_{AB}(s) = \beta(s)\log_2(1+s) = \beta(s)\log_2\left(1 + \frac{\eta T V_A}{2 + 2V_{\text{el}} + \eta T \xi}\right) \tag{8.10}$$

with $V_A$ Alice's variance and $\xi$ the excess noise referred at the channel input. If as previously we denote by $\{T_i\}$ a set of overall transmission efficiencies, and we assume that $\beta$ can be made constant independently of the SNR[47] , as well as of the parameters $V_A$ and $V_{\text{el}}$ we can simplify the expression to obtain:

$$I_{AB}^{T_i} = \beta\log_2(1+s(T_i)) = \beta\log_2\left(1 + \frac{\eta T_i V_A}{2 + 2V_{\text{el}} + \eta T_i \xi}\right) \tag{8.11}$$

If, as done previously, we adapt the set $\{T_i\}$ to a generic variable $\mathcal{T}$ that follows an ergodic process[48] $f(\mathcal{T})$, the aggregated ergodic mutual information can be calculated as:

$$I_{AB}^{\mathcal{T}} = \beta\left\langle\log_2(1+s(\mathcal{T}))\right\rangle_{\mathcal{T}} = \int_0^1 \log(1+s(\mathcal{T}))f(\mathcal{T})d\mathcal{T} \tag{8.12}$$

From the concave nature of the logarithmic function and Jensen's inequality, we can conclude that

$$\beta\left\langle\log_2(1+s(\mathcal{T}))\right\rangle_{\mathcal{T}} \leq \beta\log_2(1+\langle s(\mathcal{T})\rangle_{\mathcal{T}}) \tag{8.13}$$

This means that we cannot use the mean of the transmission efficiency to calculate the mutual information, since it is an overestimation of

[47] This is a realistic assumption that simplifies the analysis, but there is no fundamental impairment to consider $\beta$ a function of $T_i$. It would appear inside the mean in the final expression.

[48] The ergodic condition assumes that the fading is fast enough to have short temporal statistics that match the long term statistics. The outage probability (probability of having zero transmittance) in this case is not relevant. For slow fading channels, the temporal statistics are not representative of the overall process and some assumptions need to be considered, like the probability of outage when the transmission stays at a minimum for a relatively long period.

the actual value, but interestingly, for constant noise parameters, a fading channel with overall transmission efficiency average $\langle \mathcal{T} \rangle = \langle \tau^2 \rangle$ and variance $\mathrm{Var}(\tau)$ is equivalent to a fixed channel with transmission efficiency $T_{\mathrm{eff}}$ and excess noise $\xi_{\mathrm{eff}}$ following equations 8.5 and 8.6 as can be seen in figure 8.4. The mutual information between Alice and Bob over the fading channel can be expressed as

$$I_{AB}^{\mathcal{T}} = \beta \left\langle \log_2 \left(1 + s\left(\mathcal{T}\right)\right)\right\rangle_{\mathcal{T}} = \beta \log_2 \left(1 + s\left(T_{\mathrm{eff}}, \xi_{\mathrm{eff}}\right)\right) \tag{8.14}$$

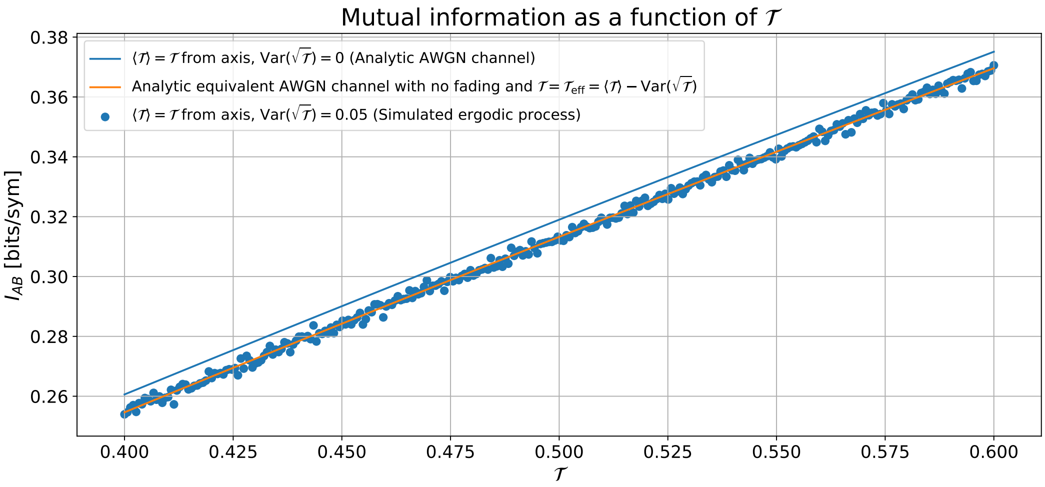


**Figure 8.4:** A process of Gaussian fading with variance $\mathrm{Var}(\tau) = 0.05$ is simulated for an interval of $\langle \tau^2 \rangle$. It can be seen that the mutual information is lower than in the fixed channel case, but it can be compared to a fixed channel with lower transmission efficiency $T_{\mathrm{eff}}$ and higher excess noise $\xi_{\mathrm{eff}}$. The parameters are close to optimal to facilitate the visualization of the effect: $V_A = 1$ SNU, $V_{\mathrm{el}} = 0.001$ SNU, $\xi = 0.001$ SNU, $\beta = 1$.

### 8.2.3 Secret key rate

Assuming that the trusted parties can estimate $N_0$ (also $V_{\mathrm{el}}$ and $\eta$[49] in the case of a trusted detector) before the quantum phase of the protocol, the rest of the parameters can be estimated from the variances and covariances of the transmitted $x_i$ and received $y_i$ symbols. For a trusted 90° hybrid detector, the three remaining parameters of table 2.3 $V_A$, $T_{\mathrm{eff}}$ and $\xi_{\mathrm{eff}}$ can be derived from the following system of equations (in shot noise units):

$$\begin{aligned} \left\langle x^2 \right\rangle &= V_A \\ \left\langle y^2 \right\rangle &= \eta T_{\mathrm{eff}} V_A + 2 + 2V_{\mathrm{el}} + \eta T_{\mathrm{eff}} \xi_{\mathrm{eff}} \\ \langle xy \rangle &= \sqrt{\eta T_{\mathrm{eff}}} V_A \end{aligned} \tag{8.15}$$

Those estimators feed the matrices involved in the Holevo bound calculations; this result needs to be subtracted from the mutual information obtained after the error correction phase (but that can be inferred also from the previous parameters). The estimation for the key rate of a

[49] For a trusted detector the overall efficiency can be divided into the product of a trusted part $\eta$ and an untrusted part $T_{\mathrm{eff}}$.

fading channel, taking all the received symbols into account would lead to the the following expression

$$K^{\mathcal{T}} = I_{AB}^{\mathcal{T}} - \chi_{BE}^{\mathcal{T}} \tag{8.16}$$

Reflecting on the results in this section it is clear that fading (even in low variances) has an important effect in the excess noise (a key parameter in CV-QKD, especially important in what relates to the maximum achievable distances). In order to reduce the impairments due to the variance in the transmission channel, it is desirable to divide the contributions to the secret key into equivalent channels, also with fading but with a much lower variance, so that the aggregated key can be expressed as

$$K_{\text{fading}}^{\text{total}} = \sum_{c} K^{\mathcal{T}_c} \tag{8.17}$$

$\mathcal{T}_c$ being the equivalent channel for a set of symbols that are expected to have similar transmission efficiencies. This would reduce in principle the variance due to the fading, and thus the excess noise, allowing for better performances. The selection of the symbols in the quantum domain is not trivial, and it can also reduce the number of samples available for parameter estimation enhancing the finite size effects. The following sections study the possible implementations and the effects on the expected performance of CV-QKD.

## 8.3 Secret key subdividing the fading channel

We will study if we can obtain a gain in performance exploiting a subdivision of the channel in sub-channels with lower fading. We divide this analysis in two steps. We first study the feasibility of classifying the symbols in affine transmission coefficients. The expected secret key is calculated as the accumulation of the secret keys for all sub-channels[50] . A simple fading model described at the beginning of the chapter will be used as example, but the methodology can be generalized to any model as long as its $\mathcal{P}(\tau)$ (PDTC) is known.

### 8.3.1 Classification of symbols in bins

The transmission efficiencies used in the secret key generation need to be estimated over the quantum signal at Bob's. This can be generally a problem, since typically in CV-QKD the modulation variances are very low with respect to the noise of the detector. Let us assume that the samples $y_i$ at Bob's follow an AWGN model of the form:

$$y_i = \sqrt{\eta T} x_i + n_i \tag{8.18}$$

where $x_i$ are Alice's symbols measured in the units of Bob[51] , that are attenuated by a channel of transmission efficiency $T = \tau^2$ and

[50] 50: Conditions on the sub-channels can be applied. For example, the channels with low secret key rate can be omitted to alleviate the computational complexity. Channels with symbols that cannot satisfy the imposed finite-size criteria should also be neglected. This will be of special importance in the satellite scenario.

[51] 51: It is typical that Alice works with symbols $\underset{\omega}{\mathrm{x}}_i$ in arbitrary units that feed a chain of devices (DAC, amplifier, modulator...). A factor $\gamma_A$ can be calculated beforehand such that $x_i = \underset{\omega}{\mathrm{x}}_i \gamma_A$ is evaluated in Bob's units ($V^2$ or $\sqrt{\mathrm{SNU}}$).

a detector of efficiency $\eta$. All the noise, including the excess noise component $\xi$, can be modelled as an independent source of 0 mean and variance $\sigma_n^2$. In the case of a 90° hybrid detector with shot noise $N_0$ and electronic noise $V_{\mathrm{el}}$, $\sigma_n^2 = N_0(2 + 2V_{\mathrm{el}} + \eta T\xi)$.

An estimation $\hat{\tau}_{d_i}$ of the transmission coefficient calculated from the revealed quantum symbols can be obtained as

$$\hat{\tau}_{d_i} = \frac{x_i y_i}{\sqrt{\eta} x_i^2} \tag{8.19}$$

For a channel with fixed transmittance, in the absence of additional perturbations, and assuming Gaussian distribution for the noise $\sigma_n^2$ in the detector of efficiency $\eta$ and capable of $p$ projections, the distribution of the estimated transmission coefficient will follow a normal distribution with mean $\langle\tau_d\rangle$ and variance $\mathrm{Var}(\tau_d)$, with

$$\langle\hat{\tau}_d\rangle = \frac{\sum_{i=1}^{N} x_i y_i}{\sqrt{\eta}\sum_{i=1}^{N} x_i^2} \tag{8.20}$$

$$\mathrm{Var}(\hat{\tau}_d) = \frac{\sigma_n^2}{p\eta\sigma_{\mathrm{mod}}^2} \tag{8.21}$$

If the channel introduces fading, the additional fluctuations $\mathrm{Var}(\tau_f)$ can be considered independent of the detection uncertainty and the variances of both processes can be added giving a total estimated variance

$$\mathrm{Var}(\hat{\tau}) = \mathrm{Var}(\tau_d) + \mathrm{Var}(\tau_f) \tag{8.22}$$

In order to classify symbols using this method, the detection variance should be much smaller than the fading variance $\mathrm{Var}(\tau_d) \ll \mathrm{Var}(\tau_f)$, which is difficult to attain in CV-QKD set ups, since as shown in figure 8.3 the required $\mathrm{Var}(\tau_f)$ are relatively low (in the order of the per thousands for low $T$) and the coherent detection uncertainty is comparatively high. Figure 8.5 illustrates the dispersion of the estimation for a fixed channel using $\sigma_{\mathrm{mod}}^2$ several orders of magnitude higher that those used during a CV-QKD protocol (what can be considered as reference symbols). Even in that case the variance of the estimated values is much higher than the desired variance calculated in the previous section (figure 8.3). Another drawback of this methodology is that the symbols measured for classification cannot be used in the generation of key, requiring additional assumptions. This is feasible but introduces additional complexity.

Having shown the difficulty of using mechanisms available in typical CV-QKD set ups to classify the symbols into bins, we will assume that an additional signal of classical levels is available as a beacon. This signal is multiplexed with the quantum signal in a way that the fading experienced by both is very similar, but paying attention to avoid interferences from the classical beacon in the quantum signal. This can be implemented in practice in different ways, but while the

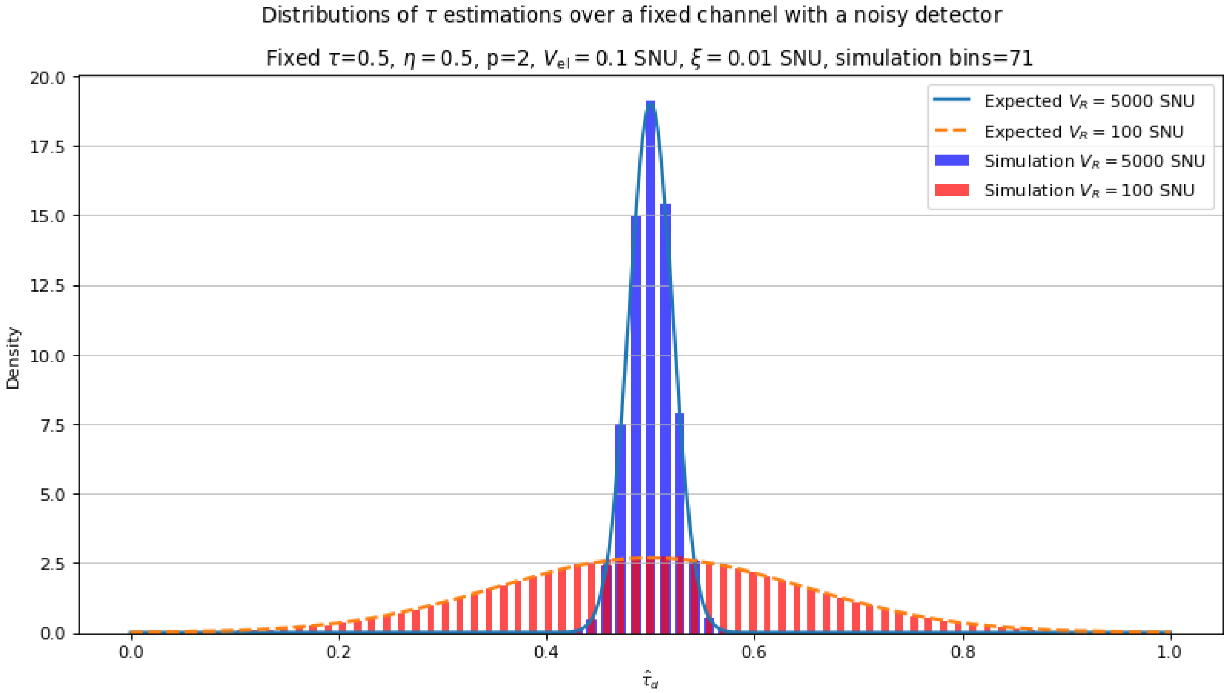


**Figure 8.5:** The distribution of the estimation of $\tau$ using different values in the transmitted variance, denoted by $V_R$. $10^6$ symbols are simulated over an AWGN channel and $\tau_{d_i}$ is estimated using equation 8.19 and separated into bins to obtain the histograms. The analytic variance of equation 8.21 is plotted to illustrate the accordance with the expected values. Note that the estimation for a typical quantum signal ($V_R$ in the order of a few SNU), would be very spread (almost flat) in this representation.

detector for the quantum signal remains coherent, the one used for the classical beacon will typically detect the intensity. This requires a method to discriminate the two signals at Bob's. A possible implementation among many would be using WDM to send the signals in nearby channels, allowing the discrimination.

If some symbols are incorrectly classified as belonging to a range of transmission coefficients, the effects would be undesirable but they will not compromise the security: the effective excess noise would increase producing a reduction of the secret key rate, so intentional attacks on the classical beacon can be considered a DoS attack.

### 8.3.2 Methodology

Assuming that we can reliably classify the quantum symbols into bins without measuring them we can perform the division of the fading channel into sub-channels with lower fading and potentially higher aggregated secret key rate. The steps are the following:

1. **Symbol exchange.** Alice sends symbols though a fast fading channel to Bob, who is located relatively static to her. The quantum signal and the classical beacon are multiplexed so that they suffer similar effects, but without interfering. Alice and Bob accumulate and index the classical and quantum values transmitted/measured for a period of time in order to obtain sufficient statistics (see finite size effects in chapter 2).

2. **PDTC estimation.** The transmission coefficients obtained from the classical beacon can be represented as a histogram that can be used to interpolate the PDTC of the channel $\mathcal{P}(\tau)$. Using the formulas in the previous section over different slices of the $\mathcal{P}(\tau)$ the optimal intervals $(\Delta\tau)_k$ to maximize the aggregated secret key taking into account additional considerations can be obtained. The optimal intervals will be different in general, but for simplicity we will assume a homogeneous distribution of $\tau$ in intervals $\Delta\tau$ between $\tau_{\text{min}}$ and $\tau_{\text{max}}$.
3. **Binning.** Once the desired distribution of classical symbols has been selected, the associated quantum symbols can be distributed in the same manner. The DSP algorithms used for mode recovery can be implemented before or after this phase. Better performances are expected if the symbols have similar $\tau$ (and hence SNR), but the DSP routines could be more complex if they need to process non consecutive symbols.
4. **Parameter estimation.** The parameter estimation is done for each bin obtaining the expected secret key rate. The bin can be discarded if the number of samples does not fulfil the requirements of the finite size constraints or if the rate is lower that a threshold (to reduce post-processing tasks).
5. **Error correction and privacy amplification.** Each bin is processed independently.
6. **Key aggregation**. The keys obtained with each channel are concatenated to obtain the aggregated key.

### 8.3.3 Example

In order to evaluate the advantages of dividing the fading channel, we will estimate the secret key for a typical fading profile given by equation D.9 illustrated in figure 8.6. The interval of the analysis is chosen between $\tau_{\text{min}} = 0.3$ and $\tau_{\text{max}} = \tau_0$ as the PDTC is zero otherwise. Without channel subdivision the variance of the PDTC would be so high that the secret key rate (SKR) would be zero, so we proceed testing different equally distributed intervals of width $\Delta\tau$. Figures 8.7, 8.8, 8.9 and 8.10 only show $\Delta\tau = 0.001$ and $\Delta\tau = 0.002$, but more values are calculated in figure 8.11.

The first step to estimate the key rate for a certain bin division is to calculate the variance of the transmission coefficient in each bin. This is displayed in figure 8.7 along with the percentage of the total symbols that are expected to fall in each bin for the given PDTC. From the $\langle\tau^2\rangle$ and $\text{Var}(\tau)$ the effective transmission efficiency $T_{\text{eff}}$ can be calculated for each bin. Similarly the effective excess noise can be predicted for given $V_A$ and $\xi$, as can be seen in figure 8.8. The secret key rate that could be achievable in any of the bins is shown in figure 8.9, but the PDTC is not yet applied. When this secret key rate is weighted by the PDTC $\mathcal{P}(\tau)$ we obtain the actual secret key rate per bin (figure 8.10. Accumulating the secret key rate from all the bins gives the aggregated secret key rate. In figure 8.11 the obtained secret key rate values as a function of $\Delta\tau$ are displayed, along with the rate for a fixed channel of transmission coefficient $\tau_0$ with the same parameters, that can be seen as the upper bound to the key rate. If no additional considerations are taken into account it is clear that we will approach the maximum secret key rate if the intervals $\Delta\tau \rightarrow 0$ [52] . This is not practical in most cases, since the portion of symbols per bin will decrease and finite size effects will become relevant. This will be of special importance in the satellite case. The number of symbols per bin will depend on the PDTC, the availability of the link and the repetition rate, so to generalize the analysis we consider the minimum percentage of symbols, that depends only on the PDTC, so that the number of symbols per bin can be extrapolated from the other two parameters. This is equivalent to putting a lower threshold on the percentage of symbols in figure 8.7. In this case bins with higher $\Delta\tau$ contain more symbols, which is required to fulfil elevated minimum required percentage of symbols (high number of symbols per bin), as can be seen in figure 8.11.

[52] As the transmission coefficients are lower than $\tau_0$ and the $V_A$ might not be optimal for all the sub-channels there is a gap between the fixed and the fading case.

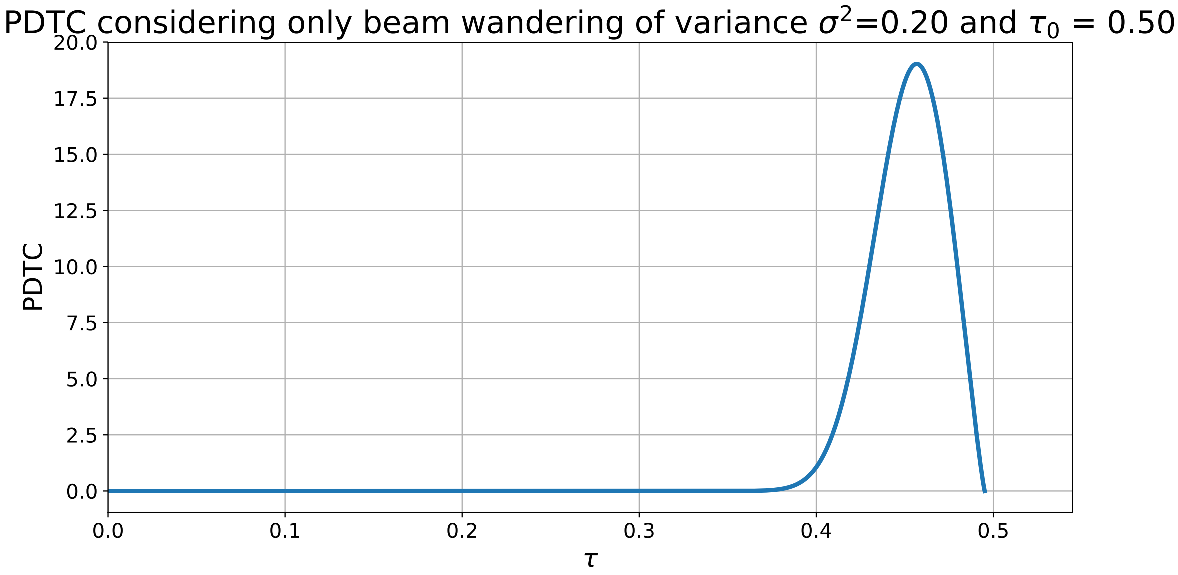


**Figure 8.6:** PDTC $\mathcal{P}(\tau)$ for a receiver with aperture radius $a = 0.75$ m, beam width at receiver $W = 2.0$ m and beam wandering variance $\sigma^2 = 0.2$ m$^2$.

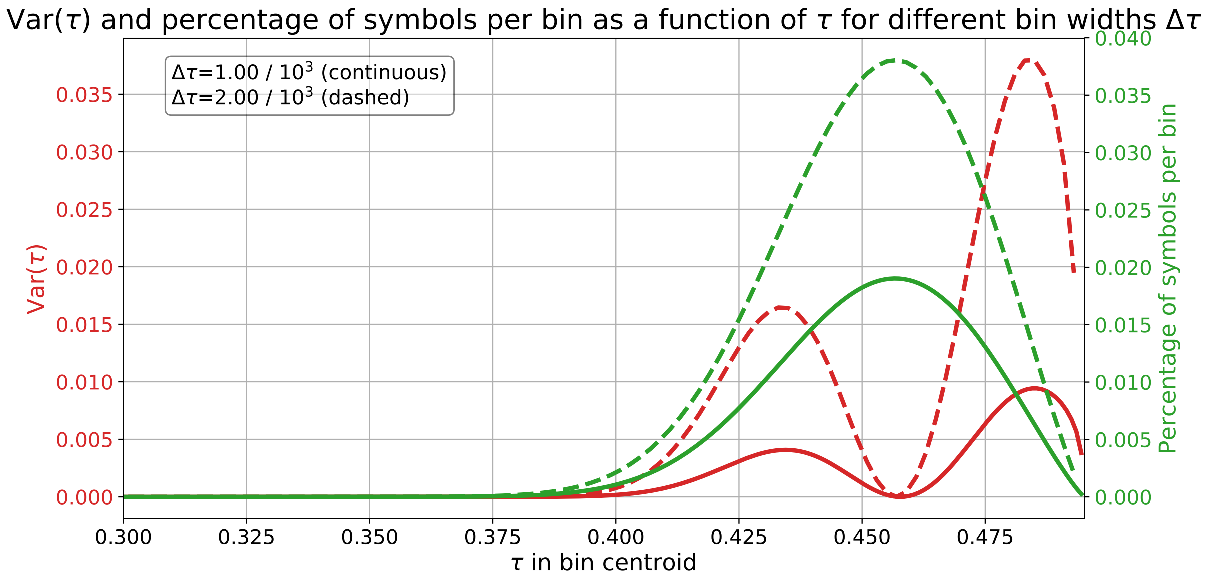


**Figure 8.7:** In red, variance of the transmission coefficient for the distribution $\mathcal{P}(\tau)$ for $\Delta\tau = 0.001$ (continuous) and $\Delta\tau = 0.002$ (dashed). The variance is more important where $\partial\mathcal{P}(\tau)/\partial\tau$ is high and it is accentuated as the width of the bins increases. For example, approaching the maximum of the peak in figure 8.6 (in the vicinity of $\tau = 0.46$) the derivative of the PDTC with respect to $\tau$ becomes smaller (the slope is softer) and we can see a reduction of the variance compared to the values of $\tau$ around it for which the slope (and hence $\partial\mathcal{P}(\tau)/\partial\tau$) is higher. The percentage of symbols is indicated in green for the same two values of $\Delta\tau$. Note that it is a scaled version of the PDTC that accounts for the fraction of symbols that are expected to fall in a certain bin and it will increase with the bin width, something positive for finite size effects.

