Convergence of quantum and classical communications

Raphaël Aymeric

INSTITUT POLYTECHNIQUE DE PARIS

NNT : 2022IPPAT033

Thèse de doctorat

Convergence of quantum and classical communications

Thèse de doctorat de l'Institut Polytechnique de Paris
préparée à Télécom Paris

École doctorale n°626 École doctorale de l'Institut Polytechnique de Paris (EDIPP)
Spécialité de doctorat : Information, Communications, Électronique

Thèse présentée et soutenue à Palaiseau, le 18/10/2022, par

RAPHAËL AYMERIC

Composition du Jury :

Eleni Diamanti CNRS Research Director, LIP6, Sorbonne Université	Rapporteur
Tobias Gehring Associate Professor, Technical University of Denmark	Rapporteur
Jean-François Roch Professor, Ecole Normale Supérieure Paris-Saclay	Président du Jury
Andreas Poppe Senior Scientist, AIT Austrian Institute of Technology, GmbH, Vienna	Examinateur
Valerio Pruneri Professor, ICFO Institute of Photonic Sciences, Barcelona	Examinateur
Yves Jaouën Professor, Télécom Paris, Institut Polytechnique de Paris	Directeur de thèse
Romain Alléaume Professor, Télécom Paris, Institut Polytechnique de Paris	Co-directeur de thèse

Acknowledgements

Et voilà, le fameux graal tant attendu, le titre de docteur. On m'avait prévenu que le doctorat était une aventure, et ça l'a certainement été pour moi. Une aventure qui n'aurait pû aboutir sans toutes les personnes qui m'ont accompagné, aidé, encouragé et supporté. Je tiens à leur adresser mes remerciements ici.

Tout d'abord, je souhaite commencer par remercier Romain et Yves, qui m'ont encadré et guidé tout au long de cette thèse. Merci à Romain pour avoir partagé ses connaissances du monde quantique et pour des discussions stimulantes sur l'avenir de la QKD et sa place dans le monde de la cryptographie. Il a toujours su me pousser a améliorer mon travail, de la méthode employée à la manière de réstituer les résultats. Merci également à Yves, qui m'a appris tout ce que je sais sur les communications cohérentes et qui a passé d'inombrables heures au laboratoire pour m'aider à matérialiser notre expérience de CV-QKD.

Je souhaite également remercier mes collègues, qui m'ont accompagné dans cette aventure. Mes collègues d'IQA, Nilesh, Francesco, Yuan, Guillaume, merci pour tous ces moments partagés ensemble. Merci à mes collègues de labo également, Pierre et Peter, pour les barres, surement causées par des prises de mesures excessives et répétées.

Cette quête dans le monde quantique a commencé à Télécom Paris avec Raja, sans qui elle n'aurait peut-être jamais commencée... Ca a été un grand bonheur d'avoir un ami aussi proche que Raja avec qui partager nos expériences respectives du doctorat et pour discuter du monde quantique ensemble.

La thèse déborde aussi sur le quotidien, et je me dois donc de remercier ceux qui l'ont partagé avec moi au long de ces 4 années. Mes remerciements vont à mes collocataires et amis, Poune et Marin, qui ont vécu cette aventure à mes côtés. Comme nous avons changés pendant ces 4 ans, nous avons chacun eu notre chemin à parcourir.

Un merci tout particulier à Inés, qui a su m'encourager dans les moments les plus difficiles et qui m'a aidé a faire retomber la pression quand j'en avais le plus besoin.

Enfin, je veux remercier mes parents, qui m'ont soutenu pendant toutes ces années d'études et sans qui je n'aurais jamais pu réussir.

Resumé de la thèse en français

Les ordinateurs quantiques ont été conceptualisés pour la première fois par Richard Feynman, qui dresse le constat suivant : un ordinateur classique ne peut pas simuler de manière efficace un système quantique. La raison sous-jacente est que le nombre de bits nécessaires pour décrire un système quantique augmente de manière exponentielle avec le nombre d'états quantiques du système, et ce à cause du principe de superposition. D'après Feynman, seul un ordinateur quantique dont les éléments de bases, les qubits, sont eux aussi quantiques, peut permettre de décrire de tels systèmes.

Les ordinateurs quantiques peuvent, par leur nature quantique, permettre de réaliser certaines taches au-dessus des capacités des ordinateurs classiques. Par exemple, il à été démontré que certains problèmes mathématiques, tels que la factorisation en nombres premiers ou le problème du logarithme discret, seraient solvables en un temps polynomial par l'ordinateur quantique. Or, ces problèmes mathématiques servent de fondations à la cryptographie à clé asymétrique. Il est donc impossible de garantir la sécurité de nos communications dans un avenir ou l'ordinateur quantique est omniprésent.