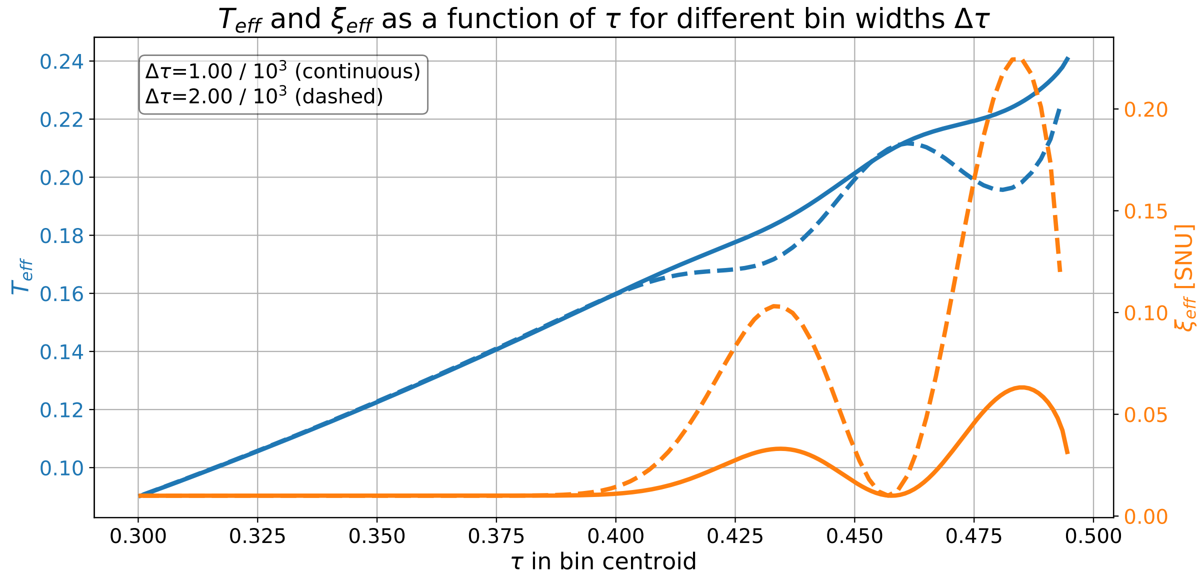


**Figure 8.8:** In blue, transformation of $\langle\tau\rangle$ and Var($\tau$) into $T_{\text{eff}}$ as a function of $\tau$ using equation 8.5. The curve is mainly below the straight line that would correspond to the fixed case, especially when Var($\tau$) is high which corresponds to high $\Delta\tau$. The same can be said for $\xi_{\text{eff}}$ represented in orange. For the calculation of $\xi_{\text{eff}}$, $V_A$ = 5.6 SNU (the optimal for the fixed case) and $\xi$ = 0.01 SNU.

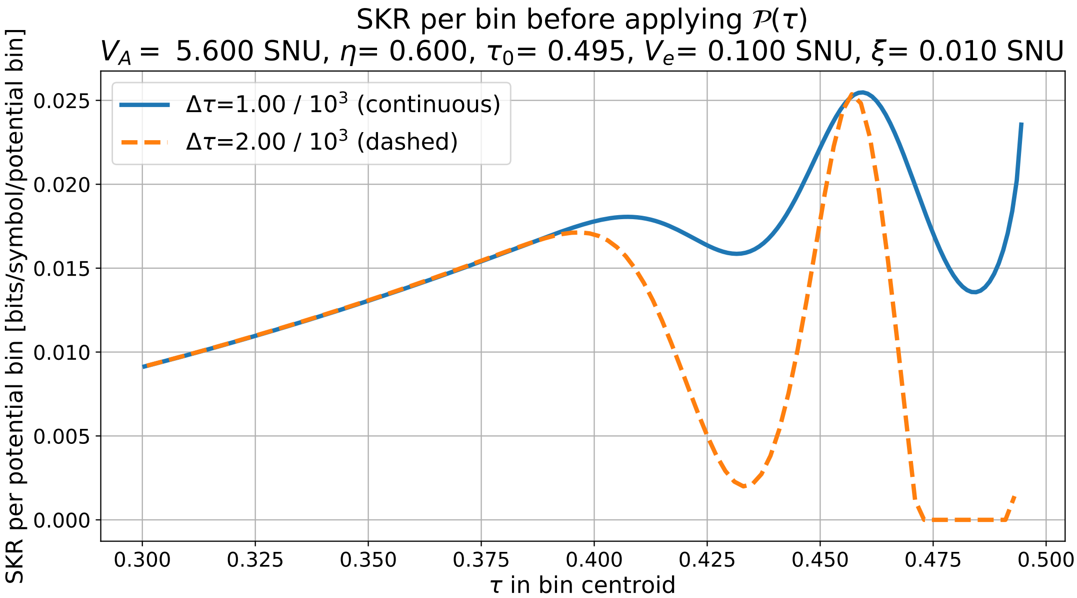


**Figure 8.9:** Secret key rate as a function of $\tau$ for the values of $T_{\text{eff}}$ and $\xi_{\text{eff}}$ in figure 8.8. Not all the values of $\tau$ in this figure are relevant in the PDTC (they need to be weighted by the percentage of symbols in the bin), so this SKR is still fictive. For example, wider bins can have lower potential rate, but it might be compensated by their higher percentage of symbols.

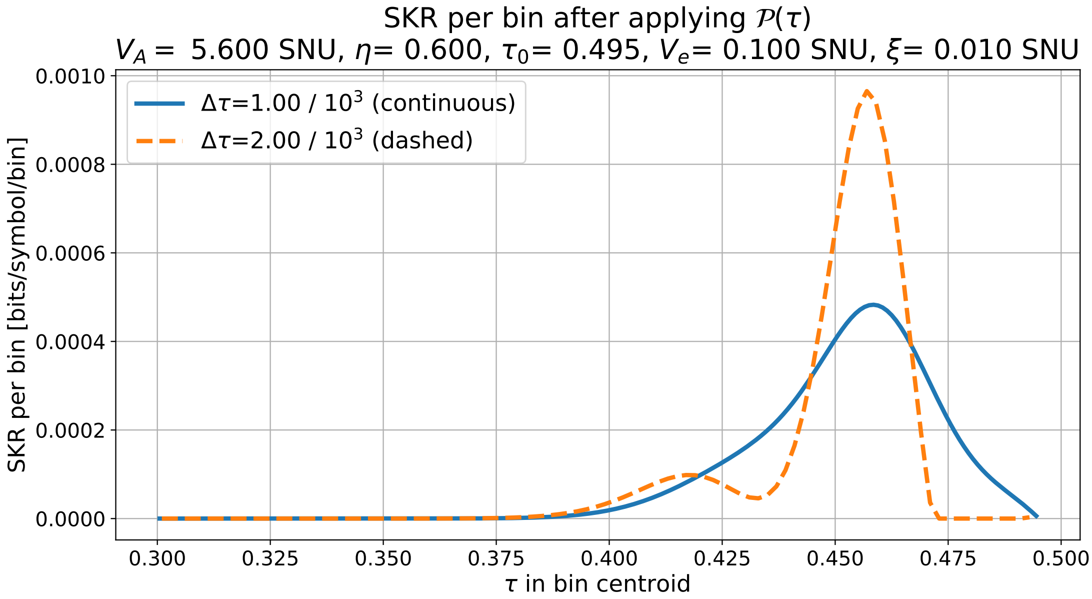


**Figure 8.10:** Secret key rate as a function of $\tau$ for the values of $T_{\text{eff}}$ and $\xi_{\text{eff}}$ in figure 8.8 ponderated by the PDTC. This represents the asymptotic secret key rate for each of the bins taking into account the percentage of symbols falling in each one. The aggregated asymptotic secret key rate is the sum of all the bins.

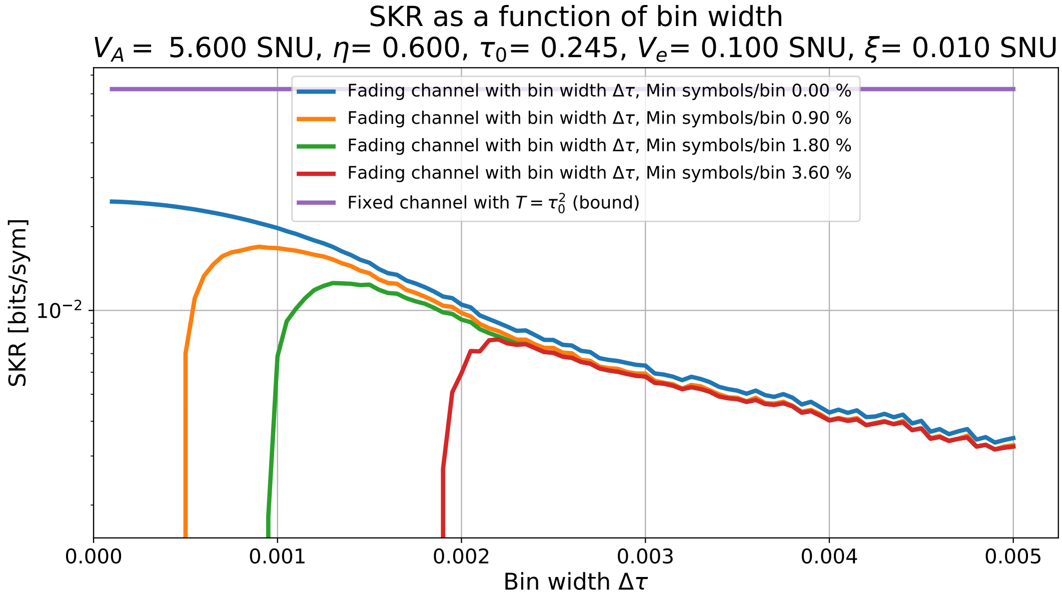


**Figure 8.11:** The secret key rate for the fixed channel of $T = \tau_0^2$ marks the bound for the used parameters. Without restrictions in the percentage of symbols it is optimal in terms of rate to use small bins, but as a minimum number of symbols per bin is imposed, it is necessary to increase the bin size, creating a trade-off situation. The irregularities in the curves can be explained by the non-uniformity of the effective parameters as the size of the bin evolves. A similar effect will be discussed in the next chapter in figure 9.7.

## 8.4 Experimental proposal

As it was described in the introduction of the chapter, a complete free-space optics link involves many components and it cannot be considered functional until it is tested under real conditions in the field, but for practical purposes it is interesting to study the influence of the different effects independently before a complete trial. With this idea in mind we propose a scheme to emulate the most relevant events that influence the free-space link. We study the suitable CV-QKD techniques and propose a proof-of-principle set up that is currently under development by the team.

### 8.4.1 Suitable schemes

The fact of using a non-guided medium for the quantum channel makes the transmission of high optical powers not advisable for security reasons. This has two main consequences: (1) the local oscillator cannot be transmitted through the channel, so we will restrict the choices to LLO schemes; (2) there is a limit to the power of the classical beacon, but we will consider that it is sufficient for the purpose of binning. At certain wavelengths and locations, there might be legal limits to the optical power, either peak or average. In some cases it would be beneficial to use a CW scheme as the power is more homogeneously distributed in time.

LLO schemes over fading channels require a DSP capable of recovering the mode at the reception under varying conditions. As discussed previously, it should be decided if the DSP tasks are performed before of after the binning. It will be assumed that part of the transmitted symbols are used as reference by the DSP.

Most of the modulation methods are feasible in principle, and one or two polarizations can be used. In cases of high loss or high variability, it would be necessary to support high values of excess noise, which make Gaussian modulation formats more robust in general.

### 8.4.2 Emulation of a free-space link

The variability of the channel is the main difference between fibre and free-space links and it is mainly caused by two factors: (1) the fading introduced by the channel; (2) the coupling of light to the detector. Both effects could be modelled and simulated numerically, but it is interesting to study their effect under realistic conditions, especially in the second case due to its more intrinsic technical nature.

The effects of a known arbitrary fading channel can be emulated using an amplitude and phase modulator (relatively slow with respect to the symbol rate). The modulators are fed with samples generated by a software configured to produce the desired fading. The effects of the polarization rotation can be added modulating a polarization controller in a similar way. It is technically simpler to implement those elements in fibre, but a free-space implementation would be analogous.

The coupling of light is a more complex and technical task. The first step is to introduce lenses that couple light in and out the fibres, but in a real scenario the signal wave front would have suffered distortions, so an additional mechanism is required to recover the wave front. This is generally accomplished by the use of adaptive optics techniques.

### 8.4.3 Proposal for a proof-of-principle free-space CV-QKD experiment

With the previous considerations a set up comprising the following physical elements is currently under test:

- **Alice.** Can be implemented using fibre components.
  - Narrow linewidth laser that generates the coherent states at Alice.
  - Stable laser to be used as classical beacon.
  - Fast modulation system (e.g.: $LiNbO_3$ IQ or amplitude and phase modulators).
  - Wavelength division multiplexer to combine beacon and quantum signal.
  - Variable optical attenuator and power meter to regulate the output optical power.
  - Fibre output.
- **Channel.** Most of the effects can be implemented using fibre components.
  - Fibre input.
  - Phase modulator.
  - Amplitude modulator.
  - Polarization controller.
  - Coupling from fibre to free space with a lens.
  - Free-space.
- **Bob.** The adaptation with respect to the fibre set up are in the coupling from free space and the requirement to detect a classical beacon.
  - Receiving lens to couple from free-space to fibre. This can be more sophisticated once the adaptive optics system is implemented.
  - WDM demultiplexer to separate beacon and quantum signal.
  - Narrow linewidth laser for the local oscillator.
  - Coherent receiver for quantum symbols.
  - Intensity detector for classical beacon signal.

The first objective is to establish a CV-QKD communication link with a well aligned optical path using standard CV-QKD DSP. Once the stable link is functioning a fading process is simulated in the channel to test the robustness of normal CV-QKD processing without binning. Binning is then introduced to improve the secret key rate generation.

The effects of wave front adaptation are more complex to test and will be taken into account in future steps. Observe that most of these processes require only software changes, except for the additional acquisition of the classical beacon and the tracking and adaptation of the wave front.

## 8.5 Conclusion

We have shown that the fading present in free-space channels can spread the dispersion of the transmittance compared to a fixed channel. It the channel can be subdivided in sub-channels as a function of their expected transmittance the corresponding fading to each of them would be lower than the total. This allows the execution of CV-QKD by sub-channels obtaining a higher aggregated SKR.

In order to do the sub-channel separation (binning), a method using a classical beacon is proposed. An example illustrates that it is possible to obtain secret key over a fading channel if the range of transmission coefficients in each bin is chosen correctly.

# Feasibility study of satellite CV-QKD

# 9

The main purpose of this chapter is to study the possibility of establishing secret keys over a satellite link using CV-QKD. For this we will extend the binning methodology of the previous chapter to non fixed objects, in particular to satellites orbiting the Earth and communicating with the ground.

The particularities of satellite communication are introduced and the most promising near term scenario is selected as case of study. A method to calculate the probability distribution of the transmission coefficient (PDTC) for the overall trajectory is proposed and the binning method is applied to calculate the secret key rate as a function of the altitude and other parameters. Possible improvements and additional cases are discussed at the end of the chapter.

9.1 Distinctive satellite communication properties . . . . . . . . 133
Scenario of analysis . . . . 135
9.2 Estimating secret key rate of a satellite passage . . . . . . . . 135
Satellite trajectories . . . . 136
PDTC of satellite passage 138
Expected secret key rates . 140
9.3 Other scenarios . . . . . . . 143
Uplink . . . . . . . . . . . . 143
Inter-satellite . . . . . . . . 144
Geostationary . . . . . . . . 144
9.4 Conclusions . . . . . . . . . 144
Extensions to the present analysis . . . . . . . . . . . . . . . . . 145

## 9.1 Distinctive satellite communication properties

Thanks to Newton and Kepler it is well known that, in the absence of drag forces, celestial bodies move following predictable trajectories. We will consider the case of orbits travelling around the Earth at different altitudes $H$. Relative motion is the most distinctive characteristic of this communication method, so to establish communication between two entities we will need a system capable of estimating the position of the objects and pointing dynamically the antennas/telescopes to the right locations (this is of particular importance in the optical regime).

Even after the entities are correctly aligned by the pointing system, their relative distances (slant range) will not be constant during the communication time, which in general will be finite. It is then necessary to estimate the distribution of slant range between the two objects as a function of the range and extrapolate the probability distribution of the transmittance taking into account the time spent at each slant distance. This distribution will not be a delta function, so the fact of communicating over a trajectory will introduce fading, which in principle could be mitigated using the binning techniques studied in the previous chapter.

If we want to use binning to reduce the effect of fading in a satellite link, we need to use a beacon as reference for classification. This is already common practice in many optical communication satellites, that require this feature for alignment and pointing, but typically in unrelated wavelengths. In our case the information and beacon wavelengths should suffer the same fading effects so ideally their modes should be close to each other.

The fact of using electromagnetic waves to communicate between objects in relative motion will introduce Doppler effect, producing detuning between the lasers of the two entities. As the involved carrier frequencies and velocities are both high, the detuning factor can be very important (see appendix E for more details). It will be assumed that it can be corrected by classical means.

Apart from the trajectory, the optics will play an important role in the attenuation of the link. The distances are typically high, so it is interesting to use a very narrow beam in the transmitter, which implies a transmitter telescope of sufficient size as a function of the wavelength. Typically the beam spot $W$ at the level of the receiver will be wider than the aperture $a$ of the receiving telescope. Wider optics at the receiver will be able to collect a bigger fraction of the light and will be beneficial in general, but they can be costly and not portable.

Depending on the elevation above see level satellite orbits are typically divided into Low Earth Orbit (LEO, up to 2 000 km), GeoSynchronous Orbit (GSO, at 35 786 km), Medium Earth Orbit (MEO, between LEO and GSO) and High Earth Orbit (HEO, above GSO). Taking into account that the radius of the Earth is 6 371 km the range of orbits is immense and not all of it is used. Most man-made objects in space are in LEO since it is easier and less costly to deploy them. Their round trip communication times are also faster than those of higher altitudes but their times of sight are also shorter. The Geosynchronous Equatorial Orbit (GEO, a special case of GSO that locates the satellites around the Equator) is very interesting for broadcasting in the RF bands, since the satellites appear to be static with respect to the ground and no dynamic pointing is required. MEO is mainly populated by Global Navigation Satellite Systems (GNSS) such as GPS, Galileo and Glonass, with orbits approximately 20 000 km away from the Earth (i.e. with a period of 12 hours).

Communication between satellites is interesting, but probably the most commercially attractive case would be to establish a secret key between a ground station and a satellite. If we are able to do this with a satellite $S$ using two physically separated ground stations $G_1$ and $G_2$, then it is possible to establish a secret key between $G_1 \leftrightarrow G_2$ using only XOR operations on the secret keys between $G_1 \leftrightarrow S$ and $G_2 \leftrightarrow S$ [109]. This would allow the exchange of keys using QKD at arbitrarily long distances around the globe.

Communications between ground and satellite imply that the communication medium will not be homogeneous. It would be vacuum in the vicinity of the satellite (and for most of the path) to increase in density until it reaches that of habitable atmosphere at the level of the ground station. In terms of perturbations in the link it is not symmetrical, since when Alice is in the satellite (downlink) the atmosphere is only affecting the final part of the communication (around 10 km), and the disturbance is minimal. When Alice is on the ground (uplink), the dispersion on the atmosphere occurs at the beginning and it broadens the transmitted beam more severely than in the downlink case. This phenomenon is usually called shower curtain effect.

The aberrations suffered by the optical wave front in the transmission would reduce the interference at the receiver, affecting the communication. In order to correct the aberrations, it is possible to use adaptive optics schemes, as mentioned in the previous chapter.

The logical first attempt would be to establish communication with LEO satellites since the attenuation would be lower, but they have the inconvenience of travelling fast, so it is important to take into account the dynamic pointing, the Doppler effect and the possible finite size effects in the parameter estimation for CV-QKD.

Satellite communications can consider more subtle effects like the effect of gravity in the satellites, the requirements of clock synchronization at high speeds or the influence of background noise. They will not be taken into account in this analysis.

### 9.1.1 Scenario of analysis

Taking into account the previous remarks, in the following section we analyse the satellite to ground downlink scenario, where Alice transmits her quantum states from the satellite to Bob, located in a ground station. Both are equipped with common free-space CV-QKD adapted to satellite communications, i.e. certified for space missions and with the required mechanisms for tracking and authenticated classical communications.

We will assume that mechanisms to correct the pointing, the aberrations in the wave front and the Doppler shift exist. In our model they will contribute with a fixed value of untrusted loss, meaning that in the trusted detector secret key estimation it will be added to the the attenuation of the channel, not to the trusted attenuation of the detector.

The proposed scheme does not depend on the used wavelength, but it is interesting to use wavelengths for which components are readily available in the market. Transmitters and detectors are well suited for 1550 nm, but modifications on the typical satellite optics might be needed to work at those wavelengths.

## 9.2 Estimating secret key rate of a satellite passage

This section describes the steps to be performed in the estimation of the expected secret key that can be obtained using orbits in the downlink configuration. The trajectory of study is calculated using geometric relations and the PDTC can be obtained at differential points of this trajectory. With the PDTC at each point and the time intervals of the differential points the secret key rate can be calculated.

### 9.2.1 Satellite trajectories

A geocentric coordinate system can be used to describe any point in the trajectory of a satellite, taking the center of the Earth as origin, in which case a point in the path is completely defined by: (1) the declination angle $\delta$ that corresponds to the angle of the point with respect to the equatorial plane; (2) the inclination angle $\iota$ with respect to some reference longitude; and (3) the distance to the center $R$.

In order to simplify the analysis we will assume that the satellites follow perfectly circular polar orbits at an altitude $H$ and communicate with an observer located at see level altitude in latitude $\psi$. The Earth is also assumed circular with radius $R_\oplus = 6371$ km. For this particular case the distance to the center is constant $R = R_\oplus + H$, as well as the angular velocity $\omega_{\text{sat}}$ which determines regular time intervals at the same latitude $\psi$. With $M_\oplus = 5.972 \times 10^{24}$ kg the mass of the Earth, the only variable for those values is the altitude $H$:

$$\omega_{\text{sat}} = \sqrt{\frac{GM_\oplus}{(R_\oplus + H)^3}} \tag{9.1}$$

$$T_{\text{sat}} = \frac{2\pi}{\omega_{\text{sat}}} \tag{9.2}$$

With the previous considerations it is easy to formulate the trajectory in geocentric coordinates with respect to a latitude $\psi$ as a function of the declination angle $\delta$. Typically we will be interested in an observer located in a longitude or initial inclination $\iota_0$ that we can set to $\iota_0 = 0$ at the longitude of the observer. For the n-th passage of the satellite, due to the relative rotation of the Earth with respect to its orbit, the new inclination angle will be $\iota = \iota_0 + n \cdot \Delta\iota$. If we denote the velocity of a point in the equator as $v_\oplus = 463.83$ m/s, the change in inclination is calculated as

$$\Delta\iota = \frac{T_{\text{sat}} v_\oplus}{R_\oplus} \tag{9.3}$$

To be strict, $\iota$ also changes slightly during the passage of the satellite, but we will omit this effect here. The relation between the inclination angle and the period of the satellite with respect of the altitude can be seen in figure 9.1.

While the geocentric coordinate system is very practical, the main interest is to define the trajectory of the satellite with respect to a point on the surface at a latitude $\psi$ (and inclination $\iota$, but we can set it to zero and work only with $\Delta\iota$). For this it is useful to translate the coordinate system to the surface of the Earth at latitude $\psi$ and figure 9.2 can be used for help. We define the zenith point $\mathcal{Z}$ as the imaginary point in the sky that is aligned with the observer and the center of the Earth. We call zenith angle $Z$ the inclination with respect to that point $\mathcal{Z}$ as seen by the observer[54] . The other angle required to characterize the position of a satellite is the azimuth angle $A$, which indicates the horizontal angle of the observer. Angles $A$, $Z$ form a cone that covers an

[54] 54: The complementary of the zenith angle $Z$ is called elevation angle.

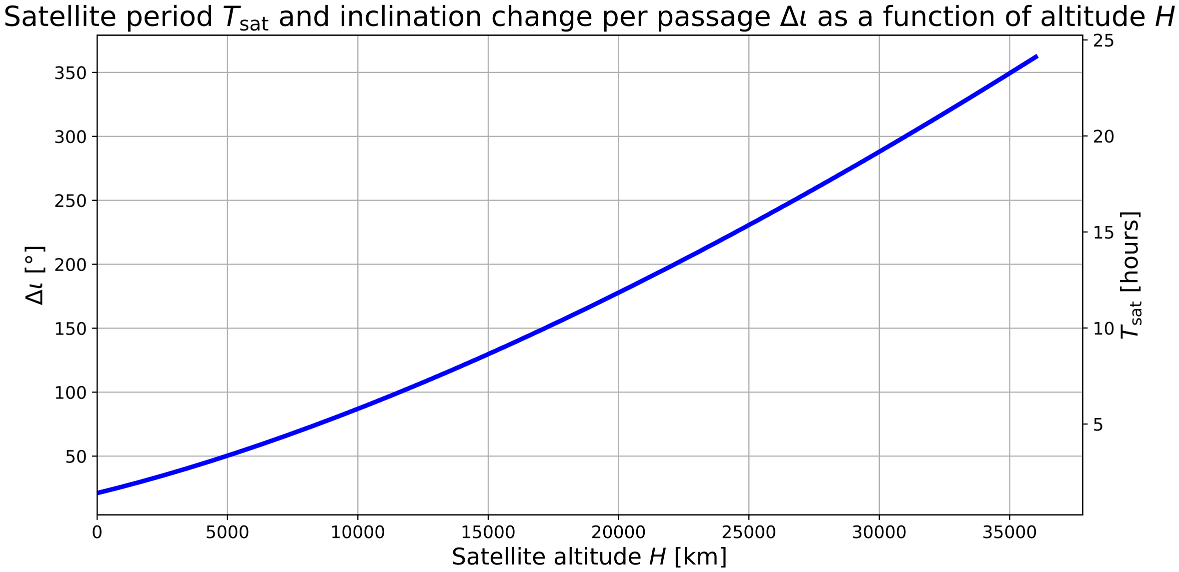


**Figure 9.1:** Satellite inclination angle and period with respect to the altitude for circular polar orbits. One of the main parameters when deciding the altitude of the orbit of the satellite is its period over a fixed latitude. It is common to choose sub-multiples of the day, for example GNSS satellites orbit at approximately 20 000 km, which corresponds to a period of 12 h, i.e. two passages per day over the same latitude. The inclination angle $\iota$ changes in a proportional way to the period. Both values are lower bounded by the radius of the Earth, but in practice this bound is higher since the density of the atmosphere below a few hundred kilometres would prevent stable orbits.

infinite distance in the sky. The slant range $L$ is the shortest apparent distance between the satellite and the observer, and completes the determination of a point in the surface system.

The observer only needs to know $A, Z$ to be able to track a satellite in the sky, independently of $L$. The satellite will not always pass directly above the observer[55] , so the interval of the zenith angle will be lower bounded as a function of the altitude. We can also consider an arbitrary higher bound to take into account practical implementations of aiming ground telescopes very close to the horizon. For the analysis we took $Z_{\mathrm{max}} = 70°$ and the zenith angle along the declination angle $\delta$ will be bounded by $Z(\delta) \in [Z_{\mathrm{min}}(\iota), Z_{\mathrm{max}}]$.

In order to calculate the PDTC at a certain location in the sky the most relevant parameter for us will be the slant range $L$ since it will be the main source of attenuation, so it is interesting to be able to calculate this parameter from the geocentric system. This can be done using basic trigonometric relations:

$$A = (R_\oplus + H)\cos(\delta - \psi)\cos(\iota) - R_\oplus \tag{9.4}$$
$$B = (R_\oplus + H)\sin(\delta - \psi) \tag{9.5}$$
$$C = (R_\oplus + H)\cos(\delta - \psi)\sin(\iota) \tag{9.6}$$
$$L = \sqrt{A^2 + B^2 + C^2} \tag{9.7}$$

Another important parameter is the communication time $t_{\mathrm{com}}$ which can be calculated as $t_{\mathrm{com}} = \frac{\Delta\delta}{\omega_{\mathrm{sat}}}$. For the same inclination angle $\iota$, higher

[55] When $\iota = 0$ the satellite passes directly above the ground observer and the shortest slant distance $L(Z = 0) = H$ can be achieved. The time of view of the satellite is also the longest possible, so it is generally denominated "best pass". The inconvenience of this pass is that it requires the observer to operate with very low zenith angles, which is not always possible.

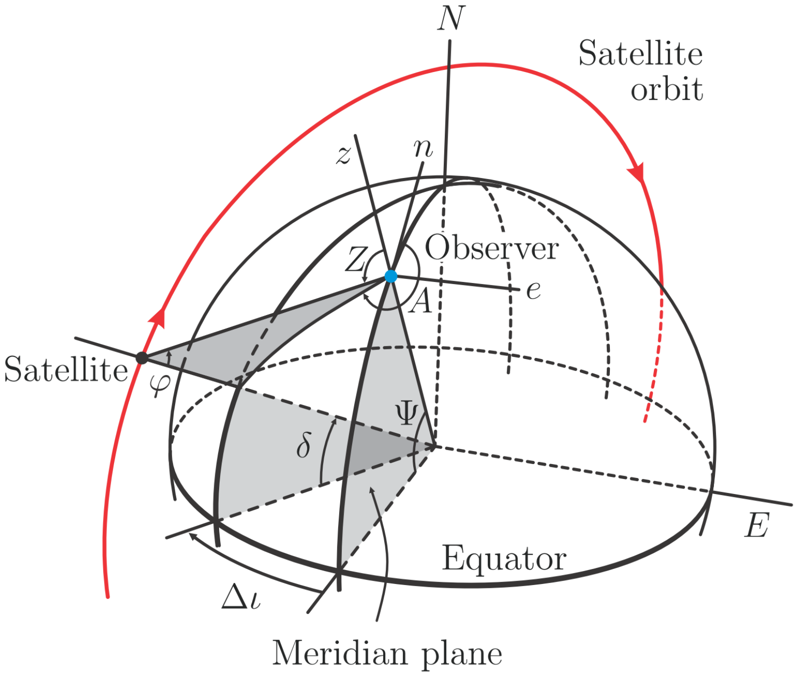


**Figure 9.2:** Relation of the angles used in this chapter. Image source: [107].

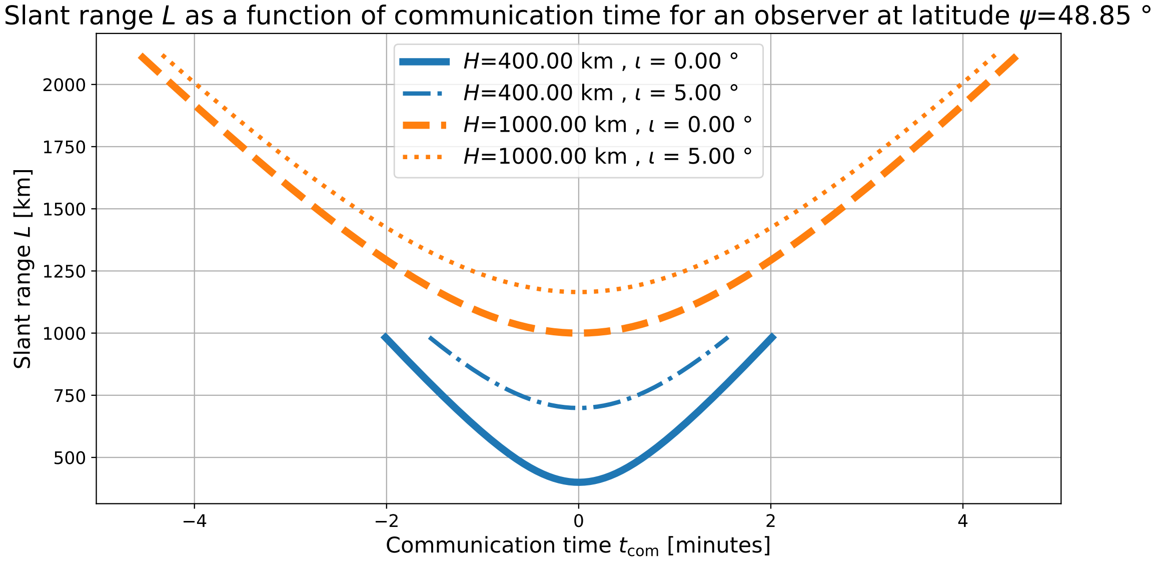


**Figure 9.3:** Satellite slant range for two different altitudes and inclinations. Higher orbits will be visible during longer times between the allowed zenith angles, but their attenuation will also be higher. An inclination $\iota = 0$ is optimal in the sense that higher inclinations of the same orbit height have less communication time and higher slant distances. The effect of inclination becomes less relevant with the altitude of the satellite.

altitude satellites will have longer communication times, but their slant distance $L$ (and hence the attenuation) will be higher, as can be seen in figure 9.3.

### 9.2.2 PDTC of satellite passage

The previous expressions allow us to calculate the expected slant distance $L$ at a latitude $\psi$ as a function of time (the time is directly proportional to the declination angle $\delta$ in a circular orbit), inclination of the orbit $\iota$ and altitude of the satellite $H$. The next stage is to divide the trajectory in differential steps and calculate the expected PDTC of each point of the trajectory. It is assumed that the observer will accumulate the values of all the satellite passage to process them later, so the combined PDTC would be the weighted sum of the PDTCs for each point in the trajectory. If the differential times are constant (which is the case for constant $\Delta\delta$ values) the weight of all the points is the same.

In order to calculate the expected PDTC at each point we used the log-negative Weibull distribution as described in [110] and in the appendix D. This model requires to know the aperture of the receiving telescope $a$ and the radius of the beam at the receiver $W$, as well as a variance value $\sigma^2$ to take into account the fluctuations. With these considerations, apart from the geometry of the trajectory, the parameters that will play a role in this model are:

- The radius of the receiving telescope $a$.
- The deviation angle $\theta_d$ that indicates the dispersion of the beam arriving from the satellite. Along with $L$ it will determine the beam width at the receiver $W = L \cdot \theta_d/2$ (if $\theta_d$ is given as a full angle).
- The pointing uncertainty angle $\theta_p$. The fluctuations will be mainly caused by the beam wandering due to the pointing, so they can be well approximated as $\sigma = L \cdot \theta_p/2$ (if $\theta_p$ is given as a full angle).

The shape of the PDTC for a fixed point is already known from the previous chapter (see figure 8.6). The values of the transmission coefficient are upper bounded by $\tau_0$ and there is a peak shortly below this value, depending on the variance $\sigma^2$. During the trajectory the values of $\tau_0$, $W$ and $\sigma$ will vary, but the shape will remain similar. The probability distribution resulting from adding the contributions of all the differential points will then be upper bounded by the highest $\tau_0$ in the trajectory and will have a resonance peak not far from it to decrease again until a likely second resonance in the order of the lower values of $\tau_0$ in the trajectory.

The losses in the receiver that we cannot include in the trusted $\eta$ will be considered fixed, and the corresponding transmission coefficient will be added to the PDTC (a multiplication in natural units), so a more compressed version of the PDTC is expected after considering these losses. The values considered are 0.8 dB due to the fact of using the main peak of the Airy diffraction pattern, 3 dB due to the fibre coupling losses and a pessimistic value of 3 dB due to the scattering absorption in the atmosphere [111], summing up to 6.8 dB.

We will use a trajectory passing by $\psi = 48.85°$ (Paris latitude) and $\iota = 0°$ at an altitude of 800 km to illustrate the main effects of the different parameters. In figure 9.4 we can see the evolution along time and the comparative effects of altitude, receiver aperture size and pointing error. If figure 9.5 we can see those effects on the accumulated PDTC of the entire passage. It is normalized to form a probability density function along one passage.

As expected it is convenient to use receiving telescopes with big radius and high precision in the pointing. Low orbit satellites have PDTCs with higher $\tau_0$ and more homogeneous distributions. This would introduce lower excess noise due to fading using the binning method, which is advantageous in terms of key rate. If we use the secret key per passage as quality measure, and especially if we take finite size effects into account, it is possible that higher orbits can recover part of the performance, since their communication times are longer than those of the lower orbits.

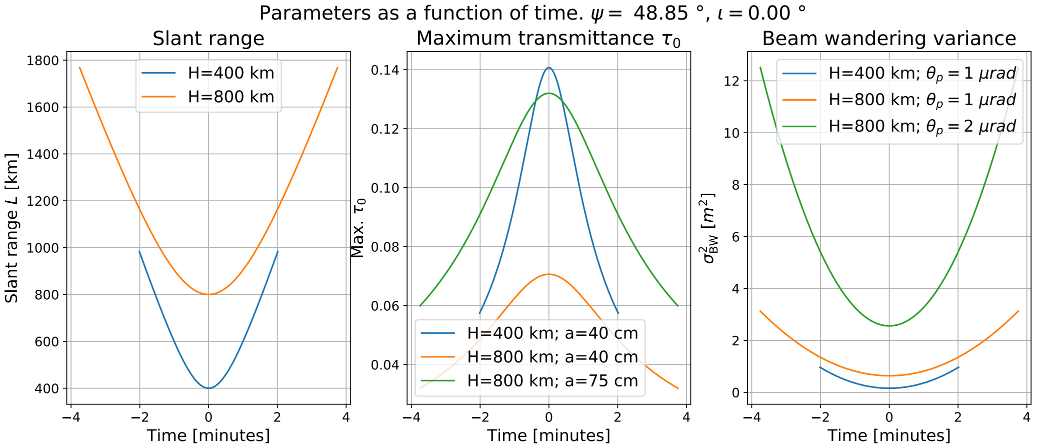


**Figure 9.4:** Variation of parameters during satellite passage. **Satellite altitude:** if $H$ is reduced to 400 km the slant distance is shorter and the maximum transmission coefficient is higher; the beam wandering variance is also higher for higher orbits. **Aperture radius:** an increase in the receiving aperture radius allows the improvement of $\tau_0$. **Pointing error:** high uncertainty angles increase $\sigma^2_{BW}$. **Time:** lower orbits have shorter communication times.

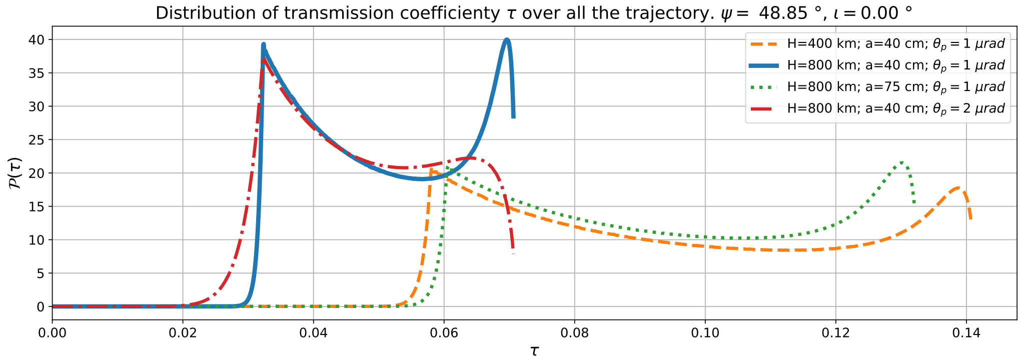


**Figure 9.5:** Influence of receiver size and pointing in passage PDTC. The bold blue curve can be used as reference for diverse effects. **Satellite altitude:** the distribution is narrower and with lower $\tau_0$ for higher altitudes. **Aperture radius:** the distribution gets broader if a bigger telescope is used at the receiver. **Pointing error:** lower pointing errors allow to resolve a finer version of the PDTC. The difference with figure 8.6 is substantial.

### 9.2.3 Expected secret key rates

Once the expected PDTC is calculated it is possible to estimate the key rate under fading conditions as in the case of a fixed fading channel. In the satellite scenario, the time gains more relevance since the communication time is limited to one or several passages. For this reason we will introduce the impairments produced by the finite size of the samples used in the parameter estimation. As seen in chapter 2, the statistics over $m$ symbols used in the parameter estimation can be bounded to a certain confidence parameter $\epsilon_{PE}$. If we decide to choose the limits of the confidence intervals for the transmission coefficient $\tau$ and the noise $\sigma_n^2$ we can sacrifice key rate to maintain security, and the parameters used in the estimation are transformed as

$$\tau_{FSE} = \sqrt{T_{\text{eff}}} - z_{\epsilon PE/2}\sqrt{\frac{\sigma_n^2}{mV_A}} \tag{9.8}$$

$$\sigma_{FSE}^2 = \sigma_n^2 + z_{\epsilon_{PE}/2}\frac{\sigma_n^2\sqrt{2}}{\sqrt{m}} \tag{9.9}$$

where the parameter $z_{\epsilon_{PE}/2} = \sqrt{2}\,\text{erf}^{-1}(1 - \epsilon_{PE})$ and for the typical value $\epsilon_{PE} = 10^{-10}$, $z_{\epsilon_{PE}/2} = 6.5$. Combining these calculations with the binning requires to do these calculations for each of the bins, with the $m$ corresponding to each bin, so the symbol rate needs to be taken into account in the estimations. The finite size effects will be small if $m$ is big, so more probable bins will be less affected by this consideration. Bins with low values of $m$ could be discarded as the key generated from them would be relatively low.

It is important to estimate the key rate that can be obtained as a function of the altitude of the satellite. In order to to so, for each satellite altitude $H$ the following sequence is followed:

1. The trajectory is calculated according to the coordinates.
2. The PDTC is estimated from the trajectory and the characteristics of the receiver and transmitter.
3. $V_A$ is assumed fixed for each satellite altitude, but its value is optimized in each altitude $H$ to the value of $\tau_0$.
4. Binning. Using the PDTC of the trajectory the division in bins is performed as in the previous chapter. For finite size effects, using the time of communication and the symbol rate, calculate the number of symbols that fall in each bin.
5. Calculate and add the effects caused by the fading in the PDTC.
6. Calculate and add the effects caused by the finite size in the parameter estimation.
7. Calculate the secret key rate and the secret key per passage.

In figure 9.6 the results for the expected secret key per passage and secret key rate are illustrated. The binning step used is $\Delta\tau = 0.001$, which is reasonable for the classic beacon classifier but not fine enough to follow perfectly the shape of the PDTC (the PDTC in the satellite has more sharp parts than the static case). This produces a discontinuous effect on the curves which could be solved with smaller steps $\Delta\tau$ or a more elaborate selection of starting points for the intervals (see figure 9.7 for an illustration). Even with this constraint it is possible to see that reasonable SKR can be achieved up to 2 000 km with a telescope of 40 cm radius in the ground. Working at 1 GBb or higher would mitigate the finite size effects notably so we can safely approximate the results by the asymptotic ones at those rates. The SKR is integrated to calculate the total key per passage and normalized to 1 Bd to simplify comparison. For example, during a passage of a satellite orbiting 1 300 km above the ground we could generate 1 Mbit of secret key operating at 1 GBd .

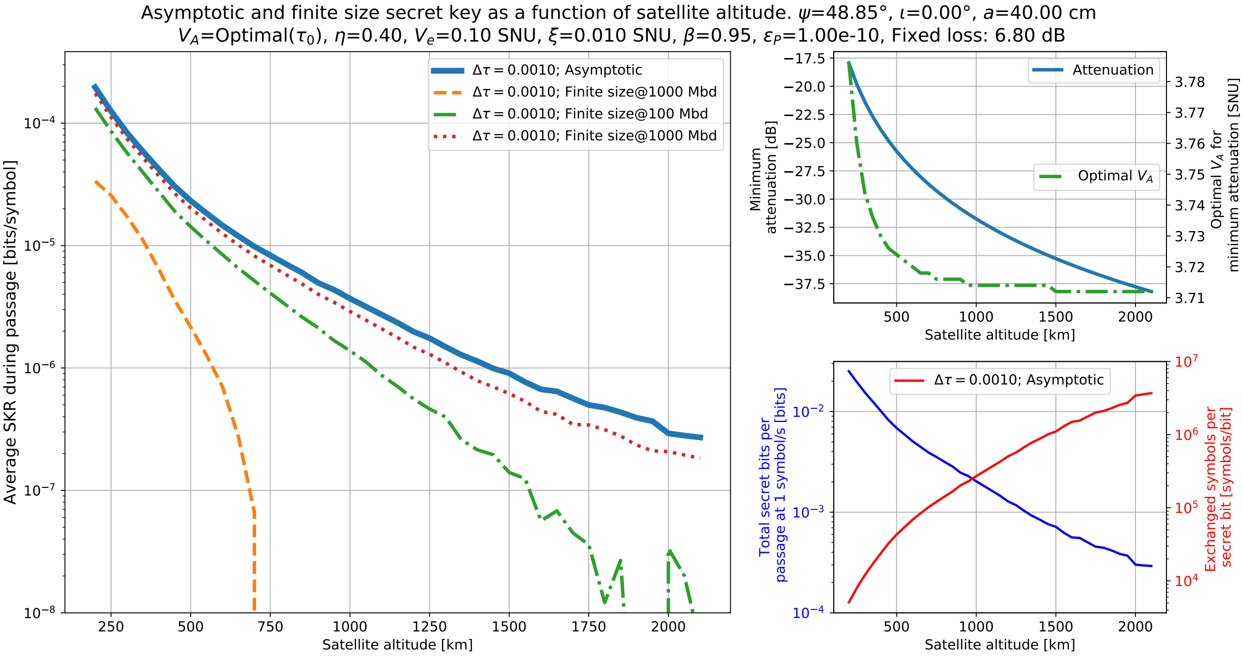


**Figure 9.6:** Average SKR over a passage as a function of satellite altitude for aperture of 40 cm. As in the fibre case the average SKR decreases with distance. The results taking into account finite size effects tend to be negligible for repetition rates higher than 1 GBd. The optimal $V_A$ tends to a fixed value as the expected attenuation increases. The total key rate is expressed by considering 1 symbol/s to facilitate the comparison and it needs to be multiplied by the repetition rate. The key rate per passage is represented along with the symbols required to generate a bit of secret key. For these two parameters only the values for the asymptotic case are represented for simplicity.

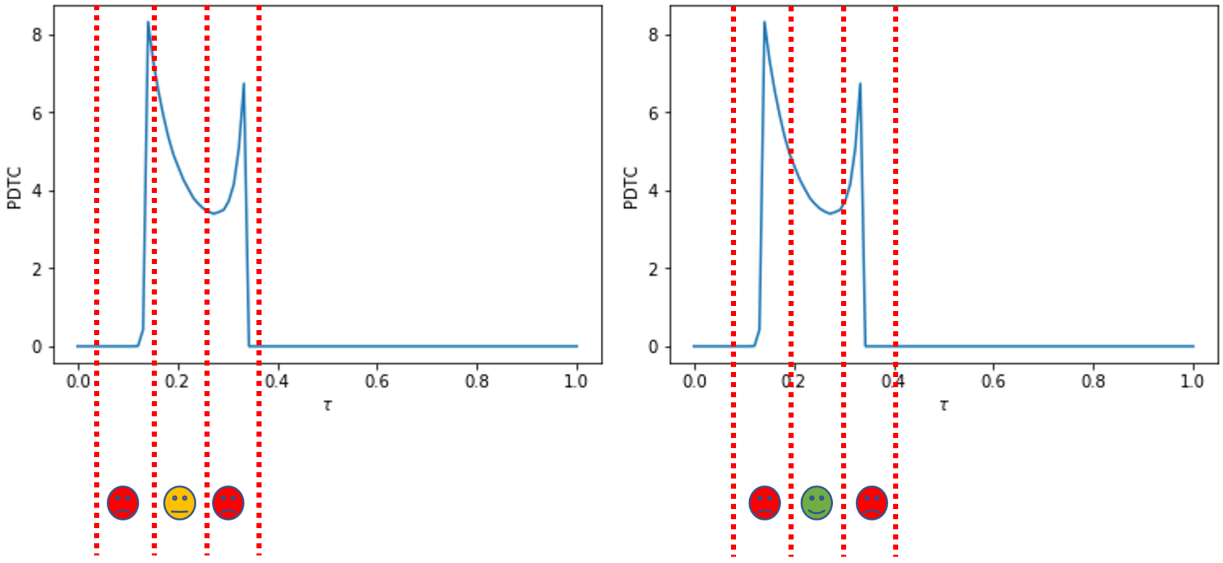


**Figure 9.7:** Influence of offset in the performance of the binning. An exaggerate bin width is presented for illustration of the influence of the position of the bin relative to the PDTC. In cases where the distribution inside the bin is less regular the achievable SKR will be lower. As the slant distance becomes larger the PDTC will be narrower and this effect will be more significant. This problem could be solved implementing a mechanism to optimize the bin size and position.

If we have a telescope on the ground with larger diameter we could extend the operation to higher altitudes, as shown in figure 9.8. In the asymptotic case the improvement in achievable altitude is substantial if we are able to obtain narrow bins, but the finite size effects are significant for a repetition rate of 1 GBd. In order to approach the asymptotic curves higher symbol rates must be used, which is not a fundamental obstacle, only a technical one. The discrimination of the PDTC in narrow beams for high altitudes might be also challenging. A possible solution is the adaptation of the classical beam power to the altitude in order to maintain the resolution, independently of the orbit of the satellite.

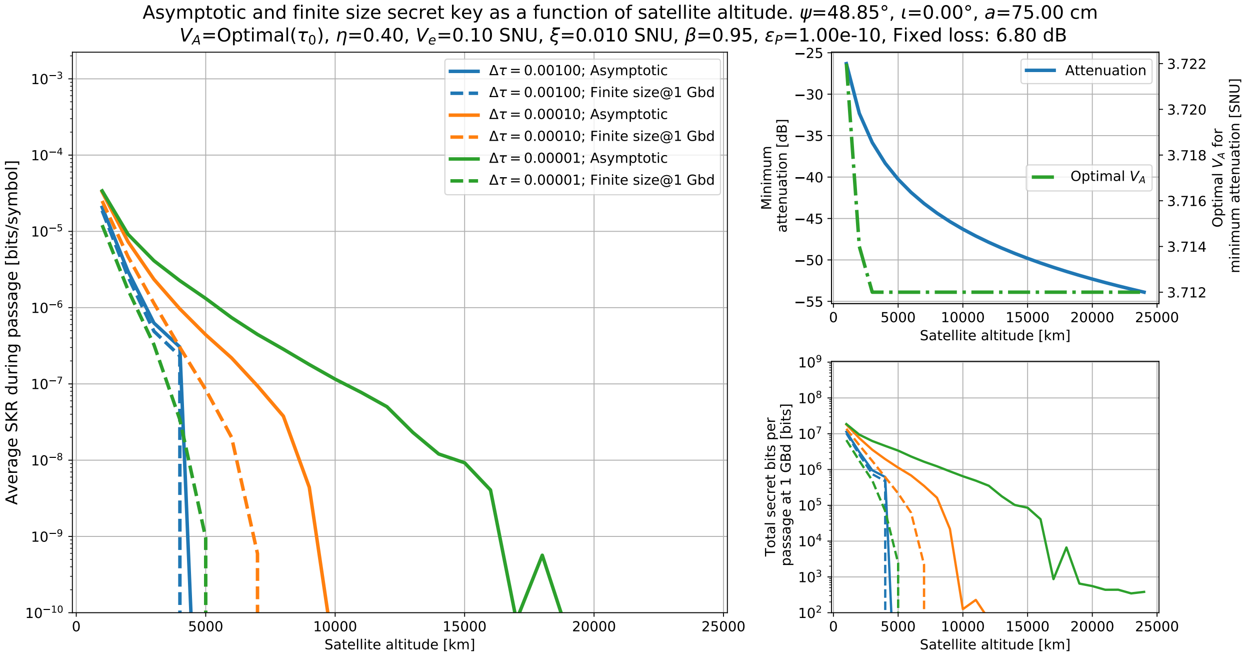


**Figure 9.8:** Average SKR over a passage as a function of satellite altitude for aperture of 75 cm. Three bin widths are considered in the asymptotic and finite size cases at 1 GBd. At this rate finite size effects would limit the communication distance. The irregularities in the curve are caused by the effect described in figure 9.7.

## 9.3 Other scenarios

The techniques discussed previously could be applied with slight variations in other scenarios of interest. The main difference would be the model considered for the PDTC.

### 9.3.1 Uplink

Uplink and downlink might seem very similar since the described trajectory is the same. The same analysis could be done taking into account a fading model that considers the shower curtain effect mentioned above. As a rule of thumb the link losses for the same satellite altitude are 10 dB higher in the uplink scenario.

The fact of having Alice on the ground and Bob on the satellite would simplify the computational requirements for the satellite (assuming reverse reconciliation) and potentially the complexity of the hardware, since only a coherent detector with a local oscillator would be needed for the optical path.

### 9.3.2 Inter-satellite

The optical communication between satellites is very interesting due to the high bandwidths that can be achieved and the reproducibility of the conditions due to the fact of operating in the vacuum of space. Of particular interest is the communication from MEO satellites using LEO satellites as relays. The communication between the satellites can be done at high rate in the optical regime while the communication with the ground can be reliably performed in RF.

The number of possible trajectories resulting from combinations of orbits would be enormous and undoubtedly of great interest. The main challenge would probably be the communications at great distances, since the required optics would be relatively large for a standard satellite. In cases of satellites with similar altitude and inclination the expected communication times would be relatively long.

### 9.3.3 Geostationary

The two main advantages of the geostationary orbit are that it does not require pointing and the communication time can be made arbitrarily long (except for the weather conditions). The main and considerable drawback is the loss introduced by the great distance to the ground (35 786 km at the Equator, higher elsewhere). It could be improved with wide aperture optics, but it is not likely to be lower that 45 or 50 dB. Even in the asymptotic case the requirements in terms of excess noise to work at this regime are quite stringent (below mSNU), before considering the excess noise due to fading. It cannot be discarded as an option, but it would require significant technological investments.

## 9.4 Conclusions

The proposed analysis considers the effects of beam wandering (caused mainly by the requirement follow the position of the satellite) as the major source of fading in a satellite to ground scenario. The results show that with these assumptions it is possible to calculate the expected distribution for the transmission coefficient (PDTC) in a system where the entities are not in relatively fixed positions. The binning technique can be applied effectively for LEO orbit satellites, where the PDTC distribution is sufficiently broad to be able to accurately separate different bins. For higher orbit satellites the effect of the fading is less relevant, but the distribution becomes very narrow and it would be difficult in practice to perform the binning technique. It is difficult in practice to achieve orbits higher than 5 000 km unless the beacon system provides very fine granularity in the classification of bins. Only the case of downlink scenario has been presented, but the method could be extended to more complex cases with simple modifications.

The required technology is not very different from the fibre case. In order to take into account finite size effects, a low electronic noise coherent detector working at rates higher than 1 GBd would be needed, but it is something already feasible in practice. The beacon system would need to be attached and its resolution should be as high as possible to reduce the fading at higher orbits.

### 9.4.1 Extensions to the present analysis

Although the main impairment is addressed in the proposed analysis, more elements could add up to the fading. In particular we have assumed that two practically challenging effects can be reliably corrected using particular separate solutions: wave front distortion and Doppler effect. The adaptive optics system has been modelled as an untrusted fixed loss but that in practice the process will not be constant and it would introduce fading. Unfortunately for the approach we followed, the modelling of those effects would be highly empirical, depending on each system. The residual Doppler effect after correction would introduce detuning in the received signal, so the bandwidth of the detector would need to be broader than the repetition rate of the signal maintaining good levels of noise.

The highly empirical nature of those effects suggests that an experimental approach should be desirable, but with all the elements considered (coherent communications, classical beacon, pointing, adaptive optics, Doppler compensation, adapted DSP...) the overall system is becoming highly complex. A set of incremental steps from the experimental proposal suggested in the previous chapter would be recommended.

In a more abstract sense the followed analysis could be extended to calculate the secret key rate that could be achieved in a network with multiple ground stations and a constellation of satellites travelling around the Earth. Combining it with expected weather conditions and the trajectories of the satellites, the expected availability of secret key for an area could be calculated. Several aspects could be taken into account: downlink, uplink and inter-satellite to favour the communication between two separated regions of land, which is usually the main purpose of satellite communications.

# CONCLUSIONS

# Conclusions 10

10.1 Bandwidth efficient CV-QKD . . . . . . . . . . . . . . . 150
10.2 On-chip CV-QKD . . . . . . 151
10.3 Free-space CV-QKD . . . . . 151

We have covered a wide range of aspects related to the improvement of CV-QKD technologies, from a theoretical study on the feasibility of the use of CV-QKD in satellite links, to three novel experimental implementations each one with its particular characteristics of interest. The main features of the proposed experimental set ups are displayed in table 10.1.

**Table 10.1:** Main characteristics of the presented experimental set ups.

| | **CW CV-QKD**<br>(chapter 4) | **High rate CW CV-QKD**<br>(chapter 5) | **On-chip detector**<br>(chapter 7) |
|---|---|---|---|
| **Signal** | CW | CW | Pulsed |
| **Local oscillator** | Transmitted/Local LO, CW | Local LO, CW | Transmitted LO, pulsed |
| **Modulation** | IQ or AM/PM, controller | DP IQ, controller | AM/PM, control by SW |
| **Constellation** | Gaussian | QPSK, PCS-QAM | Gaussian |
| **Polarizations** | 1 TX, 2 RX | 2 | 1 |
| **Detector architecture** | 90° hybrid | 90° hybrid | 180° hybrid |
| **Receiver** | DP 90°h + 4 × balanced det. | DP ICR | PIC |
| **Amplification** | TIA | TIA | Charge amplifier |
| **Intermediate frequency** | Homodyne/Intradyne<br>$0 \leq \omega_{\text{IF}} < B/2$ | Intradyne<br>$0 < \omega_{\text{IF}} < B/2$ | Homodyne<br>$\omega_{\text{IF}} = 0$ |
| **Demodulation** | DSP | DSP | Direct |
| **Phase reference** | QPSK | QPSK, blind, Kalman... | QPSK |
| **Symbol rate** | 1 to 50 MBd | 1 to 2.5 GBd | 1 MBd |
| **Processing** | Real-time | Off-line | Real-time/off-line |
| **Difficulties** | Low electronics bandwidth<br>Local LO | DSP complexity<br>Noise calibration | Low efficiency<br>Noise calibration |
| **Advantages** | Compatibility classical comms.<br>Configurable for CV-QKD<br>Upgradable to higher rates | Compatibility classical comms.<br>Phase tracking<br>High rate | Reduced size and cost<br>Integration potential<br>Heterodyne possible |

The possibility of using classical techniques like pulse shaping is very attractive for CV-QKD, since it optimizes the use of the bandwidth and avoids the requirement of carving the transmitted signal, working in CW. The use of DSP techniques can also simplify the set up, for example performing all the polarization recovery tasks by software using a polarization diverse detector (even in the case of sending information in only one polarization). It is also less stringent on the frequency matching of signal and LO, providing the possibility of working in intradyne mode.

The two CW schemes are the ones that share more characteristics and their hardware could potentially be the same. The acquisition hardware is the main limitation of the system described in chapter 4 but it is the price to pay in order to have a flexible system that can run in real time. Most of the tasks of a CV-QKD system could be performed off-line as in the high rate version of chapter 5, but it is difficult to acquire a sufficient number of symbols maintaining the appropriate calibration requirements on the shot noise (multiple acquisitions need to be made and the conditions might change).

The high rate system can deal efficiently with local LO configurations, since the relative phase of the two lasers can be estimated more accurately due to the high symbol rate. Also, as the used DSP was originally designed for classical communication systems, many configurable phase recovery schemes are available. Such a flexibility can also make the DSP more complex and difficult to adapt to CV-QKD, contrary to the lower rate system that was developed with CV-QKD in mind.

The proposed on-chip system uses a transmitted LO scheme, stringent in terms of use cases but simpler and more cost effective due to the its direct detection and low required bandwidths. It can provide a good platform for low end devices capable of operating at short distances (e.g. connection to trusted terminals). From the discussion regarding the obtained results, it is feasible that a non-defective version of the chip could obtain performances comparable to bulk devices.

The satellite feasibility study is in principle independent of the implementation once the aforementioned requirements are considered (classical beacon, tracking mechanism and adaptive optics mainly). Nevertheless, it indicates that a high rate CW scheme would be the most suitable approach, since the communication periods can be relatively short at LEO orbits and a sufficient number of symbols needs to be collected in order to overcome the finite size effects.

All the proposed experimental implementations allowed us to learn how to ameliorate the systems towards future implementations. The following sections cover the most interesting future improvements.

## 10.1 Bandwidth efficient CV-QKD

The approach of classical coherent communications and CV-QKD appears suitable for practical CV-QKD field deployments. They share practically the same components and two fundamental modifications would need to be implemented:

- A mechanism to calibrate regularly the shot noise in order to optimize the estimation of the excess noise. This condition could be mitigated if only small attenuations are targeted, since higher excess noise could be supported.
- A gain control mechanism (in the hardware and the DSP) that maintains a constant relation with the average number of photons at the input of the detector and the result of the DSP. This would allow the estimation of the channel transmittance $T$.

The recent advances in discrete modulation security proofs should also encourage the use of these technologies, although the introduction of higher density constellation is a path already in progress in classical communications. These constellations resemble a Gaussian modulation and should help to increase the SKR.

The implementation of a high rate system like the one described in chapter 5 might be challenging in the beginning, especially if real-time processing is required (not counting post-processing). Operating at high rates requires the use of specific hardware like FPGAs or ASICs, which demand a considerable programming effort. As an intermediate step off-line processing will be useful for testing and for initial implementations.

The generation and acquisition system described in chapter 4 is a good example of those systems and it is not the only alternative. More hardware platforms could be used in the implementation and finding a good combination of hardware parameters (sampling rate, analogue bandwidth, resolution, number of channels...) is an interesting challenge in order to build a cost-effective system that could simplify the access to CV-QKD in the near term.

## 10.2 On-chip CV-QKD

Commercial receivers made of heterogeneous technologies like the current ICR or $\mu$ICR are good candidates for the detection part. It is even possible that the lasers could be integrated in the near future, but it is likely that the first integrated lasers will not provide the required performance for CV-QKD (especially in terms of linewidth).

In the current context, where the LO laser is external, silicon photonics is a particularly interesting technology for the detection due to its compatibility with CMOS technology. This would allow the direct integration with the amplification stage and potentially with the logical control to form a monolithic ASIC dedicated to CV-QKD and classical coherent communications, certainly a very attractive idea for the long term.

The shorter term improvements of the system described in this document are the transition to more standard packaging supports in order to accelerate the testing cycle, and also the test of new components like the 90° hybrid and the Alice on-chip. The amplification chain is also being adapted to operate with TIAs, that will allow the operation at higher rates and open the door to the previously described CW techniques. The 180° hybrid could potentially operate in heterodyne mode in this case.

## 10.3 Free-space CV-QKD

The feasibility study in the previous chapter shows that it is potentially possible to exchange secret keys at intercontinental distances using CV-

QKD, but some considerations were taken into account. The analysis has been done assuming that certain technical challenges can be solved with particular accuracy (mainly pointing and adaptive optics), but this does not mean that they are not challenging.

The life cycle of a satellite, from conception to retirement, is very long and costly, so all the considerations (technical and marketing) need to be very well considered beforehand. For this reason we are currently building a free-space CV-QKD system in the lab with the objective of testing particular features of satellite communications like fading, pointing and adaptive optics.

Another interesting topic that could be treated analytically would be the hypothetical construction of a network of satellites and ground stations, studying their estimated SKR as a function of their actual locations and real orbits. This type of study would be partially informative since in many occasions external elements like the weather conditions are the most relevant factors in the throughput of the link.

# Appendix

# Phase space representation A

A.1 Phase space representation 155
Canonical quantization . . 155
Extension to multiple modes156
Recapitulation . . . . . . . 158
A.2 Interesting states in phase space . . . . . . . . . . . . . . . 158
Quadrature eigenstates . . 158
Coherent states . . . . . . . 158

This appendix studies the possibility of extending the representation of quantum states to the phase space. The concepts of symplectic invariants, characteristic and Wigner functions are introduced. Quadrature and coherent states are described as interesting entities to be described using the phase space formalism. Only the basic aspects are covered, [64, 112] can be consulted for more information.

## A.1 Phase space representation

In classical Hamiltonian mechanics, the state of a particle can be defined by its position $x$ and momentum $p$. If we define two functions of $N$ particles[58] $f\left(x_i, p_i, t\right)$ and $g\left(x_i, p_i, t\right)$, the Poisson bracket operation $\{f, g\}$ can be calculated as

$$\{f, g\} = \sum_{i=1}^{N} \left[ \frac{\partial f}{\partial x_i} \frac{\partial g}{\partial p_i} - \frac{\partial f}{\partial p_i} \frac{\partial g}{\partial x_i} \right] \tag{A.1}$$

Classical mechanics allows only transformation that maintain the Poisson bracket invariant. Some interesting properties of $x_i$ and $p_i$ are the following relations:

$$\left\{x_i, x_j\right\} = 0, \quad \left\{x_i, p_j\right\} = \delta_{i,j}, \quad \left\{p_i, p_j\right\} = 0 \tag{A.2}$$

Variables $x_i$ and $y_i$ are called canonical variables and together with the Poisson bracket they characterize the canonical or symplectic structure of classical mechanics.

### A.1.1 Canonical quantization

The previous framework can be adapted to quantum mechanics changing the variables by operators $\hat{x}_i$ and $\hat{p}_i$, and the Poisson bracket by a commutator. If we set $\hbar = 1$ and $N_0 = \frac{1}{2}$ the relations between operators become:

$$\left[\hat{x}_i, \hat{x}_j\right] = 0, \quad \left[\hat{x}_i, \hat{p}_j\right] = i\delta_{i,j}, \quad \left[\hat{p}_i, \hat{p}_j\right] = 0 \tag{A.3}$$

Which lead to the famous Heisenberg uncertainty relation:

$$\Delta\hat{x}\Delta\hat{p} \geq \frac{1}{2}|\langle[\hat{x}, \hat{p}]\rangle| = \frac{1}{2} \tag{A.4}$$

[58] Note that $2N + 1$ independent variables are involved in those expressions: $N$ for $\{x_i\}_N$, $N$ for $\{p_i\}_N$ and one for the time $t$.

A Fock space $\mathcal{H}_i$ can describe a particular mode (space and time wave functions, energy and polarization). Its basis $\{|0\rangle, |1\rangle, \cdots, |i\rangle, \cdots\}$ represents each possible mode $i$, and in the continuous variables setting it is infinite. For photons, the notation $|n\rangle_i$ indicates the presence of $n$ indistinguishable photons in mode $i$ (the subindex $i$ will be omitted in the notation unless it can lead to ambiguity). Photons can leave or enter the mode using the creation $\hat{a}_i$ and annihilation $\hat{a}_i^\dagger$ operators:

$$\begin{aligned} \hat{a}_i|n\rangle_i &= \sqrt{n}|n-1\rangle_i \\ \hat{a}_i^\dagger|n\rangle_i &= \sqrt{n+1}|n+1\rangle_i \end{aligned} \tag{A.5}$$

Creation and annihilation operators are related to the canonical quadrature operators $\hat{x}$ and $\hat{p}$:

$$\hat{x} = \frac{1}{\sqrt{2}}\left(\hat{a} + \hat{a}^\dagger\right) \quad \text{and} \quad \hat{p} = -\frac{i}{\sqrt{2}}\left(\hat{a} - \hat{a}^\dagger\right) \tag{A.6}$$

And the commutation relations are transformed in the equivalent ones for $\hat{a}_i$ and $\hat{a}_i^\dagger$:

$$\left[\hat{a}_i, \hat{a}_j\right] = 0, \quad \left[\hat{a}_i, \hat{a}_j^\dagger\right] = \delta_{i,j}, \quad \left[\hat{a}_i^\dagger, \hat{a}_j^\dagger\right] = 0 \tag{A.7}$$

### A.1.2 Extension to multiple modes

When $N$ modes are involved, their state can be calculated as the tensor product of $N$ Fock spaces $\mathcal{H}_i$:

$$\mathcal{H} = \bigotimes_{k=1}^{N} \mathcal{H}_k \tag{A.8}$$

The basis of the resulting space is the result of tensoring the original basis, which for CV also results in an infinite number of dimensions. The generic shape is described by $|n_1, \cdots, n_N\rangle$ and in order to efficiently represent the states we can use several tools.

#### Density matrix

Density matrices are very usual in discrete variable analysis, and can also be used in CV, but their dimension will be infinite. If we denote $\mathbf{m} = (m_1, \cdots, m_N)$ and $\mathbf{n} = (n_1, \cdots, n_N)$, the density matrix $\rho$ is given by:

$$\rho = \sum_{\mathbf{m},\mathbf{n}=0}^{\infty} \rho_{\mathbf{m},\mathbf{n}} \left|m_1, \cdots, m_N\right\rangle \left\langle n_1, \cdots, n_N\right| \tag{A.9}$$

### Symplectic invariants

Although a valid formalism, density matrices might be not practical for CV, so generally we will work with the quadrature operators in the phase space representation. If we denote $\hat{r}_i = (\hat{x}_i, \hat{p}_i)$, the quadratures of a N-mode system can be grouped together as:

$$\hat{r} = (\hat{r}_1, \hat{r}_2 \cdots, \hat{r}_{2N})^T = (\hat{x}_1, \hat{p}_1, \hat{x}_2, \hat{p}_2, \cdots, \hat{x}_N, \hat{p}_N)^T \tag{A.10}$$

And the bosonic canonical commutation relations can be written as:

$$[\hat{r}_k, \hat{r}_l] = i\Omega_{kl} \tag{A.11}$$

Where Ω corresponds to the symplectic form

$$\Omega = \bigoplus_{i=1}^{N} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \tag{A.12}$$

If a simplectic form is invariant to the effect of a real-valued operator $S$, this operator $S$ is said to be a symplectic operator. We have transformed the tensor product structure into direct sums.

### Characteristic function

We can define the single-mode Weyl displacement operator according to phase space operators $\hat{r}$, $\xi$ being a 2N-dimensional vector:

$$\hat{D}(\xi) \equiv e^{-i\xi^T \Omega \hat{r}} \tag{A.13}$$

The displacement operator can be used to relate the density matrix in Hilbert space to a new representation called characteristic function:

$$\chi_\rho(\xi) = \mathrm{tr}[\rho \hat{D}(\xi)] \leftrightarrow \rho = \frac{1}{(2\pi)^N} \int \mathrm{d}^{2N}\xi \, \chi_\rho(-\xi)\hat{D}(\xi) \tag{A.14}$$

### Wigner function

The Fourier transform of the characteristic function is the Wigner function:

$$W_\rho(\xi) = \frac{1}{(2\pi)^N} \int \mathrm{d}^{2N}\zeta \, e^{i\xi^T \Omega \zeta} \chi_\rho(\zeta) \tag{A.15}$$

The Wigner function offers a quasi-probabilistic distribution in phase space and it is equivalent to the density distribution formalism.

### A.1.3 Recapitulation

The characteristics of CV make it interesting to have the option of representing the states in phase space, converting the infinite dimensional Hilbert space into a 2N-dimensional one (where N is the number of modes). Tensor products $\otimes$ are converted into direct sums $\oplus$, and the density matrix $\rho$ can be represented by the characteristic function $\chi_\rho$ or the Wigner function. A clear comparison is done by [112] in table A.1. We will see in appendix B that for Gaussian modes this formalism will be even more interesting, since covariance matrices (along with displacements) will be sufficient to characterize the states.

**Table A.1:** Comparison of Hilbert and phase space representations, as illustrated in [112].

| | **Hilbert space $\mathcal{H}$** | **Phase space $\Gamma$** |
|---|---|---|
| Dimensions | $\infty$ | $2N$ |
| Structure | $\otimes$ | $\oplus$ |
| Description | $\rho$ | $\chi_\rho$, $W_\rho$ |

## A.2 Interesting states in phase space

Phase space representation is especially well adapted to describe some particular states: quadrature and coherent states.

### A.2.1 Quadrature eigenstates

Quadrature eigenstates are defined as eigenstates of the position and momentum operators:

$$\begin{aligned} \hat{x}|x\rangle &= x|x\rangle \\ \hat{p}|p\rangle &= p|p\rangle \end{aligned} \tag{A.16}$$

They are related to the wave function $\psi(x)$ of the state $|\psi\rangle$ and its Fourier transform in momentum space $\psi(p)$:

$$\begin{aligned} \psi(x) &= \langle x|\psi\rangle \\ \psi(p) &= \langle p|\psi\rangle \end{aligned} \tag{A.17}$$

They are ideal mathematical entities useful for analysis, but not implementable physically, since the energy would diverge.

### A.2.2 Coherent states

Coherent states are more practical entities that approximate the states obtainable by a laser and can be physically implementable. A coherent state is defined as the eigenstate $|\alpha\rangle$ of the annihilation operator $\hat{a}$:

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle \qquad \alpha \in \mathbb{C} \tag{A.18}$$

This property will make them easily representable in phase space and will make the states non orthogonal due to the fact that $\hat{a}$ is a non Hermitian operator.

We would like to relate the coherent states $|\alpha\rangle$ to the number states $|n\rangle$. For this we define the Weyl displacement operator in terms of creation and annihilation operators over $\hat{D}(\alpha)$ as

$$\hat{D}(\alpha) = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}} \tag{A.19}$$

And applying certain transformation we arrive to the expression

$$|\alpha\rangle = e^{-|\alpha^2|/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle \tag{A.20}$$

The action of the displacement operator by a complex number $\alpha$ on the position and momentum operators is the following:

$$\begin{aligned}\hat{D}^\dagger(\alpha)\hat{x}\hat{D}(\alpha) &= \hat{x} + \sqrt{2}\,\mathrm{Re}(\alpha)\\ \hat{D}^\dagger(\alpha)\hat{p}\hat{D}(\alpha) &= \hat{p} + \sqrt{2}\,\mathrm{Im}(\alpha)\end{aligned} \tag{A.21}$$

According to this, a coherent state $|\alpha\rangle$ can be represented as a vacuum state $|0\rangle$ displaced by a quantity $d_x = \sqrt{2}\,\mathrm{Re}(\alpha)$ along the quadrature $\hat{x}$ and by $d_p = \sqrt{2}\,\mathrm{Im}(\alpha)$ along the quadrature $\hat{p}$. Graphically it can be interpreted as a point in the complex plane.

An interesting property of coherent states is that they saturate the uncertainty principle, so the uncertainty over their quadratures is minimal.

Other relevant property, especially for QKD is that they do not form an orthonormal basis, since

$$\langle\alpha|\beta\rangle = e^{-\left(|\alpha|^2+|\beta|^2\right)/2}\sum_{n=0}^{\infty}\frac{(\alpha^*\beta)^n}{n!} = e^{-\frac{1}{2}\left(|\alpha|^2+|\beta|^2-\alpha^*\beta\right)} \neq 0 \tag{A.22}$$

If we calculate the probability of the previous expression:

$$|\langle\alpha|\beta\rangle|^2 = e^{-|\alpha-\beta|^2} \tag{A.23}$$

It can be seen that for two close states (small $|\alpha-\beta|$) the uncertainty principle will be very relevant, while for more separated states (large $|\alpha-\beta|$) the uncertainty plays a much lesser role. The tendency in CV-QKD will be to work with distributions of states with very small separations, while in coherent classical communications the separations will tend to be larger in order to clearly distinguish the states at the reception.

Note that the phase space formalism is already common in classical coherent communications, where signals are denoted by the in-phase $I$ and quadrature $Q$ components, that are merely the real and imaginary part of a vector in phase space.

# Gaussian states B

This appendix covers the basic aspects of Gaussian states, identifying the most relevant for CV-QKD and providing the tools to operate with them and to obtain the expected entropy. A more extensive approach can be found in [64].

B.1 Properties of Gaussian states . . . . . . . . . . . . . . . . . 161
Symplectic spectrum and invariants . . . . . . . . . . . . . 162
B.2 Some useful Gaussian states165
One-mode Gaussian states 165
Two-mode Gaussian states 166
B.3 Gaussian operations . . . 166
Symplectic transformations 167
Completely positive maps 168
Partial measurements . . . 168
B.4 Entropy of continuous variables . . . . . . . . . . . . . . . 170
Entropy of Gaussian states 170
Extremality of Gaussian states . . . . . . . . . . . . . . . . . 171
B.5 Recapitulation . . . . . . . . 171

## B.1 Properties of Gaussian states

Gaussian states are those whose Wigner function (and hence the characteristic function) is Gaussian. Assuming a general state $\rho$ we can define the displacement vector $d \in \mathbb{R}^{2N}$ as:

$$d = \langle \hat{r} \rangle = \mathrm{tr}[\rho \hat{r}] \tag{B.1}$$

With the displacement vector $d$ and the phase space operator $\hat{r}$ we can use the anticommutator $\{\}$ to define the positive-semidefinite matrix $\gamma$ of size $2N \times 2N$ and coefficients

$$\gamma_{ij} = \mathrm{tr}\left[\rho \left\{\hat{r}_i - d_i, \hat{r}_j - d_j\right\}\right] \tag{B.2}$$

Defining $D = \Omega d$ and $\Gamma = \Omega\gamma\Omega$ the Wigner and the characteristic functions can be expressed as

$$W(r) = \frac{1}{\pi^{2N}\sqrt{\det\gamma}} e^{-(r-d)^T \gamma^{-1}(r-d)} \tag{B.3}$$

$$\chi_\rho(\xi) = \exp\left(-\frac{1}{4}\xi^T \Gamma \xi + i D^T \xi\right) \tag{B.4}$$

One important property of Gaussian states is that they are entirely described by their first two moments, despite of the infinite dimension of the underlying Hilbert space. It is also interesting that the states can be completely determined by the covariance matrix $\gamma$, but not any matrix is physically possible. There is a necessary and sufficient condition that $\gamma$ should satisfy [113]

$$\gamma + i\Omega \geq 0 \tag{B.5}$$

### B.1.1 Symplectic spectrum and invariants

Williamsom's theorem [114] states that for a covariance matrix $\gamma$ there exists a non unique symplectic transformation that generates the matrix $\nu$ that corresponds to the normal form of matrix $\gamma$, i.e. a diagonal matrix whose elements are the symplectic eigenvalues of the covariance matrix $\gamma$:

$$S^T \gamma S = \nu = \bigoplus_{k=1}^{N} \begin{bmatrix} \nu_k & 0 \\ 0 & \nu_k \end{bmatrix} \tag{B.6}$$

The set of $\nu_k$ defines the symplectic spectrum of the covariance matrix $\gamma$ and in order to validate the uncertainty principle they cannot be lower than one:

$$\nu_k \geq 1 \quad \text{for} \quad k = 1, \cdots, N \tag{B.7}$$

This is general for any covariance matrix, but Gaussian states are the only ones that can saturate the uncertainty.

The spectrum is the result of calculating the eigenvalues of the operator $|i\Omega\gamma|$, something which is not easy to to in practice. An alternative is to calculate the symplectic invariants, quantities that are invariant under the action of the symplectic group $\mathrm{Sp}(2N, \mathbb{R})$.

#### Normal decomposition using principal minors

Let us denote as $M_k(\alpha)$ the principal minor of order $k$ for the matrix $\alpha$. For an N-mode matrix, the k-th invariant $\Delta_k^N$ has the following relation to the principal minors:

$$\Delta_k^N \equiv M_{2k}(\Omega\gamma) \tag{B.8}$$

The relation of the invariants with the symplectic eigenvalues is the following, and can be used to relate to the principal minors:

$$\Delta_k^N = \sum_{\mathcal{S}_k^N} \prod_{j \in \mathcal{S}_k^N} \nu_j^2 = M_{2k}(\Omega\gamma) \tag{B.9}$$

The sum runs over all the possible k-subsets $\mathcal{S}_k^N$ of the first $N$ natural integers.

### One-mode normal decomposition

For one mode states the covariance matrix $\gamma_1$ has size $2 \times 2$ and we can use the symplectic invariant to determine $\nu_1$. Realising that the determinant of $\gamma_1$ is invariant to any symplectic operator $S$

$$\det\left(S\gamma S^T\right) = \det\gamma \tag{B.10}$$

We can use it to calculate the eigenvalue $\nu_1$:

$$\nu_1 = \sqrt{\det\gamma_1} \tag{B.11}$$

### Two-mode normal decomposition

The covariance matrix of a two-mode state has the form

$$\gamma_{12} = \begin{pmatrix} \gamma_1 & C_{12} \\ C_{12} & \gamma_2 \end{pmatrix} \tag{B.12}$$

where the submatrices are $2 \times 2$ real matrices. In this case we use the second symplectic invariant $\Delta$, which corresponds to the principal minor of order 2 of the complete matrix $\gamma$.

$$\Delta = \det\gamma_1 + \det\gamma_2 + 2\det C_{12} \tag{B.13}$$

and the symplectic eigenvalues $\nu_1$ and $\nu_2$ are the roots of $X^2 - \Delta X + \det\gamma_{12} = 0$:

$$\nu_{1,2}^2 = \frac{1}{2}[\Delta \pm \sqrt{\Delta^2 - 4\det\gamma_{12}}] \tag{B.14}$$

### Three-mode normal decomposition

For a matrix $\gamma_{AFG|b}$ that can be decomposed as

$$\gamma_{AFG|b} = \begin{bmatrix} \gamma_A & \sigma_{AF} & \sigma_{AG} \\ \sigma_{AF}^T & \gamma_F & \sigma_{FG} \\ \sigma_{AG}^T & \sigma_{FG}^T & \gamma_G \end{bmatrix} \tag{B.15}$$

the symplectic invariances of a three-mode state should satisfy

$$P(x) = x^3 - \Delta_1^3 x^2 + \Delta_2^3 x - \Delta_3^3 = 0 \tag{B.16}$$

$$P(1) = 0 \tag{B.17}$$

which can be simplified to

$$Q(x) = x^2 - \left(\Delta_1^3 - 1\right) x + \Delta_3^3 \tag{B.18}$$

where

$$\begin{aligned}\Delta_1^3 &= \det\gamma_A + \det\gamma_G + 2\det\sigma_{AF} + 2\det\sigma_{AG} + 2\det\sigma_{FG} = \alpha + 1\\ \Delta_3^3 &= \det\gamma_{AFG|b} = \beta\end{aligned}$$

and the symplectic eigenvalues can be calculated as

$$\begin{aligned}\nu_3^2 &= \tfrac{1}{2}(\alpha + \sqrt{\alpha^2 - 4\beta})\\ \nu_4^2 &= \tfrac{1}{2}(\alpha - \sqrt{\alpha^2 - 4\beta})\\ \nu_5^2 &= 1\end{aligned} \tag{B.19}$$

**Example from chapter 2** When the measurement is done only in one quadrature the sub-matrices of $\gamma_{AFG|b}$ correspond to

$$\gamma_A^{1P} = \begin{pmatrix} -\frac{\eta T Z^2}{\eta+\eta T(\xi+V_A)-\eta v+v} + V_A + 1 & 0 \\ 0 & V_A + 1 \end{pmatrix} \tag{B.20}$$

$$\gamma_F^{1P} = \begin{pmatrix} \frac{Tv(\xi+V_A)+v}{\eta+\eta T(\xi+V_A)-\eta v+v} & 0 \\ 0 & \eta v - (\eta-1)(T(\xi+V_A)+1) \end{pmatrix} \tag{B.21}$$

$$\gamma_G^{1P} = \begin{pmatrix} v - \frac{(1-\eta)\left(v^2-1\right)}{\eta+\eta T(\xi+V_A)-\eta v+v} & 0 \\ 0 & v \end{pmatrix} \tag{B.22}$$

$$\sigma_{AF}^{1P} = \begin{pmatrix} \frac{\sqrt{1-\eta}\sqrt{T}vZ}{\eta+\eta T(\xi+V_A)-\eta v+v} & 0 \\ 0 & \sqrt{1-\eta}\left(-\sqrt{T}\right)Z \end{pmatrix} \tag{B.23}$$

$$\sigma_{AG}^{1P} = \begin{pmatrix} \frac{\sqrt{-(\eta-1)\eta}\sqrt{T}\sqrt{v^2-1}Z}{\eta+\eta T(\xi+V_A)-\eta v+v} & 0 \\ 0 & 0 \end{pmatrix} \tag{B.24}$$

$$\sigma_{FG}^{1P} = \begin{pmatrix} -\frac{\sqrt{\eta}\sqrt{v^2-1}(T(\xi+\mathrm{VA})+1)}{(\eta-1)v-\eta(T(\xi+\mathrm{VA})+1)} & 0 \\ 0 & \sqrt{\eta}\left(-\sqrt{v^2-1}\right) \end{pmatrix} \tag{B.25}$$

and the value of $v = 1 + V_{\mathrm{el}}/(1-\eta)$. For two simultaneous quadratures $v = 1 + 2V_{\mathrm{el}}/(1-\eta)$ and the sub-matrices are

$$\gamma_A^{2P} = \begin{pmatrix} -\frac{\eta T Z^2}{\eta+\eta\xi T+\eta T V_A-\eta v+v+1} + V_A + 1 & 0 \\ 0 & -\frac{\eta T Z^2}{\eta+\eta\xi T+\eta T V_A-\eta v+v+1} + V_A + 1 \end{pmatrix} \tag{B.26}$$

$$\gamma_F^{2P} = \begin{pmatrix} \frac{v(\eta+T(\xi+V_A)+1)-(\eta-1)(T(\xi+V_A)+1)}{\eta+\eta\xi T+\eta T V_A-\eta v+v+1} & 0 \\ 0 & \frac{v(\eta+T(\xi+V_A)+1)-(\eta-1)(T(\xi+V_A)+1)}{\eta+\eta\xi T+\eta T V_A-\eta v+v+1} \end{pmatrix} \tag{B.27}$$

$$\gamma_G^{2P} = \begin{pmatrix} v - \frac{(1-\eta)\left(v^2-1\right)}{\eta+\eta\xi T+\eta T V_A-\eta v+v+1} & 0 \\ 0 & v - \frac{(1-\eta)\left(v^2-1\right)}{\eta+\eta\xi T+\eta T V_A-\eta v+v+1} \end{pmatrix} \tag{B.28}$$

$$\sigma_{AF}^{2P} = \begin{pmatrix} \frac{\sqrt{1-\eta}\sqrt{T}(v+1)Z}{\eta+\eta\xi T+\eta T V_A-\eta v+v+1} & 0 \\ 0 & -\frac{\sqrt{1-\eta}\sqrt{T}(v+1)Z}{\eta+\eta\xi T+\eta T V_A-\eta v+v+1} \end{pmatrix} \tag{B.29}$$

$$\sigma_{AG}^{2P} = \begin{pmatrix} \frac{\sqrt{-(\eta-1)\eta}\sqrt{T}\sqrt{v^2-1}Z}{\eta+\eta\xi T+\eta T V_A-\eta v+v+1} & 0 \\ 0 & \frac{\sqrt{-(\eta-1)\eta}\sqrt{T}\sqrt{v^2-1}Z}{\eta+\eta\xi T+\eta T V_A-\eta v+v+1} \end{pmatrix} \tag{B.30}$$

$$\sigma_{AF}^{2P} = \begin{pmatrix} -\frac{\sqrt{\eta}\sqrt{v^2-1}(T(\xi+V_A)+2)}{-\eta(T(\xi+V_A)+1)+(\eta-1)v-1} & 0 \\ 0 & \frac{\sqrt{\eta}\sqrt{v^2-1}(T(\xi+V_A)+2)}{-\eta(T(\xi+V_A)+1)+(\eta-1)v-1} \end{pmatrix} \tag{B.31}$$

## B.2 Some useful Gaussian states

### B.2.1 One-mode Gaussian states

One-mode Gaussian states are defined by a displacement vector $d = \left(d_x, d_p\right)$ and a covariance matrix $\gamma$. The most relevant for us will be coherent, squeezed and thermal states.

**Coherent states.** The covariance matrix is $\gamma = \mathbb{1}_2$ and a particular case is the vacuum state that corresponds to a displacement $d = (0, 0)$.

**Squeezed states.** The coherent states can be generalized in order to distribute the variance between the two quadratures (one of them becomes squeezed while the other becomes anti-squeezed). Denoting by $r$ the squeezing parameter the general form of a a one-mode Gaussian state is given by the matrix

$$\gamma = \begin{pmatrix} e^{-2r} & 0 \\ 0 & e^{2r} \end{pmatrix} \tag{B.32}$$

**Thermal states.** Their displacement vector is null $d = (0, 0)$ and the covariance matrix depends only on the mean photon number $\langle n \rangle$:

$$\gamma = \begin{pmatrix} 2\langle n \rangle + 1 & 0 \\ 0 & 2\langle n \rangle + 1 \end{pmatrix} \tag{B.33}$$

### B.2.2 Two-mode Gaussian states

Two-mode Gaussian states have a displacement vector with the form $d = \left(d_{x_1}, d_{p_1}, d_{x_2}, d_{p_2}\right)$ and a $4 \times 4$ matrix $\gamma_{12}$ of the form

$$\gamma_{12} = \begin{pmatrix} \gamma_1 & C_{12} \\ C_{12}^T & \gamma_2 \end{pmatrix} \tag{B.34}$$

The one-mode states can be obtained tracing out the other mode, e.g. if we trace out the second mode we obtain the displacement and the covariance matrix of the first mode. $C_{12}$ indicates the correlations between the two Gaussian modes, and in the particular case where it is zero, $\rho_{12} = \rho_1 \otimes \rho_2 = \mathrm{tr}_2\, \rho_{12} \otimes \mathrm{tr}_1\, \rho_{12}$.

**TMS.** Two-mode squeezed states are characterized by the following covariance matrix:

$$\gamma_{\mathrm{TMS}} = \begin{pmatrix} \cosh 2r \mathbb{1}_2 & \sinh 2r \sigma_z \\ \sinh 2r \sigma_z & \cosh 2r \mathbb{1}_2 \end{pmatrix} \tag{B.35}$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{B.36}$$

A TMS is a pure state, since $\det \gamma_{\mathrm{TMS}} = 1$ and tracing out the second mode we obtain a thermal state for the first one. This provides a way to purify thermal noise interpreting it as one half of a pure two-mode squeezed vacuum (TMSV). A TMSV is a particular case of TMS with $d = (0, 0, 0, 0)$ that can be expressed in the Fock basis as

$$|\mathrm{TMS}\rangle = \frac{1}{\cosh r} \sum_{n=0}^{\infty} \tanh^n r |n, n\rangle \tag{B.37}$$

## B.3 Gaussian operations

Gaussian operations are linear transformations on Gaussian states. They are very interesting because they comprise the operation that can be implemented using linear optics and the measurement operations.

### B.3.1 Symplectic transformations

Gaussian operations are entirely characterized by their actions on the displacement operator $d$ and the covariance matrix $\gamma$ and any unitary Gaussian operation has associated a symplectic operation $S \in \mathrm{Sp}(2N, \mathbb{R})$. The resulting displacement vector $d'$ and covariance matrix $\gamma'$ are

$$\begin{aligned} d' &= Sd \\ \gamma' &= S\gamma S^T \end{aligned} \tag{B.38}$$

The Gaussian operations that preserve the number of photons (passive) are described by the particular compact group $K(N) = \mathrm{Sp}(2N, \mathbb{R}) \cap O(2N)$. We will see some of the most interesting Gaussian transformations.

**Phase shift.** Maps a rotation of a single mode in phase space and corresponds to the symplectic transformation $S_{\mathrm{PS}}(\theta) \in \mathrm{Sp}(2, \mathbb{R})$.

$$S_{\mathrm{PS}}(T) = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \tag{B.39}$$

**Beam splitter.** Combines coherently two modes weighting by a factor $T$ and it is described by the symplectic transformation $S_{\mathrm{BS}}(T) \in \mathrm{Sp}(4, \mathbb{R})$.

$$S_{\mathrm{BS}}(T) = \begin{bmatrix} \sqrt{T}\cdot \mathbb{1}_2 & \sqrt{1-T}\cdot \mathbb{1}_2 \\ -\sqrt{1-T}\cdot \mathbb{1}_2 & \sqrt{T}\cdot \mathbb{1}_2 \end{bmatrix} \tag{B.40}$$

**Squeezing.** Squeezes one $S_{\mathrm{Sq}}(r) \in \mathrm{Sp}(2, \mathbb{R})$ or two $S_{\mathrm{Sq2}}(r) \in \mathrm{Sp}(4, \mathbb{R})$ modes by squeezing factor $r$.

$$S_{\mathrm{Sq}}(r) = \begin{bmatrix} e^{-r} & 0 \\ 0 & e^{r} \end{bmatrix} \tag{B.41}$$

$$S_{\mathrm{Sq2}}(r) = \begin{bmatrix} \cosh r \cdot \mathbb{1}_2 & \sinh r \cdot \sigma_z \\ \sinh r \cdot \sigma_z & \cosh r \cdot \mathbb{1}_2 \end{bmatrix} \tag{B.42}$$

**Euler decomposition.** States that any $S \in \mathrm{Sp}(2N, \mathbb{R})$ can be decomposed in: (1) a first passive transformation $L \in K(N)$, (2) a single-mode squeezing by $r \in \mathbb{R}$ over the $N$ modes, and (3) a second passive transformation $L \in K(N)$.

$$S = K \bigoplus_{k=1}^{N} \begin{bmatrix} e^{-r_k} & 0 \\ 0 & e^{r_k} \end{bmatrix} L \tag{B.43}$$

**Local operations.** Any two-mode covariance matrix of the type B.34 can be transformed by local Gaussian operations into a Gaussian state with covariance matrix in the standard form

$$\gamma'_{12} = \begin{bmatrix} a & 0 & c_+ & 0 \\ 0 & a & 0 & c_- \\ c_+ & 0 & b & 0 \\ 0 & c_- & 0 & b \end{bmatrix} \tag{B.44}$$

## B.3.2 Completely positive maps

Completely positive maps (CPM) are the most general transformations that can be applied to a state. Gaussian CPM are characterized by two $2N \times 2N$ matrices $X$ and $Y$ the transform the initial state as follows:

$$\begin{aligned} d_{\text{out}} &= X d_{\text{in}} \\ \gamma_{\text{out}} &= X \gamma_{\text{in}} X^T + Y \end{aligned} \tag{B.45}$$

Matrix $Y$ is symmetric and the positivity condition implies

$$Y + i\Omega - iX\Omega X^T \geq 0 \tag{B.46}$$

We can use the CPM to describe the most common channels:

**Lossy channel** A channel of transmission efficiency $T$ is characterized by $X = \sqrt{T} \cdot \mathbb{1}$ and $Y = (1 - T) \cdot \mathbb{1}$.

**Thermal noise channel** A channel of transmission efficiency $T$ and excess noise $\xi$ can be modelled by $X = \sqrt{T} \cdot \mathbb{1}$ and $Y = (1 - T + T\xi) \cdot \mathbb{1}$.

## B.3.3 Partial measurements

Partial measurements are a special type of completely positive maps that consist in measuring part of a multipartite states. We will study the case for bipartite states. Let us consider a bipartite Gaussian state $\rho_{AB}$ of $(N_A + N_B)$ modes with displacement vector $d = (d_A, d_B)$ and covariance matrix

$$\gamma = \begin{bmatrix} A & C \\ C^T & B \end{bmatrix} \tag{B.47}$$

Each part of the bipartite state $\rho_{AB}$ can be measured mainly according two procedures: (a) the detection can be done directly over one quadrature (projection) that corresponds to $\hat{x}$ or $\hat{p}$ (up to a global phase), or (b) a balanced beam splitter can be used to divide the mode into components separated by a phase of 90° and measure the two quadratures $(\hat{x}, \hat{p})$ (always up to a global phase)[60] . An important property is that the resulting Gaussian state does not depend on the result of the measurements, only on the type.

In practical optical implementations, the previous measurements are done with the help of a local oscillator (LO) signal that facilitates the recovery of the measurement under thermal noise conditions.

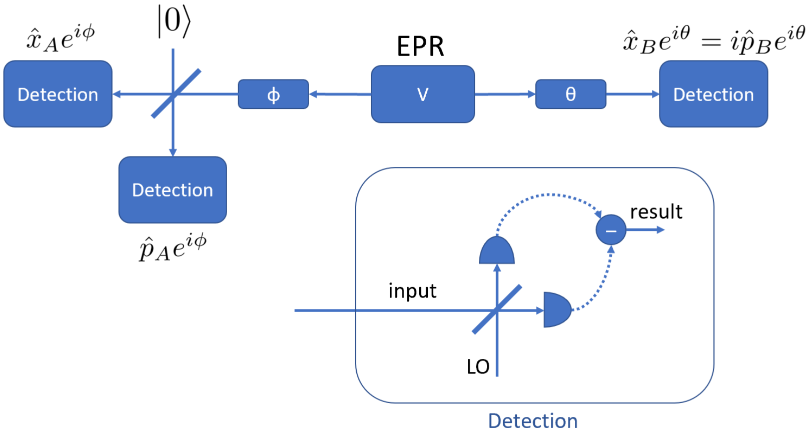


**Figure B.1:** Measurement of a bipartite state. On the left part of the figure a double quadrature (heterodyne) projection over the part $A$ of the state is presented. On the right we can see the single quadrature (homodyne) projection over the part $B$. A way to ensure the distribution of the LO is required in the scheme.

**One quadrature per measurement (homodyne).** The results of a direct projection on part $B$ of the state give the results $m = (x_1, 0, x_2, 0, \cdots, x_{N_B}, 0)$ and the state $\rho_A$ is projected to the Gaussian state $\rho'_A$ characterized by displacement vector $d'_A$ and covariance matrix $A'$:

$$d'_A = d_A + C(XBX)^{\mathrm{MP}}(m - d_B) \tag{B.48}$$

$$A' = A - C(XBX)^{\mathrm{MP}} C^T \tag{B.49}$$

Where $X = \mathrm{diag}(1, 0, 1, 0, \cdots, 1, 0)$ indicates with ones the quadratures that have been measured. This measurement can be observed on the right part of figure B.1. If the measurement would have been done over the part $B$ the resulting displacement vector and covariance matrix would have been

$$d'_B = d_B + C(XAX)^{\mathrm{MP}}(m - d_A) \tag{B.50}$$

$$B' = B - C(XAX)^{\mathrm{MP}} C^T \tag{B.51}$$

**Two quadratures per measurement (heterodyne).** As indicated before it is possible to measure both quadratures at the same time using a balanced beam splitter. The beam splitter introduces losses of 3 dB per quadrature, but the additional information can compensate the effect. The result of the measure is $m = (x_1, p_1, \cdots, x_{N_B}, p_{N_B})$ in this case and the Gaussian state $\rho'_A$ after a double quadrature measurement can be described by the following displacement vector and covariance matrix:

[60] Those methods are illustrated in figure B.1 and are typically called in the physics literature homodyne (a) and heterodyne (b) detection, but we will note use this nomenclature when possible to avoid confusion with the use of these terms in classical coherent communications.

$$d'_A = d_A + \sqrt{2}C\left(B + \mathbb{1}_{2N_B}\right)^{-1}(m - d_B) \tag{B.52}$$

$$A' = A - C\left(B + \mathbb{1}_{2N_B}\right)^{-1} C^T \tag{B.53}$$

Other technique uses the differential entropies (see [72]).

## B.4 Entropy of continuous variables

Generic CV states have the particularity of dealing with infinite components in the density matrix, like it was expressed in equation A.9. However, if the energy of the states is bounded, the sum becomes countable and the expression for the density matrix is

$$\rho = \sum_{\mathbf{m},\mathbf{n}=0}^{\infty} \rho_{\mathbf{m},\mathbf{n}} \left|m_1, \cdots, m_N\right\rangle \left\langle n_1, \cdots, n_N\right| \tag{B.54}$$

And the Von Neumann entropy will converge and can be calculated as

$$S(\rho) = -\operatorname{tr}\rho\log\rho \tag{B.55}$$

### B.4.1 Entropy of Gaussian states

The entropy of a Gaussian state can be determined by its covariance matrix $\gamma$. Due to Williamson theorem we know that there is a symplectic transformation $S$ that satisfies

$$S\gamma S^T = \bigoplus_{k=1}^{N} \begin{bmatrix} \nu_k & 0 \\ 0 & \nu_k \end{bmatrix} \tag{B.56}$$

where $\{\nu_k\}\ k = 1, \cdots, N$ are the symplectic eigenstates of $\gamma$. Also according to the same theorem there exists a unitary mapping between the Gaussian state and the product of $N$ thermal states with average photon number per mode $k$ equal to $\bar{n}_k = \frac{1}{2}(\nu_k - 1)$.

$$S(\rho_G) = \sum_{k=1}^{N} S(\rho_{\text{th}}(\bar{n}_k)) \tag{B.57}$$

Where $\rho_{\text{th}}$ is a single-mode thermal state with average photon number $\bar{n}$ and density matrix

$$\rho_{\text{th}} = \sum_{n=0}^{\infty} \frac{\bar{n}^n}{(\bar{n}+1)^{n+1}} |n\rangle\langle n| \tag{B.58}$$

where $\bar{n} = \mathrm{tr}(\rho n)$ is the average photon number in the state. Calculating the Von Neumann entropy gives

$$\begin{aligned} S(\rho_{\mathrm{th}}) &= -\,\mathrm{tr}\,\rho_{\mathrm{th}} \log_2 \rho_{\mathrm{th}} \\ &= -\frac{1}{\bar{n}+1} \sum_{k=0}^{\infty} \left(\frac{\bar{n}}{\bar{n}+1}\right)^k \log_2 \left[\frac{1}{\bar{n}+1} \left(\frac{\bar{n}}{\bar{n}+1}\right)^k\right] \\ &= -\frac{1}{\bar{n}+1} \sum_{k=0}^{\infty} \left(\frac{\bar{n}}{\bar{n}+1}\right)^k \left[-\log_2(\bar{n}+1) + k \log_2 \frac{\bar{n}}{\bar{n}+1}\right] \\ &= (\bar{n}+1)\log_2(\bar{n}+1) - \bar{n}\log_2 \bar{n} \end{aligned} \tag{B.59}$$

The following relation has been used in the last equality:

$$\sum_{k=0}^{\infty} k x^k = \frac{x}{(1-x)^2} \tag{B.60}$$

### B.4.2 Extremality of Gaussian states

It can be proven that Gaussian states are extremal for the Von Neumann entropy and various entanglement measures, which will be very interesting for some applications. The theorem reads [115]

**Theorem** Let $f : \mathcal{B}\left(\mathcal{H}^{\otimes N}\right) \to \mathbb{R}$ be a continuous functional, which is strongly sub-additive and invariant under local unitaries $f\left(U^{\otimes N} \rho U^{\dagger \otimes N}\right) = f(\rho)$. Then for every density operator $\rho$ describing an N-partite system with finite first and second moments, we have that

$$f(\rho) \leq f\left(\rho^G\right) \tag{B.61}$$

where $\rho^G$ is the Gaussian state with the same first and second moments as $\rho$.

## B.5 Recapitulation

The properties of table A.1 can be extended with table B.1.

| | **Hilbert space $\mathcal{H}$** | **Phase space $\Gamma$** |
|---|---|---|
| Criterion | $\rho \geq 0$ | $\gamma + i\Omega \geq 0$ |
| Operators | $U : \begin{cases} U^\dagger U = \mathbb{1} \\ \rho \mapsto U\rho U^\dagger \end{cases}$ | $S : \begin{cases} S^T \Omega S = \Omega \\ \gamma \mapsto S\gamma S^T \end{cases}$ |
| Spectra | $U\rho U^\dagger = \mathrm{diag}\{\lambda_k\}$<br>$0 \leq \lambda_k \leq 1$ | $S\gamma S^T = \mathrm{diag}\{\nu_k\}$<br>$1 \leq \nu_k \leq \infty$ |

**Table B.1:** Comparison of Hilbert and phase space representations for Gaussian states, as illustrated in [112].

# Mutual information C

C.1 Mutual information and Holevo bound . . . . . . . . . . 173
Channel capacity . . . . . . 174
Modulation and reconciliation efficiency . . . . . . . . . . . . 175
Mutual information between Alice and Bob . . . . . . . . . 176
Mutual information between Eve and Bob . . . . . . . . . . . 177
C.2 Holevo bound . . . . . . . 178
Holevo bound in CV-QKD 178

## C.1 Mutual information and Holevo bound

The mutual information (MI) [1] is a method to relate the amount of information obtained about one variable through the measurement of another. It is commonly used in information and probability theory, so without loss of generality we will define the mutual information between two random variables $X$ and $Y$ separated by a noisy channel with the following assumptions.

- $X$ is the random variable with alphabet $\mathcal{X}$ at the input of the noisy channel.
- $Y$ is the random variable with alphabet $\mathcal{Y}$ at the output of the noisy channel.
- The noisy channel can be modelled by the conditional probability distribution function of $Y$ given $X$: $p(y|x) = p_{Y|X}(y|x)$. The conditional probability of the channel can be linked to the joint probability of $X$ and $Y$ as $p_{X,Y}(x,y) = p_X(x)p_{Y|X}(y|x)$.

Before defining the mutual information, let us introduce the relative entropy or Kullback–Leibler divergence $D_{\mathrm{KL}}$. For a discrete distribution the relative entropy can be expressed as:

$$D_{\mathrm{KL}}(P\|Q) = -\sum_{x\in\mathcal{X}} P(x)\log\left(\frac{Q(x)}{P(x)}\right) = \sum_{x\in\mathcal{X}} P(x)\log\left(\frac{P(x)}{Q(x)}\right) \tag{C.1}$$

The mutual information can then be defined as the relative entropy between the joint distribution of $X$ and $Y$ and the product of the two marginals:

$$\mathrm{I}(X;Y) = D_{\mathrm{KL}}\left(P_{(X,Y)}\|P_X\otimes P_Y\right) \tag{C.2}$$

For discrete distributions it can be expressed as:

$$\begin{aligned}\mathrm{I}(X;Y) &= \sum_{y\in\mathcal{Y}}\sum_{x\in\mathcal{X}} p_{X,Y}(x,y)\log\left(\frac{p_{(X,Y)}(x,y)}{p_X(x)p_Y(y)}\right) && \text{(C.3)}\\ &= \sum_{y\in\mathcal{Y}}\sum_{x\in\mathcal{X}} p_X(x)p_{Y|X}(y|x)\log\left(\frac{\cancel{p_X(x)}p_{Y|X}(y|x)}{\cancel{p_X(x)}p_Y(y)}\right) && \text{(C.4)}\end{aligned}$$

And for continuous distributions as:

$$\begin{aligned} \mathrm{I}(X;Y) &= \int_{\mathcal{Y}}\int_{\mathcal{X}} p_{X,Y}(x,y)\log\left(\frac{p_{(X,Y)}(x,y)}{p_X(x)p_Y(y)}\right)dxdy && \text{(C.5)} \\ &= \int_{\mathcal{Y}}\int_{\mathcal{X}} p_X(x)p_{Y|X}(y|x)\log\left(\frac{\cancel{p_X(x)}p_{Y|X}(y|x)}{\cancel{p_X(x)}p_Y(y)}\right)dxdy && \text{(C.6)} \end{aligned}$$

### Mutual information properties

Some important properties are:

**Non negativity** $\mathrm{I}(X;Y) \geq 0$

**Symmetry** $\mathrm{I}(X;Y) = \mathrm{I}(Y;X)$

**Relation to entropy**

$$\begin{aligned} \mathrm{I}(X;Y) &\equiv \mathrm{H}(X) - \mathrm{H}(X|Y) \\ &\equiv \mathrm{H}(Y) - \mathrm{H}(Y|X) \\ &\equiv \mathrm{H}(X) + \mathrm{H}(Y) - \mathrm{H}(X,Y) \\ &\equiv \mathrm{H}(X,Y) - \mathrm{H}(X|Y) - \mathrm{H}(Y|X) \end{aligned} \tag{C.7}$$

## C.1.1 Channel capacity

As the joint distribution $p_{X,Y}(x,y)$ is completely determined by the choice of the marginal distribution $p_X(x)$ ($p_{X,Y}(x,y) = p_X(x)p_{Y|X}(y|x)$), under some conditions it is possible to find the distribution $p_X(x)$ that maximizes the mutual information (the supremum):

$$C = \sup_{p_X(x)} I(X;Y) \tag{C.8}$$

The resulting value of mutual information is known as the capacity of the channel and it depends only on its properties.

### AWGN channel capacity

An interesting case of channel capacity corresponds to the additive white Gaussian noise (AWGN) channel. In this case, the channel response is modelled as a random variable $Y$ relating two random variables: the input variable $X$ that is multiplied by a constant attenuation parameter $t$ and a random variable $N$ that is added to the previous one. A sample $i$ would be represented as:

$$y_i = tx_i + n_i \tag{C.9}$$

In order to calculate the capacity we will make two assumptions:

- The signal power at the transmitter Var($X$) is bounded, which is reasonable since the energy at the transmitter is a valuable resource.
- The noise power $n$ is bounded and its distribution is known. For the white case we will assume that its spectrum is flat in frequency, but it could be generalized to coloured spectra.

With these two limitations it is possible to calculate the signal-to-noise ratio (SNR) in natural units $s$ as:

$$s = \frac{t^2 \mathrm{Var}(X)}{\mathrm{Var}(N)} \tag{C.10}$$

And the capacity density per dimension $d$ used in the modulation can be expressed as:

$$C^d_{AWGN}(s) = \frac{d}{2} \log(1+s) \tag{C.11}$$

It is typical to express the logarithm in base two to obtain the capacity in bits per channel use or bits per symbol:

$$C^d_{AWGN}(s) = \frac{d}{2} \log_2(1+s) \qquad \text{[bits/sym]} \tag{C.12}$$

The capacity density can be multiplied by the symbol rate $R$ to obtain the capacity in bits per unit of time.

$$C^d_{AWGN}(s) = R\frac{d}{2} \log_2(1+s) \qquad \text{[bits/u.t.]} \tag{C.13}$$

### C.1.2 Modulation and reconciliation efficiency

It is not always possible to work in the conditions that satisfy the that the mutual information is equal to the capacity of the channel. The main impairments are the following:

- By definition, the capacity is calculated assuming that the two communication entities use error correcting codes of perfect efficiency (redundancy tends to zero). This is only possible using code words of infinite length, something that is not possible in practice. For words of finite length, the coding efficiency will be lower that 100% and it will in general depend on the SNR in natural units $s$: $\beta^{\mathrm{code}}(s) < 1$.
- The optimal distribution $p_X(x)$ might be continuous and/or unbounded (like in the AWGN channel), something that is not realizable in practice with digital processing (we are limited by the resolution and the power). The impairment introduced by a discrete modulation is more relevant as the SNR increases, so we can introduce the efficiency parameter $\beta^{\mathrm{mod}}(s) < 1$ to take into account the effects of an imperfect modulation.

In order to simplify the calculation of the actual mutual information, the two previous parameters can be combined into a parameter $\beta(s)$. Assuming that the SNR is sufficiently high to be able to use an efficient error correcting code and sufficiently low so that the mutual information is close to the capacity, the dependence with the SNR can be omitted and use only $\beta$, always lower than one. This parameter is known as reconciliation efficiency and indicates how far is the actual mutual information from the capacity of the channel.

Note that in classical communications the mutual information is used in the forward sense (encoded by Alice and decoded by Bob). The same is true for CV-QKD with direct reconciliation (DR), but with this method CV-QKD is limited to communication losses of less than 3 dB. For this reason it is more common to use reverse reconciliation (RR), where the information (after some processing) is encoded by Bob, sent to Alice through a classical channel, and decoded by Alice.

Knowing $\beta(s)$ the mutual information can be expressed as a fraction of the capacity of the channel and the dimensions $d$:

$$I^d_{X;Y}(s) = \beta(s) C^d(s) \tag{C.14}$$

This is practical for the calculation of expected secret key rates over a known channel, since its capacity would be known and the reconciliation efficiency can be adapted (designing the right error correcting codes and using the right modulation depth depending on the SNR). It also allows to have an estimate of the final secret key rate just after the parameter estimation phase, without the need of error correction.

In a complete system, an estimation of the mutual information can be obtained calculating the relative entropy of the same fragment of the coded and decoded messages. Note that there is a trade off in this operation, since an accurate estimation of the mutual information requires a large number of samples and the fact of revealing them prevents their use in the final secret key. For this reason it is generally preferred to use the previous approach.

### C.1.3 Mutual information between Alice and Bob

The mutual information will depend on the number of dimensions used to encode the information. In coherent communications the dimension will be one if we measure only one projection and two if we measure both at the same time.

**One projection (homodyne)**

$$I^{\mathrm{1P}}_{\mathrm{AB}} = \beta(s)\frac{1}{2}\log_2(1+s) = \beta(s)\frac{1}{2}\log_2\left(1+\frac{\eta T V_A}{1+V_{el}+\eta T\xi}\right) \tag{C.15}$$

**Two projections (heterodyne)**

$$I_{\mathrm{AB}}^{\mathrm{2P}} = \beta(s)\frac{2}{2}\log_2(1+s) = \beta(s)\log_2\left(1 + \frac{\eta T V_A}{2 + 2V_{el} + \eta T \xi}\right) \tag{C.16}$$

### C.1.4 Mutual information between Eve and Bob

In some cases it is interesting to calculate the bound on the information that Eve can infer from the information measured by Bob. This is useful for the security proofs against individual attacks that are not covered in this document.

**One projection (homodyne)** The proofs can be found in [116, 117] and the results are

$$I_{\mathrm{BE}}^{\mathrm{1P}} = \frac{1}{2}\log_2\frac{V_{\mathrm{B}}}{V_{\mathrm{B|E}}} = \frac{T^2\left(V + \chi_{\mathrm{tot}}^{\mathrm{1P}}\right)\left(1/V + \chi_{\mathrm{line}}\right)}{1 + T\chi_{\mathrm{det}}^{\mathrm{1P}}\left(1/V + \chi_{\mathrm{line}}\right)}, \text{where} \tag{C.17}$$

$$\chi_{\mathrm{line}} = \frac{1}{T} - 1 + \xi \tag{C.18}$$

$$\chi_{\mathrm{det}}^{\mathrm{1P}} = \frac{1 + V_{\mathrm{el}}}{\eta} - 1 \tag{C.19}$$

$$\chi_{\mathrm{tot}}^{\mathrm{1P}} = \chi_{\mathrm{line}} + \chi_{\mathrm{det}}^{\mathrm{1P}}/T \tag{C.20}$$

**Two projections (heterodyne)** Following [118, 119], let us define

$$\chi_{\mathrm{det}}^{\mathrm{2P}} = \frac{2 + 2V_{\mathrm{el}}}{\eta} - 1 \tag{C.21}$$

$$\chi_{\mathrm{tot}}^{\mathrm{2P}} = \chi_{\mathrm{line}} + \chi_{\mathrm{det}}^{\mathrm{2P}}/T \tag{C.22}$$

$$x_{\mathrm{E}} = T(2-\xi)^2/(\sqrt{2 - 2T + T\xi} + \sqrt{\xi})^2 + 1 \tag{C.23}$$

If Eve has access to Bob's detector noise the bound on $V_{\mathrm{B|E}}$ is

$$V_{\mathrm{B|E}} = \left(\frac{V x_{\mathrm{E}} + 1}{V + x_{\mathrm{E}}} + 1\right)/2 \tag{C.24}$$

or a more realistic bound, assuming the detection is not accessible to Eve:

$$V_{\mathrm{B|E}} = \eta\left(\frac{V x_{\mathrm{E}} + 1}{V + x_{\mathrm{E}}} + \chi_{\mathrm{det}}^{\mathrm{2P}}\right)/2 \tag{C.25}$$

$$I_{\mathrm{BE}}^{\mathrm{2P}} = \log_2\frac{V_{\mathrm{B}}}{V_{\mathrm{B|E}}} = \log_2\frac{T\left(V + \chi_{\mathrm{tot}}^{\mathrm{2BD}}\right)\left(V + x_{\mathrm{E}}\right)}{V x_{\mathrm{E}} + 1 + \chi_{\mathrm{det}}^{\mathrm{2BD}}\left(V + x_{\mathrm{E}}\right)} \tag{C.26}$$

## C.2 Holevo bound

The Holevo bound upper bounds the information that can be contained in a quantum system assuming a particular ensemble. A famous consequence is that a qubit cannot contain more than one bit of information.

For a state given by $\rho = \sum_i p_i \rho_i$, the outcome of any measurement defined by POVM elements is upper bounded by the quantity

$$\chi := S(\rho) - \sum_i p_i S(\rho_i) \tag{C.27}$$

where $S(\cdot)$ is the Von Neumann entropy.

### C.2.1 Holevo bound in CV-QKD

The Holevo bound [120] is typically used in CV-QKD to obtain an upper bound $S(b:E)$ on the information that Eve can obtain from the communication between Alice and Bob. For example, for the realistic case studied in section 2, $S(b:E)$ for one projection measurement can be expressed as

$$S(b:E) \leqslant S(\rho_E) - \int \Pr(m_B)\, S\left(\rho_E^{x_B}\right) \mathrm{d}x_B \tag{C.28}$$

We can simplify the previous expression using the following facts:

- $\rho_{AB_1E}$ is a pure state, then $S(\rho_E) = S\left(\rho_{AB_1}\right)$.
- The state after projective measurement over $X_B$ at Bob's is pure and $S\left(\rho_E^{m_B}\right) = S\left(\rho_{AFG}^{m_B}\right)$.
- Due to the extremality of Gaussian states [115] it is possible to use the Holevo bound of a thermal state.
- The state $\rho_{ABFG}$ is Gaussian (a mix of Gaussian states), and the measure over $X_B$ does not depend on the measure $x_B$, so $S\left(\rho_{AFG}^{m_B}\right)$ is not dependent of $m_B$ and can come out of the integral.

Equation C.28 can then be written as:

$$S(b:E) \leqslant S\left(\rho_{\mathrm{AB_1}}\right) - S\left(\rho_{\mathrm{AFG}}^{m_{\mathrm{B}}}\right) \tag{C.29}$$

The Holevo bound can be calculated from the symplectic eigenvalues of the involved correlation matrices: $\{\nu_1, \nu_2\}$ from $\gamma_{\mathrm{AB_1}}$ and $\{\nu_3, \nu_4, \nu_5\}$ from $\gamma_{\mathrm{AFG|b}}$. The upper limit is then:

$$S(b:E) = \sum_{i=1}^{2} G\left(\frac{\nu_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\nu_i - 1}{2}\right) \tag{C.30}$$

Where $G(x)$ is the Von Neumann entropy:

$$G(x) = (x + 1)\log_2(x + 1) - x\log_2 x \tag{C.31}$$

# Probability Distribution of Transmittance (PDT)

# D

D.1 Probability Distribution of Transmission Efficiency (PDTE) . . . . . . . . . . . . . . . . 181
D.2 Probability Distribution of Transmission Coefficient (PDTC) . . . . . . . . . . . . . . 182
D.3 Sources of uncertainty . . 183
Beam wandering . . . . . . 183
Atmospheric turbulence . 183
Other sources . . . . . . . . 183

This appendix is a compendium of the basic elements required to understand the turbulence considerations treated on the manuscript. For additional details we invite you to consult [107, 110].

## D.1 Probability Distribution of Transmission Efficiency (PDTE)

Assume a detector of opening area $\mathcal{A}$, the integration of the light intensity $I(\boldsymbol{r}, L_r)$ as a function of position $\boldsymbol{r}$ and distance $L_r$ results in the transmission efficiency $T = \tau^2$:

$$\tau = \int_{\mathcal{A}} \mathrm{d}^2\boldsymbol{r} I(\boldsymbol{r}, L_r) \tag{D.1}$$

In the case of low intensities, a quantum treatment can be followed, associating $T$ to the transmission efficiency of a beam splitter the simulates the channel. $\hat{a}_{\text{in}}$ denotes the input field annihilation operator and $\hat{c}$ is the environmental mode operator. The output field field annihilator operator can be denoted as

$$\hat{a}_{\text{out}} = \sqrt{T}\hat{a}_{\text{in}} + \sqrt{1-T}\hat{c} \tag{D.2}$$

In this model $T$ follows a generic random distribution with values $T \in [0, 1]$. Assuming that we know the distribution $\mathcal{P}(T)$ and the quasi-probability distribution[63] $P_{\text{in}}$, we can obtain the quasi-probability distribution at the output of the channel as

$$P_{\text{out}}(\alpha) = \int_0^1 \mathrm{d}T\mathcal{P}(T)\frac{1}{T}P_{\text{in}}\left(\frac{\alpha}{\sqrt{T}}\right) \tag{D.3}$$

The propagation can then be reduced to the identification of the probability distribution of transmission efficiency $\mathcal{P}(T)$, also abbreviated as PDTE.

$$\mathcal{P}(T) = \int_{\mathbb{R}^2} \mathrm{d}^2\boldsymbol{r}_0 P(T|\boldsymbol{r}_0)\,\rho(\boldsymbol{r}_0) \tag{D.4}$$

[63] In the sense of the Glauber–Sudarshan P representation, where $P(\alpha)$ generate a diagonal density matrix $\hat{\rho}$ in the basis of coherent states $\{|\alpha\rangle\}$: $\hat{\rho} = \int P(\alpha)|\alpha\rangle\langle\alpha|d^2\alpha$, where $d^2\alpha \equiv d\,\mathrm{Re}(\alpha)d\,\mathrm{Im}(\alpha)$.

## D.2 Probability Distribution of Transmission Coefficient (PDTC)

In many practical cases it is useful to use the probability distribution of the transmission coefficient or PDTC, which holds the same relation as D.4, but for the transmission coefficient $\tau = \sqrt{T}$:

$$\mathcal{P}(\tau) = \int_{\mathbb{R}^2} \mathrm{d}^2\boldsymbol{r}_0 P\left(\tau|\boldsymbol{r}_0\right)\rho\left(\boldsymbol{r}_0\right) \tag{D.5}$$

The most commonly assumed distribution for $\rho\left(\boldsymbol{r}_0\right)$ is the Rice distribution

$$\rho(r,d,\sigma) = \frac{r}{\sigma^2}\mathrm{I}_0\left(\frac{r\,d}{\sigma^2}\right)\exp\left[-\frac{r^2+d^2}{2\sigma^2}\right] \tag{D.6}$$

where $d = |\boldsymbol{d}|$ is the offset between the center of the aperture and the center of the fluctuation, $r = |\boldsymbol{r}|$ is the deflection from the center of the distribution and $I_0$ is the modified Bessel function. If the transmission coefficient can be approximated by

$$T(r) = T_0\exp\left[-\left(\frac{r}{R}\right)^{\lambda}\right] \tag{D.7}$$

then the PDTC is given by the log-negative generalized Rice distribution,

$$\begin{aligned}\mathcal{P}(\tau) = \frac{2R^2}{\sigma^2\lambda\tau}\left(2\ln\frac{\tau_0}{\tau}\right)^{\frac{2}{\lambda}-1}\mathrm{I}_0\left(\frac{Rd}{\sigma^2}\left[2\ln\frac{\tau_0}{\tau}\right]^{\frac{1}{2}}\right)\\ \times\exp\left[-\frac{1}{2\sigma^2}\left\{R^2\left(2\ln\frac{\tau_0}{\tau}\right)^{\frac{2}{\lambda}}+d^2\right\}\right]\end{aligned} \tag{D.8}$$

It can be simplified to a Weibull distribution when the beam fluctuates around the aperture center. The expression is then simplified between the interval $\tau \in [0,1]$ (the rest is 0) as

$$\mathcal{P}(\tau) = \frac{2R^2}{\sigma^2\lambda\tau}\left(2\ln\frac{\tau_0}{\tau}\right)^{\frac{2}{\lambda}-1}\exp\left[-\frac{1}{2\sigma^2}R^2\left(2\ln\frac{\tau_0}{\tau}\right)^{\frac{2}{\lambda}}\right] \tag{D.9}$$

With

$$\tau_0^2 = 1-\exp\left[-2\frac{a^2}{W^2}\right] \tag{D.10}$$

$$\begin{aligned}\lambda =& 8\frac{a^2}{W^2}\frac{\exp\left[-4\frac{a^2}{W^2}\right]\mathrm{I}_1\left(4\frac{a^2}{W^2}\right)}{1-\exp\left[-4\frac{a^2}{W^2}\right]\mathrm{I}_0\left(4\frac{a^2}{W^2}\right)}\\ &\times\left[\ln\left(\frac{2\tau_0^2}{1-\exp\left[-4\frac{a^2}{W^2}\right]\mathrm{I}_0\left(4\frac{a^2}{W^2}\right)}\right)\right]^{-1}\end{aligned} \tag{D.11}$$

$$R = a \left[ \ln \left( \frac{2\tau_0^2}{1 - \exp\left[-4\frac{a^2}{W^2}\right] I_0\left(4\frac{a^2}{W^2}\right)} \right) \right]^{-\frac{1}{\lambda}} \tag{D.12}$$

Where $a$ is the radius of the receiving telescope, $W$ is the beam spot radius at the receiver point, $I_0$ and $I_1$ are the modified Bessel functions of order 0 and 1 respectively.

The parameter $\sigma^2$ denotes the uncertainty in the distribution of $r$ and can provide from several sources.

## D.3 Sources of uncertainty

Several sources can contribute to the uncertainty of the deflection $r$ and they can be independent in nature, so they should be added up. For our study the most relevant will be beam wandering, and in most cases the global variance can be approximated by the variance of the beam wandering.

### D.3.1 Beam wandering

We denote beam wandering the fluctuations of the beam around the expected target. If the source has an uncertainty angle denoted by $\theta_p$, then the variance after a distance $z$ can be well approximated as

$$\sigma_{BW}^2 = \theta_p^2 \cdot z^2 \tag{D.13}$$

### D.3.2 Atmospheric turbulence

When the atmospheric turbulence is weak, its value after a propagation distance $z$ over a medium of index-of-refraction structure constant $C_n^2$ is given by the expression[121]

$$\sigma_{\text{atm}}^2 \approx 1.919\, C_n^2\, z^3\, (2W_0)^{-1/3} \tag{D.14}$$

$W_0$ is the beam width when entering the atmospheric medium. Typical values for $C_n^2$ are in the order of $10^{-14}$ m$^{-2/3}$.

### D.3.3 Other sources

The effects described above can occur naturally in a free space system, but other sources of technical origin can also appear. One example could be the effect of limitations in the adaptive optics mechanisms.

# Doppler effect in satellites | E

E.1 Introduction . . . . . . . . . 185
Frequency mixing . . . . . 185
E.2 Doppler effect . . . . . . . 186
Fast evaluation of order of magnitude . . . . . . . . . . . . . . 186
Doppler shift cancellation . 187

## E.1 Introduction

In systems that rely on coherent detection (mixing of received signal with a local oscillator, LO) it is important to keep track of the possible detuning along the system. Ideally, if no frequency drifts were present, the signal and the LO would interfere and the result would be centred at 0 Hz. The other components of the mix usually lay out of the frequencies managed by the electronics so they can be discarded.

In real scenarios the frequency drift will be usually non-zero, and the center of the resulting signal will be shifted from 0 Hz by certain amount $\Delta f_{\text{mix}}$. The components affecting the mismatch are the following:

- $f_{\text{A}}$: Nominal frequency of Alice's laser.
- $f_{\text{B}}$: Nominal frequency of Bob's laser.
- $\Delta f_{\text{A}}(t)$: Frequency drift in Alice's laser.
- $\Delta f_{\text{B}}(t)$: Frequency drift in Bob's laser.
- $\Delta f_{\text{atm}}(t)$: Atmospheric frequency drift effects.
- $\Delta f_{\text{Doppler}}(t)$: Doppler frequency drift due to the variation in apparent velocity during the satellite trajectory.

The reference points are the following:

- $f_{\text{B-in}}(t)$: Frequency at Bob's input.
- $f_{\text{B-LO}}(t)$: Frequency of Bob's effective LO.

$$f_{\text{B-LO}}(t) = f_{\text{B}} + \Delta f_{\text{B}}(t) \tag{E.1}$$

$$f_{\text{B-in}}(t) = f_{\text{A}} + \Delta f_{\text{A}}(t) + \Delta f_{\text{atm}}(t) + \Delta f_{\text{Doppler}}(t) \tag{E.2}$$

### E.1.1 Frequency mixing

With the previous notation, the result of the optical mixing is the following:

$$\begin{aligned} |f_{\text{mix}}(t)| &= |f_{\text{B-LO}}(t) - f_{\text{B-in}}(t)| & \text{(E.3)} \\ &= |f_{\text{B}} - f_{\text{A}} + \Delta f_{\text{B}}(t) - \Delta f_{\text{A}}(t) - \Delta f_{\text{atm}}(t) - \Delta f_{\text{Doppler}}(t)| & \text{(E.4)} \end{aligned}$$

## E.2 Doppler effect

The apparent velocity of the satellite over the sky will change depending on the described arc during the time of sight. High elevation angles (i.e. satellite flying over the ground station) permit a longer time of sight, but the variation of the relative velocity would also be higher, being maximum when the trajectory of the satellite passes through the zenith of the ground station ($\theta = 90^{o}$). On the other hand, low elevation measures do not suffer from high velocity variation, but the time of sight is shorter.

In order to take all the parameters into account, we have to consider the spherical geometry of the orbits. We will assume that the satellite orbits are circular and the angular velocity is constant. Under this conditions, a previous analysis has been done in [122]. The final expression is quite complex, but figure E.1 summarizes the relative Doppler shift for different elevations.

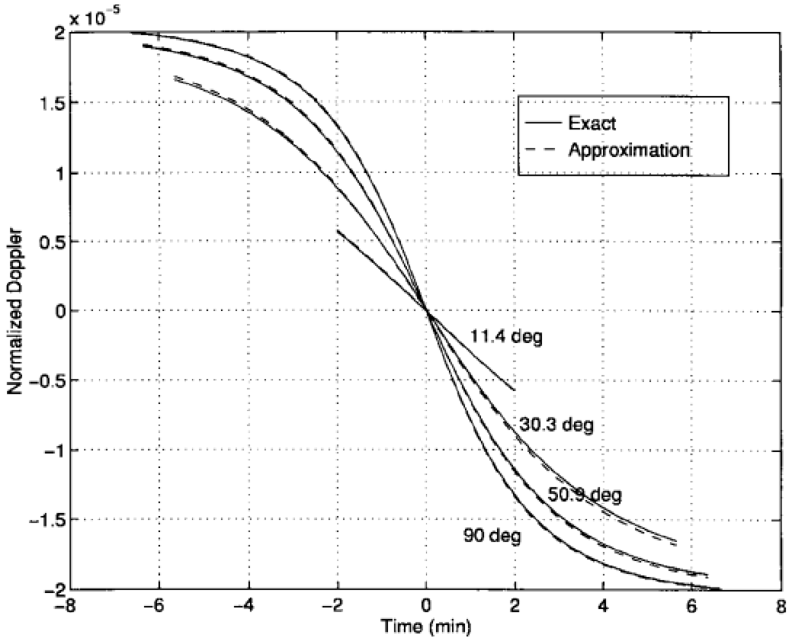


**Figure E.1:** Normalized Doppler shift depending on the elevation [122].

The evaluation of the worst case ($\theta$=90$^{o}$, $2 \times 10^{-5}$ relative Doppler shift) assuming that we are using a wavelength of 1550 nm gives a Doppler shift of 3.9 GHz[65] . Even milder cases as $\theta$=11$^{o}$ give shifts in the order of 1 GHz.

### E.2.1 Fast evaluation of order of magnitude

A faster way to get the order of magnitude of Doppler shift is using the Doppler equation E.5 and the velocity of the satellite as velocity shift (although it is an overestimation).

$$\Delta f_{\text{Doppler}} = \frac{\Delta v}{c} f_0 = \frac{\Delta v}{\lambda_0} \tag{E.5}$$

[65] Using longer wavelengths decreases the effect of Doppler drift. For example, using green light instead of telecom wavelengths will increase the Doppler shift by a factor of three.

Using light at 1550 nm, this gives for LEO satellites traveling at 8000 m/s results in the order of 5 GHz.

### E.2.2 Doppler shift cancellation

Considering that the relative position of the satellite and the ground station cannot be hijacked, Bob can calculate the Doppler frequency shift that is expected at each moment, so he can apply some strategies to cancel it. Some possibilities are:

- Modify Bob's LO frequency. This will require a tunable laser in the range of ± 4 GHz at low rates (the expected Doppler changes are relatively slow in time).
- Use a high bandwidth detector (>8 GHz) and correct the shift digitally. This will likely increase the level of electronic noise and increase the complexity, especially in the case of trusted noise, since it will not be constant at all frequencies.

In any case, considering that the estimation of the Doppler effect is not perfect, there will be some remnant drift $\Delta f_{\text{Doppler-rem}}$ apart from the atmospheric drift. The total frequency detuning will be:

$$|f_{\text{mix}}(t)| = |\Delta f_B(t) - \Delta f_A(t) - \Delta f_{\text{Doppler-rem}}(t) - \Delta f_{\text{atm}}(t)| \tag{E.6}$$

It is probable that the numeric values would be in the order of tens to hundreds of MHz, depending on the efficiency of the Doppler drift correction and the frequency stability o the lasers. It is important that the detector has sufficient bandwidth to deal with this drift, added to the actual bandwidth of the signal.

# Bibliography

Here are the references in citation order.

[1] C. E. Shannon. 'A mathematical theory of communication'. In: *The Bell System Technical Journal* 27.3 (July 1948), pp. 379–423. DOI: 10.1002/j.1538-7305.1948.tb01338.x (cited on pages 3, 39, 173).

[2] Auguste Kerckhoffs. 'La cryptographie militaire'. In: *Journal des sciences militaires* IX (Jan. 1883), pp. 5–38 (cited on page 4).

[3] Federal Information Processing Standards. *Announcing the ADVANCED ENCRYPTION STANDARD (AES)*. 2001 (cited on page 5).

[4] Steven M. Bellovin. 'Frank Miller: Inventor of the One-Time Pad'. In: *Cryptologia* 35.3 (2011), pp. 203–222. DOI: 10.1080/01611194.2011.583711 (cited on page 5).

[5] C. E. Shannon. 'Communication theory of secrecy systems'. In: *The Bell System Technical Journal* 28.4 (Oct. 1949), pp. 656–715. DOI: 10.1002/j.1538-7305.1949.tb00928.x (cited on page 5).

[6] Ralph C. Merkle. 'Secure Communications over Insecure Channels'. In: *Commun. ACM* 21.4 (Apr. 1978), pp. 294–299. DOI: 10.1145/359460.359473 (cited on page 6).

[7] W. Diffie and M. Hellman. 'New directions in cryptography'. In: *IEEE Transactions on Information Theory* 22.6 (Nov. 1976), pp. 644–654. DOI: 10.1109/TIT.1976.1055638 (cited on page 6).

[8] R. L. Rivest, A. Shamir, and L. Adleman. 'A Method for Obtaining Digital Signatures and Public-key Cryptosystems'. In: *Commun. ACM* 21.2 (Feb. 1978), pp. 120–126. DOI: 10.1145/359340.359342 (cited on page 6).

[9] Taher ElGamal. 'A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms'. In: *Advances in Cryptology*. Ed. by George Robert Blakley and David Chaum. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985, pp. 10–18 (cited on page 6).

[10] P. W. Shor. 'Algorithms for quantum computation: discrete logarithms and factoring'. In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. Nov. 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700 (cited on page 6).

[11] Nick Herbert. 'FLASH—A superluminal communicator based upon a new kind of quantum measurement'. In: *N. Found Phys* 12.12 (1982), pp. 1171–1179. DOI: https://doi.org/10.1007/BF00729622 (cited on page 7).

[12] W. H. Zurek W. K. Wootters. 'A single quantum cannot be cloned'. In: *Nature* 299 (1982), pp. 802–803. DOI: https://doi.org/10.1038/299802a0 (cited on page 7).

[13] D. Dieks. 'Communication by EPR devices'. In: *Physics Letters A* 92.6 (1982), pp. 271–272. DOI: https://doi.org/10.1016/0375-9601(82)90084-6 (cited on page 7).

[14] James L. Park. 'The concept of transition in quantum mechanics'. In: *Foundations of Physics* 1.1 (1970), pp. 23–33. DOI: https://doi.org/10.1007/BF00708652 (cited on page 7).

[15] Stephen Wiesner. 'Conjugate Coding'. In: *SIGACT News* 15.1 (Jan. 1983), pp. 78–88. DOI: 10.1145/1008908.1008920 (cited on page 7).

[16] C. H. Bennett and G. Brassard. 'Quantum cryptography: Public key distribution and coin tossing'. In: *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*. 1984, pp. 175–179 (cited on pages 8, 13).

[17] Artur K. Ekert. 'Quantum cryptography based on Bell's theorem'. In: *Phys. Rev. Lett.* 67 (6 Aug. 1991), pp. 661–663. DOI: 10.1103/PhysRevLett.67.661 (cited on page 10).

[18] Charles H. Bennett, Gilles Brassard, and N. David Mermin. 'Quantum cryptography without Bell's theorem'. In: *Phys. Rev. Lett.* 68 (5 Feb. 1992), pp. 557–559. DOI: 10.1103/PhysRevLett.68.557 (cited on page 10).

[19] Nicolas Sangouard et al. 'Quantum repeaters based on atomic ensembles and linear optics'. In: *Rev. Mod. Phys.* 83.1 (Mar. 2011), pp. 33–80. DOI: 10.1103/RevModPhys.83.33 (cited on page 10).

[20] Stefano Pirandola et al. 'Fundamental limits of repeaterless quantum communications'. In: *Nature Communications* 8.1 (Apr. 2017). DOI: 10.1038/ncomms15043 (cited on page 10).

[21] M. Lucamarini et al. 'Overcoming the rate–distance limit of quantum key distribution without quantum repeaters'. In: *Nature* 557.7705 (May 2018), pp. 400–403. DOI: 10.1038/s41586-018-0066-6 (cited on page 11).

[22] M. Minder et al. 'Experimental quantum key distribution beyond the repeaterless secret key capacity'. In: *Nature Photonics* 13.5 (Mar. 2019), pp. 334–338. DOI: 10.1038/s41566-019-0377-7 (cited on page 11).

[23] Qiang Zhang et al. 'Large scale quantum key distribution: challenges and solutions [Invited]'. In: *Optics Express* 26.18 (Aug. 2018), p. 24260. DOI: 10.1364/oe.26.024260 (cited on page 11).

[24] Dominic Mayers and Andrew Yao. *Quantum Cryptography with Imperfect Apparatus*. 1998 (cited on page 11).

[25] Roger Colbeck. *Quantum And Relativistic Protocols For Secure Multi-Party Computation*. 2009 (cited on page 11).

[26] B. Hensen et al. 'Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres'. In: *Nature* 526 (Oct. 2015), 682 EP - (cited on page 11).

[27] Marissa Giustina et al. 'Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons'. In: *Phys. Rev. Lett.* 115 (25 Dec. 2015), p. 250401. DOI: 10.1103/PhysRevLett.115.250401 (cited on page 11).

[28] Lynden K. Shalm et al. 'Strong Loophole-Free Test of Local Realism'. In: *Phys. Rev. Lett.* 115 (25 Dec. 2015), p. 250402. DOI: 10.1103/PhysRevLett.115.250402 (cited on page 11).

[29] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. 'Measurement-Device-Independent Quantum Key Distribution'. In: *Physical Review Letters* 108.13 (Mar. 2012). DOI: 10.1103/physrevlett.108.130503 (cited on page 11).

[30] Feihu Xu et al. 'Practical aspects of measurement-device-independent quantum key distribution'. In: *New Journal of Physics* 15.11 (Nov. 2013), p. 113007. DOI: 10.1088/1367-2630/15/11/113007 (cited on page 11).

[31] Kyo Inoue, Edo Waks, and Yoshihisa Yamamoto. 'Differential Phase Shift Quantum Key Distribution'. In: *Phys. Rev. Lett.* 89 (3 June 2002), p. 037902. DOI: 10.1103/PhysRevLett.89.037902 (cited on page 11).

[32] K. Inoue, E. Waks, and Y. Yamamoto. 'Differential-phase-shift quantum key distribution using coherent light'. In: *Phys. Rev. A* 68 (2 Aug. 2003), p. 022317. DOI: 10.1103/PhysRevA.68.022317 (cited on page 11).

[33] Damien Stucki et al. 'Fast and simple one-way quantum key distribution'. In: *Applied Physics Letters* 87.19 (2005), p. 194108. DOI: 10.1063/1.2126792 (cited on page 11).

[34] Won-Young Hwang. 'Quantum Key Distribution with High Loss: Toward Global Secure Communication'. In: *Physical Review Letters* 91.5 (Aug. 2003). DOI: 10.1103/physrevlett.91.057901 (cited on page 12).

[35] S. Pirandola et al. *Advances in Quantum Cryptography*. 2019 (cited on page 12).

[36] Feihu Xu et al. *Quantum cryptography with realistic devices*. 2019 (cited on page 12).

[37] Eleni Diamanti and Anthony Leverrier. 'Distributing Secret Keys with Quantum Continuous Variables: Principle, Security and Implementations'. In: *Entropy* 17.9 (2015), pp. 6072–6092. DOI: 10.3390/e17096072 (cited on page 12).

[38] P. Sibson et al. 'Chip-based quantum key distribution'. In: *Nature Communications* 8.1 (2017), p. 13984. DOI: 10.1038/ncomms13984 (cited on page 12).

[39] Mauro Persechino et al. 'Correlations with on-chip detection and modulation for CVQKD (poster)'. In: *QCrypt 2017*. Cambridge, United Kingdom, Sept. 2017 (cited on page 12).

[40] G. Zhang et al. 'An integrated silicon photonic chip platform for continuous-variable quantum key distribution'. In: *Nature Photonics* (2019). DOI: 10.1038/s41566-019-0504-5 (cited on page 12).

[41] Giuseppe Vallone et al. 'Experimental Satellite Quantum Communications'. In: *Phys. Rev. Lett.* 115 (4 July 2015), p. 040502. DOI: 10.1103/PhysRevLett.115.040502 (cited on page 12).

[42] Kevin Günthner et al. 'Quantum-limited measurements of optical signals from a geostationary satellite'. In: *Optica* 4.6 (June 2017), pp. 611–616. DOI: 10.1364/OPTICA.4.000611 (cited on page 12).

[43] Hideki Takenaka et al. 'Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite'. In: *Nature Photonics* 11 (July 2017). Article, 502 EP - (cited on page 12).

[44] Sheng-Kai Liao et al. 'Satellite-to-ground quantum key distribution'. In: *Nature* 549 (Aug. 2017). Article, 43 EP - (cited on page 12).

[45] Juan Yin et al. 'Satellite-to-Ground Entanglement-Based Quantum Key Distribution'. In: *Phys. Rev. Lett.* 119 (20 Nov. 2017), p. 200501. DOI: 10.1103/PhysRevLett.119.200501 (cited on page 12).

[46] Robert Bedington, Juan Miguel Arrazola, and Alexander Ling. 'Progress in satellite quantum key distribution'. In: *npj Quantum Information* 3.1 (2017), p. 30. DOI: 10.1038/s41534-017-0031-5 (cited on page 12).

[47] Carlos Abellan et al. 'Quantum entropy source on an InP photonic integrated circuit for random number generation'. In: *Optica* 3.9 (Sept. 2016), p. 989. DOI: 10.1364/optica.3.000989 (cited on pages 13, 85).

[48] Xiao-Guang Zhang et al. 'Note: Fully integrated 3.2 Gbps quantum random number generator with real-time extraction'. In: *Review of Scientific Instruments* 87.7 (July 2016), p. 076102. DOI: 10.1063/1.4958663 (cited on pages 13, 85).

[49] Francesco Raffaelli et al. 'Generation of random numbers by measuring phase fluctuations from a laser diode with a silicon-on-insulator chip'. In: *Opt. Express* 26.16 (Aug. 2018), pp. 19730–19741. DOI: 10.1364/OE.26.019730 (cited on pages 13, 85).

[50] Leilei Huang and Hongyi Zhou. 'Integrated Gbps quantum random number generator with real-time extraction based on homodyne detection'. In: *J. Opt. Soc. Am. B* 36.3 (Mar. 2019), B130–B136. DOI: 10.1364/JOSAB.36.00B130 (cited on pages 13, 85).

[51] Mark Hillery, Vladimír Bužek, and André Berthiaume. 'Quantum secret sharing'. In: *Physical Review A* 59.3 (Mar. 1999), pp. 1829–1834. DOI: 10.1103/physreva.59.1829 (cited on page 13).

[52] Anna Pappa et al. 'Experimental plug and play quantum coin flipping'. In: *Nature Communications* 5.1 (Apr. 2014). DOI: 10.1038/ncomms4717 (cited on page 13).

[53] Mathieu Bozzio et al. 'Experimental investigation of practical unforgeable quantum money'. In: *npj Quantum Information* 4.1 (Jan. 2018). DOI: 10.1038/s41534-018-0058-2 (cited on page 13).

[54] Mathieu Bozzio, Eleni Diamanti, and Frédéric Grosshans. 'Semi-device-independent quantum money with coherent states'. In: *Physical Review A* 99.2 (Feb. 2019). DOI: 10.1103/physreva.99.022336 (cited on page 13).

[55] Niraj Kumar, Eleni Diamanti, and Iordanis Kerenidis. 'Efficient quantum communications with coherent state fingerprints over multiple channels'. In: *Physical Review A* 95.3 (Mar. 2017). DOI: 10.1103/physreva.95.032337 (cited on page 13).

[56] Niraj Kumar, Iordanis Kerenidis, and Eleni Diamanti. 'Experimental demonstration of quantum advantage for one-way communication complexity surpassing best-known classical protocol'. In: *Nature Communications* 10.1 (Sept. 2019). DOI: `10.1038/s41467-019-12139-z` (cited on page 13).

[57] Stephanie Wehner, David Elkouss, and Ronald Hanson. 'Quantum internet: A vision for the road ahead'. In: *Science* 362.6412 (2018). DOI: `10.1126/science.aam9288` (cited on page 13).

[58] *Quantum Internet Alliance (QIA)*. `http://quantum-internet.team/`. Accessed: 2019-09-30 (cited on page 13).

[59] *Industry Specification Group (ISG) on Quantum Key Distribution for Users (QKD)*. `https://www.etsi.org/committee/1430-qkd`. Accessed: 2019-09-30 (cited on page 14).

[60] Frédéric Grosshans. 'Communication et cryptographie quantiques avec des variables continues'. M. André DUCASSE, Président M. Nicolas CERF, Rapporteur M. Juan-Ariel LEVENSON, Rapporteur M. Thierry DEBUISSCHERT, Examinateur M. Claude FABRE, Examinateur M. Gerd LEUCHS, Membre invité M. Philippe GRANGIER, Directeur de thèse. Theses. Université Paris Sud - Paris XI, Dec. 2002 (cited on page 15).

[61] Jérôme Wenger. 'Dispositifs impulsionnels pour la communication quantique à variables continues'. Jury composé de : M. Alain ASPECT (Président) M. Nicolas CERF M. Juan-Ariel LEVENSON (Rapporteur) M. Jean-François ROCH (Rapporteur) Mme Rosa TUALLE-BROURI. Theses. Université Paris Sud - Paris XI, Sept. 2004 (cited on page 15).

[62] Jérôme Lodewyck. 'Quantum key distribution device with coherent states at telecom wavelength'. Theses. Université Paris Sud - Paris XI, Dec. 2006 (cited on page 15).

[63] Simon Fossier. 'Implementation and Evaluation of Quantum Key Distribution Devices at Telecom Wavelength'. Theses. Université Paris Sud - Paris XI, Oct. 2009 (cited on page 15).

[64] Anthony Leverrier. 'Theoretical study of continuous-variable quantum key distribution'. Theses. Télécom ParisTech, Nov. 2009 (cited on pages 15, 23, 155, 161).

[65] Paul Jouguet. 'Security and performance of continuous-variable quantum key distribution systems'. Theses. Télécom ParisTech, Sept. 2013 (cited on pages 15, 95).

[66] Mauro Persechino. 'Experimental study of the integration of continuous-variable quantum key distribution into a silicon photonics device'. Theses. Université Paris-Saclay, Dec. 2017 (cited on pages 15, 101).

[67] Renato Renner. *Security of Quantum Key Distribution*. 2005 (cited on page 15).

[68] Robert König et al. 'Small Accessible Quantum Information Does Not Imply Security'. In: *Phys. Rev. Lett.* 98 (14 Apr. 2007), p. 140502. DOI: `10.1103/PhysRevLett.98.140502` (cited on page 15).

[69] T. C. Ralph. 'Continuous variable quantum cryptography'. In: *Phys. Rev. A* 61 (1 Dec. 1999), p. 010303. DOI: `10.1103/PhysRevA.61.010303` (cited on page 16).

[70] Mark Hillery. 'Quantum cryptography with squeezed states'. In: *Phys. Rev. A* 61 (2 Jan. 2000), p. 022309. DOI: `10.1103/PhysRevA.61.022309` (cited on page 16).

[71] N. J. Cerf, M. Lévy, and G. Van Assche. 'Quantum distribution of Gaussian keys using squeezed states'. In: *Phys. Rev. A* 63 (5 Apr. 2001), p. 052311. DOI: `10.1103/PhysRevA.63.052311` (cited on page 16).

[72] Frédéric Grosshans and Philippe Grangier. 'Continuous Variable Quantum Cryptography Using Coherent States'. In: *Phys. Rev. Lett.* 88 (5 Jan. 2002), p. 057902. DOI: `10.1103/PhysRevLett.88.057902` (cited on pages 16, 27, 170).

[73] Frédéric Grosshans et al. 'Quantum key distribution using gaussian-modulated coherent states'. In: *Nature* 421.6920 (Jan. 2003), pp. 238–241. DOI: `10.1038/nature01289` (cited on pages 16, 27).

[74] Kazuro Kikuchi. 'Fundamentals of Coherent Optical Fiber Communications'. In: *J. Lightwave Technol.* 34.1 (Jan. 2016), pp. 157–179 (cited on pages 18, 19, 37, 41, 42, 49, 53).

[75] A. Davis et al. 'Phase diversity techniques for coherent optical receivers'. In: *Journal of Lightwave Technology* 5.4 (Apr. 1987), pp. 561–572. DOI: 10.1109/JLT.1987.1075539 (cited on page 18).

[76] Paul Jouguet et al. 'Experimental demonstration of long-distance continuous-variable quantum key distribution'. In: *Nature Photonics* 7 (Apr. 2013), 378 EP - (cited on pages 20, 31, 87, 103).

[77] Paul Jouguet, Sébastien Kunz-Jacques, and Eleni Diamanti. 'Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution'. In: *Physical Review A* 87.6 (June 2013). DOI: 10.1103/physreva.87.062313 (cited on page 21).

[78] Bing Qi et al. 'Generating the Local Oscillator "Locally" in Continuous-Variable Quantum Key Distribution Based on Coherent Detection'. In: *Phys. Rev. X* 5 (4 Oct. 2015), p. 041009. DOI: 10.1103/PhysRevX.5.041009 (cited on page 21).

[79] Daniel B. S. Soh et al. 'Self-Referenced Continuous-Variable Quantum Key Distribution Protocol'. In: *Phys. Rev. X* 5 (4 Oct. 2015), p. 041010. DOI: 10.1103/PhysRevX.5.041010 (cited on page 21).

[80] Fabian Laudenbach et al. 'Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator'. In: *Quantum* 3 (Oct. 2019), p. 193. DOI: 10.22331/q-2019-10-07-193 (cited on page 21).

[81] Raúl García-Patrón and Nicolas J. Cerf. 'Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution'. In: *Phys. Rev. Lett.* 97 (19 Nov. 2006), p. 190503. DOI: 10.1103/PhysRevLett.97.190503 (cited on page 25).

[82] Miguel Navascués, Frédéric Grosshans, and Antonio Acín. 'Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography'. In: *Phys. Rev. Lett.* 97 (19 Nov. 2006), p. 190502. DOI: 10.1103/PhysRevLett.97.190502 (cited on page 25).

[83] R. Renner and J. I. Cirac. 'de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography'. In: *Physical Review Letters* 102.11 (Mar. 2009). DOI: 10.1103/physrevlett.102.110504 (cited on page 26).

[84] Anthony Leverrier. 'Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction'. In: *Physical Review Letters* 118.20 (May 2017). DOI: 10.1103/physrevlett.118.200501 (cited on page 26).

[85] Anthony Leverrier and Philippe Grangier. 'Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation'. In: *Phys. Rev. A* 83 (4 Apr. 2011), p. 042312. DOI: 10.1103/PhysRevA.83.042312 (cited on pages 27, 77).

[86] Shouvik Ghorai et al. 'Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation'. In: *Phys. Rev. X* 9 (2 June 2019), p. 021059. DOI: 10.1103/PhysRevX.9.021059 (cited on pages 27, 77).

[87] Jie Lin, Twesh Upadhyaya, and Norbert Lütkenhaus. *Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution*. 2019 (cited on pages 27, 77).

[88] Eneet Kaur, Saikat Guha, and Mark M. Wilde. *Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution*. 2019 (cited on pages 27, 77).

[89] Raúl García-Patrón. 'Quantum Information with Optical Continuous Variables: from Bell Tests to Key Distribution'. Theses. 2008 (cited on page 27).

[90] Paul Jouguet et al. 'Analysis of imperfections in practical continuous-variable quantum key distribution'. In: *Physical Review A* 86.3 (Sept. 2012). DOI: 10.1103/physreva.86.032309 (cited on pages 28, 63).

[91] R. H. Norden. 'A Survey of Maximum Likelihood Estimation'. In: *International Statistical Review / Revue Internationale de Statistique* 40.3 (1972), pp. 329–354 (cited on page 32).

[92] Proakis. *Digital Communications 5th Edition*. McGraw Hill, 2007 (cited on page 37).

[93] Alan V. Oppenheim, Ronald W. Schafer, and John R. Buck. *Discrete-Time Signal Processing*. Second. Prentice-hall Englewood Cliffs, 1999 (cited on page 37).

[94] Alex Alvarado et al. 'Achievable Information Rates for Fiber Optics: Applications and Computations'. In: *Journal of Lightwave Technology* PP (July 2017). DOI: 10.1109/JLT.2017.2786351 (cited on page 43).

[95] P. Welch. 'The use of fast Fourier transform for the estimation of power spectra: A method based on time averaging over short, modified periodograms'. In: *IEEE Transactions on Audio and Electroacoustics* 15.2 (June 1967), pp. 70–73. DOI: 10.1109/TAU.1967.1161901 (cited on page 64).

[96] Paul Jouguet, David Elkouss, and Sébastien Kunz-Jacques. 'High-bit-rate continuous-variable quantum key distribution'. In: *Physical Review A* 90.4 (Oct. 2014). DOI: 10.1103/physreva.90.042329 (cited on page 72).

[97] S. Tanzilli et al. 'On the genesis and evolution of Integrated Quantum Optics'. In: *Laser & Photonics Reviews* 6.1 (2012), pp. 115–143. DOI: 10.1002/lpor.201100010 (cited on page 83).

[98] Adeline Orieux and Eleni Diamanti. 'Recent advances on integrated quantum communications'. In: *Journal of Optics* 18.8 (July 2016), p. 083002. DOI: 10.1088/2040-8978/18/8/083002 (cited on page 83).

[99] Gordon E. Moore. 'Cramming more components onto integrated circuits'. In: *Electronics* 38.8 (Apr. 1965) (cited on page 83).

[100] Lars Thylén and L. Wosinski. 'Integrated photonics in the 21st century'. In: *Photonics Research* 2 (Apr. 2014). DOI: 10.1364/PRJ.2.000075 (cited on page 83).

[101] C. Dragone. 'An N*N optical multiplexer using a planar arrangement of two star couplers'. In: *IEEE Photonics Technology Letters* 3.9 (Sept. 1991), pp. 812–815. DOI: 10.1109/68.84502 (cited on page 83).

[102] *Refractive index database*. https://refractiveindex.info/. Accessed: 2019-09-30 (cited on page 84).

[103] F. S. Ujager, S. M. H. Zaidi, and U. Younis. 'A review of semiconductor lasers for optical communications'. In: *7th International Symposium on High-capacity Optical Networks and Enabling Technologies*. Dec. 2010, pp. 107–111. DOI: 10.1109/HONET.2010.5715754 (cited on page 85).

[104] Kieran Cooney and Frank H. Peters. 'Analysis of multimode interferometers'. In: *Opt. Express* 24.20 (Oct. 2016), pp. 22481–22515. DOI: 10.1364/OE.24.022481 (cited on page 85).

[105] Eng Png Ching, Song Sun, and Ping Bai. 'nanoph'. In: vol. 4. 3. 2019 2015. Chap. State-of-the-art photodetectors for optoelectronic integration at telecommunication wavelength, p. 277. DOI: 10.1515/nanoph-2015-0012 (cited on page 85).

[106] Lee Carroll et al. 'Photonic Packaging: Transforming Silicon Photonic Integrated Circuits into Photonic Devices'. In: *Applied Sciences* 6.12 (2016). DOI: 10.3390/app6120426 (cited on page 86).

[107] D. Vasylyev, W. Vogel, and F. Moll. 'Satellite-mediated quantum atmospheric links'. In: *Phys. Rev. A* 99 (5 May 2019), p. 053830. DOI: 10.1103/PhysRevA.99.053830 (cited on pages 117, 138, 181).

[108] Vladyslav C. Usenko et al. 'Entanglement of Gaussian states and the applicability to quantum key distribution over fading channels'. In: *New Journal of Physics* 14.9 (Sept. 2012), p. 093048. DOI: 10.1088/1367-2630/14/9/093048 (cited on page 118).

[109] Sheng-Kai Liao et al. 'Satellite-Relayed Intercontinental Quantum Network'. In: *Physical Review Letters* 120.3 (Jan. 2018). DOI: 10.1103/physrevlett.120.030501 (cited on page 134).

[110] D. Yu. Vasylyev, A. A. Semenov, and W. Vogel. 'Toward Global Quantum Communication: Beam Wandering Preserves Nonclassicality'. In: *Phys. Rev. Lett.* 108 (22 June 2012), p. 220501. DOI: 10.1103/PhysRevLett.108.220501 (cited on pages 139, 181).

[111] Arun Majumdar and Jennifer Ricklin. 'Free-Space Laser Communications'. In: (Jan. 2008). DOI: 10.1007/978-0-387-28677-8 (cited on page 139).

[112] Gerardo Adesso and Fabrizio Illuminati. 'Entanglement in continuous-variable systems: recent advances and current perspectives'. In: *Journal of Physics A: Mathematical and Theoretical* 40.28 (June 2007), pp. 7821–7880. DOI: 10.1088/1751-8113/40/28/s01 (cited on pages 155, 158, 171).

[113] R. Simon, N. Mukunda, and Biswadeb Dutta. 'Quantum-noise matrix for multimode systems: U(n) invariance, squeezing, and normal forms'. In: *Phys. Rev. A* 49 (3 Mar. 1994), pp. 1567–1583. DOI: 10.1103/PhysRevA.49.1567 (cited on page 161).

[114] R. Simon, S. Chaturvedi, and V. Srinivasan. 'Congruences and canonical forms for a positive matrix: Application to the Schweinler–Wigner extremum principle'. In: *Journal of Mathematical Physics* 40.7 (July 1999), pp. 3632–3642. DOI: 10.1063/1.532913 (cited on page 162).

[115] Michael M. Wolf, Geza Giedke, and J. Ignacio Cirac. 'Extremality of Gaussian Quantum States'. In: *Physical Review Letters* 96.8 (Mar. 2006). DOI: 10.1103/physrevlett.96.080502 (cited on pages 171, 178).

[116] Frédéric Grosshans and Nicolas J. Cerf. 'Continuous-Variable Quantum Cryptography is Secure against Non-Gaussian Attacks'. In: *Phys. Rev. Lett.* 92 (4 Jan. 2004), p. 047905. DOI: 10.1103/PhysRevLett.92.047905 (cited on page 177).

[117] Jérôme Lodewyck et al. 'Quantum key distribution over 25 km with an all-fiber continuous-variable system'. In: *Phys. Rev. A* 76 (4 Oct. 2007), p. 042305. DOI: 10.1103/PhysRevA.76.042305 (cited on page 177).

[118] Jérôme Lodewyck and Philippe Grangier. 'Tight bound on the coherent-state quantum key distribution with heterodyne detection'. In: *Phys. Rev. A* 76 (2 Aug. 2007), p. 022332. DOI: 10.1103/PhysRevA.76.022332 (cited on page 177).

[119] J. Sudjana et al. 'Tight bounds on the eavesdropping of a continuous-variable quantum cryptographic protocol with no basis switching'. In: *Phys. Rev. A* 76 (5 Nov. 2007), p. 052301. DOI: 10.1103/PhysRevA.76.052301 (cited on page 177).

[120] Alexander S Holevo. *Probabilistic and Statistical Aspects of Quantum Theory; 2nd ed.* Publications of the Scuola Normale Superiore Monographs. Dordrecht: Springer, 2011 (cited on page 178).

[121] R. L. Fante. 'Electromagnetic beam propagation in turbulent media: An update'. In: *Proceedings of the IEEE* 68.11 (Nov. 1980), pp. 1424–1443. DOI: 10.1109/PROC.1980.11882 (cited on page 183).

[122] I. Ali, N. Al-Dhahir, and J.E. Hershey. 'Doppler characterization for LEO satellites'. In: *Communications, IEEE Transactions on* 46.3 (Mar. 1998), pp. 309–313. DOI: 10.1109/26.662636 (cited on page 186).

# Glossary

The next list describes several symbols and acronyms used within the body of the document.

| | |
|---|---|
| AC | Alternating Current |
| ADC | Analogue to Digital Converter |
| AES | Advanced Encryption Standard |
| AIR | Achievable Information Rate |
| AM | Amplitude Modulator |
| ASIC | Application-specific Integrated Circuit |
| AWG | Arbitrary Waveform Generator |
| AWGN | Additive White Gaussian Noise |
| B2B | Back-to-Back |
| BB84 | Bennet-Brassard 1984 |
| Bd | Baud or symbol per second |
| BER | Bit Error Rate |
| BQP | Bounded-error Quantum Polynomial time |
| BS | Beam Splitter |
| BW | Beam Wandering |
| CAZAC | Constant Amplitude Zero Autocorrelation |
| CFE | Carrier Frequency Estimation |
| CMA | Constant Modulus Algorithm |
| CMOS | Complementary Metal-Oxide Semiconductor |
| CMRR | Common Mode Rejection Ratio |
| COW | Coherent One-Way |
| CPE | Carrier Phase Estimation |
| CPM | Completely Positive Map |
| CV | Continuous Variable |
| CV-QDK | Continuous Variable Quantum Key Distribution |
| CW | Continuous Wave |

| | |
|---|---|
| DAC | Digital to Analogue Converter |
| DAQ | Digital AcQuisition (card) |
| DC | Direct Current |
| DD-LMS | Decision Directed Least Mean Squares |
| DI-QKD | Device Independent Quantum Key Distribution |
| DoS | Denial-of-Service |
| DP | Double Polarization |
| DPS | Differential Phase Shift |
| DR | Direct Reconciliation |
| DSP | Digital Signal Processing |
| DUT | Device Under Test |
| DV-QKD | Discrete-Variable Quantum Key Distribution |
| EDFA | Erbium-Doped Fibre Amplifiers |
| EIC | Electronic Integrated Circuit |
| EOM | Electro-Optical Modulator |
| EPR | Einstein-Podolsky-Rosen |
| ETSI | European Telecommunications Standards Institute |
| FEC | Forward Error Correction |
| FIR | Finite Impulse Response |
| FPGA | Field-programmable gate array |
| FSK | Frequency Shift Keying |
| FSO | Free-Space Optics |
| FZC | Frank–Zadoff–Chu |
| GEO | Geosynchronous Equatorial Orbit |
| GG02 | Grosshans-Grangier 2002 |
| GMI | Generalized Mutual Information |
| GNSS | Global Navigation Satellite Systems |
| GPS | Global Positioning System |
| GSO | GeoSynchronous Orbit |

| | |
|---|---|
| HEO | High Earth Orbit |
| IC | Integrated Circuit |
| ICR | Integrated Coherent Receiver |
| ICT | Information and Communication Technology |
| IEEE | Institute of Electrical and Electronics Engineers |
| IETF | Internet Engineering Task Force |
| IM-DD | Intensity Modulation and Direct Detection |
| InGaAs | Indium Gallium Arsenide |
| InP | Indium Phosphide |
| IOGS | Institut d'Optique Graduate School |
| IQ | In-phase and Quadrature |
| IQM | In-Phase and Quadrature Modulator |
| ISI | Inter-Symbol Interference |
| LDPC | Low-Density Parity-Check |
| LEO | Low Earth Orbit |
| LLO | Local Local Oscillator |
| LMS | Least Mean Squares |
| LO | Local Oscillator |
| LTI | Linear and Time Invariant |
| MDI-QKD | Measure Device Independent Quantum Key Distribution |
| MEO | Medium Earth Orbit |
| MI | Mutual Information |
| MLE | Maximum Likelihood Estimator |
| MSPS | MegaSamples Per Second |
| NIST | National Institute of Standards and Technology |
| NP | Nondeterministic Polynomial time |
| OOK | On-Off Keying |
| OPLL | Optical Phase Locking Loop |
| OSA | Optical Spectrum Analyser |

| | |
|---|---|
| PBS | Polarization Beam Splitter |
| PCB | Printed Circuit Board |
| PCI | Peripheral Component Interface |
| PCS | Probabilistic Constellation Shaping |
| PDK | Process Design Kit |
| PDT | Probability Distribution of Transmittance |
| PDTC | Probability Distribution of Transmission Coefficient |
| PDTE | Probability Distribution of Transmission Efficiency |
| PE | Parameter(s) Estimation |
| PIC | Photonic Integrated Circuit |
| PLL | Phase Locking Loop |
| PM | Phase Modulator |
| PM | Polarization Maintaining (fibre) |
| POVM | Positive-Operator Valued Measure |
| PSD | Power Spectral Density |
| PXI | PCI eXtensions for Instrumentation |
| QAM | Quadrature Amplitude Modulation |
| QBER | Quantum Bit Error Rate |
| QKD | Quantum Key Distribution |
| QPSK | Quadrature Phase Shift Keying |
| QRNG | Quantum Random Number Generator |
| R& D | Research and Development |
| RC | Raised Cosine |
| RF | Radio Frequency |
| RIN | Relative Intensity Noise |
| RNG | Random Number Generator |
| ROF | Roll-off factor |
| RR | Reverse Reconciliation |
| RRC | Root-raised cosine |

| | |
|---|---|
| RSA | Rivest–Shamir–Adleman |
| RX | Receiver |
| SKR | Secret Key Rate |
| SMF | Single Mode Fibre |
| SNR | Signal-to-noise ratio |
| SNU | Shot Noise Unit |
| SOI | Silicon On Insulator |
| SP | Single Polarization |
| TE | Transverse Electric |
| TF-QKD | Twin-Field Quantum Key Distribution |
| TIA | Transimpedance Amplifier |
| TLO | Transmitted Local Oscillator |
| TM | Transverse Magnetic |
| TMS | Two-Mode Squeezed (state) |
| TMSV | Two-Mode Squeezed Vacuum |
| TX | Transmitter |
| VOA | Variable Optical Attenuator |
| WDM | Wavelength Division Multiplexing |
| XOR | Exclusive OR |

ÉCOLE DOCTORALE
Ondes et Matière
(EDOM)

**Titre :** Conception et réalisation de dispositifs de distribution de clé quantique à variables continues à haute performance

**Mots clés :** optique quantique, cryptographie quantique, télécommunications optiques, photonique sur silicium, détection cohérente

**Résumé :** La distribution quantique de clé (QKD) est une des premières technologies quantiques qui ait atteint un stade commercial, en proposant une solution au problème de la distribution d'une clé cryptographique entre deux entités, et en garantissant une sécurité à long terme. Elle est maintenant proche de la maturité technologique, et plusieurs méthodes sont disponibles en pratique. Cette thèse étudie la distribution quantique de clé à variables continues (CV-QKD), qui a plusieurs éléments communs avec les communications optiques cohérentes classiques, et qui pourrait permettre à beaucoup d'utilisateurs d'accéder à la QKD.
L'utilisation de techniques de traitement numérique (Digital Signal Processor ou DSP), typiques en communications classiques, a été seulement partiellement exploitée dans les implémentations CV-QKD précédentes. Dans ce travail nous mettons en œuvre expérimentalement des techniques usuelles dans les communications classiques, comme la mise en forme d'impulsions, le filtrage adaptatif et la récupération de mode. Notre objectif est d'augmenter ainsi le taux de clé secrète, et d'optimiser l'utilisation de la bande passante disponible.
La possibilité d'intégrer des composants dans un circuit photonique (PIC) est un autre avantage de CV-QKD. Nous avons testé un PIC en silicium intégrant un coupleur hybride 180° et deux photodiodes en germanium. Les paramètres mesurés sont compatibles avec la génération de clé secrète dans ces dispositifs.
Un des facteurs les plus limitants de QKD est la chute des performances dans les canaux ayant des pertes très élevées, typiquement des fibres optiques dont la longueur dépasse la centaine de kilomètres. Mais la distance utile peut être étendue notablement en utilisant des liens en espace libre, en particulier avec des satellites, où les pertes à une certaine distance peuvent être inférieures à celles des fibres. Nous considérons un modèle pour le canal descendant et prédisons les taux de clé secrète attendus à différentes altitudes pour CV-QKD. Ces résultats aboutissent à une technologie potentiellement utilisable pour les communications par satellite, en étendant la portée jusqu'à des distances intercontinentales.

**Title :** Design and implementation of high-performance devices for continuous-variable quantum key distribution

**Keywords :** quantum optics, quantum cryptography, optical telecommunication, silicon photonics, coherent detection systems

**Abstract :** Quantum key distribution (QKD) is one of the first quantum technologies that were able to provide commercially meaningful solutions to the problem of distributing cryptographic keys between trusted parties, guaranteeing long term security. It is now progressing towards technical maturity, by proposing multiple implementation alternatives. In this thesis, we study Continuous-Variables QKD (CV-QKD), which shares many common elements with classical coherent communication systems, and is a good candidate to facilitate the access to QKD for more users.
The use of digital signal processing (DSP) techniques typical in classical communications has been only partially exploited in previous CV-QKD implementations. We experimentally implement standard telecommunication techniques like pulse shaping, adaptive filtering and mode recovery in order to improve the quantum secret key rate and optimize the occupied bandwidth.
The potential of integration of the components in a photonic integrated circuit (PIC) is another important aspect of CV-QKD. We have tested a silicon photonics PIC integrating a 180° hybrid detector with two germanium photodiodes, showing that measured parameters are compatible with the generation of secret key.
One of the most limiting factors of QKD is the performance under lossy channels, which is common in optical fibre for distances in the order of hundred kilometers. The range can be significantly extended using free space communications, and in particular satellites, where the losses at longer distances can be lower than those in fibre. We consider a model for a downlink satellite channel and predict the achievable secret key rates at different altitudes for CV-QKD, resulting in a potentially feasible technology for satellite communications, extending the range to intercontinental distances.

**Université Paris-Saclay**
Espace Technologique / Immeuble Discovery
Route de l'Orme aux Merisiers RD 128 / 91190 Saint-Aubin, France