Les ordinateurs quantiques renferment donc de grandes promesses d'avancées technologiques, mais ils représentent aussi une menace pour la sécurité de nos systèmes de communications actuels. Face à ce problème, une solution est développée qui est appelée *cryptographie post-quantique*. Ce domaine cherche à construire des algorithmes de chiffrements basés sur des problèmes mathématiques pour lesquels l'ordinateur quantique ne présente pas, à priori, d'avantage significatif sur un ordinateur classique. Une deuxième approche, plus originale, à également vu le jour pour pallier au problème de l'ordinateur quantique. Cette dernière s'appelle la *distribution quantique de clé* (QKD) et est l'objet principal de cette thèse.

Les protocoles de distribution de clé quantique (QKD) permettent de construire des canaux de communications sensibles à l'espionage grace aux propriétés quantiques fondamentales de la lumière. Ces protocoles ont déjà été validés en laboratoire et même sur le terrain. Cependant l'un des principaux défis à surpasser pour déployer de tels protocoles à grande échelle est le coût de déploiement de la technologie, lié à l'installation de toute l'infrastructure nécessaire pour générer, transmettre et mesurer les états quantiques. Une solution attrayante en ce sens serait d'exploiter l'infrastructure de fibre optique déjà existante pour executer mettre en oeuvre de tels protocoles.

Cela implique cependant de faire coexister des signaux quantiques avec des signaux télécoms classiques, déjà présents sur cette infrastructure. Cette coexistence peut être un défi technique à cause de la sensibilité des états quantiques aux perturbations extérieures. Dans cette thèse, nous nous intéressons plus particulièrement aux protocoles de distribution de clé quantique à variables continues (CV-QKD), car leur proximité avec les communications cohérentes classiques indiquent qu'ils sont de bons candidats pour coexister sur une même fibre.

En partant du principe que les protocoles CV-QKD sont destinés, à terme, à être déployés de manière conjointe avec des protocoles de communication classique, la question qui se pose est la suivante. Cette coexistence avec des signaux classiques est-elle forcément un désavantage pour la CV-QKD ? Nous articulons notre réponse en deux projets distincts et nous montrons qu'en construisant de façon conjointe des protocoles de communication quantique et classique, la coexistence avec des signaux classiques peut présenter des avantages exploitables pour la CV-QKD.

Notre premier travail est une démonstration expérimentale dans laquelle nous montrons que le

signal classique peut servir, dans certains cas, de signal pilote au signal quantique. Cette construction permet notamment de s'affranchir de signaux pilotes auxiliaires généralement nécessaires en CV-QKD et d'effectuer des communications classiques et quantiques de manière conjointe.

Dans un second travail, nous montrons que le bruit généré par des canaux classiques peut servir à dissimuler le signal quantique. La communication quantique peut alors être réalisée de façon indétectable, ou « covert », ce qui, combiné à une échange de clé par QKD permet d'envisager des garanties de sécurité extrêmement élevées. Nous analysons les conditions nécessaires, à la faisabilité du déploiement covert de la CV-QKD et proposons des modèles pertinents à l'études de tels protocoles. Les conclusions tirées de ce travail de doctorat sont que, dans un contexte de coexistence classique/quantique, la construction des protocoles de communication de manière conjointe peut-être bénéfique à la fois aux communications quantiques et aux communications quantiques.

Contents

Introduction

From quantum mechanics to quantum technologies.

Our journey begins with the inception of quantum mechanics at the beginning of the 20^{th} century. At the time classical physics used to describe macroscopic systems were though to be absolute and to apply to all physical systems. Then, German physicist Max Planck introduced energy quanta and showed that this enables a complete description of blackbody radiation at thermal equilibrium, a challenge scientists were unable to tackle using classical physics. I personally find it amazing that he introduced his quantification *reluctantly* because of how absurd this concept was at the time, and how by doing so he initiated a series of pioneering works which led to the formalism of quantum mechanics used today.

Towards the middle of the 20^{th} century, two other major scientific fields were born which play a central role today. On the one hand the field of information theory, whose founding father is arguably the American scientist Claude Shannon, formally defines the notion of information and derives the amount that can be shared over a channel. Information theory is a cornerstone of modern digital communications. On the other hand the field of computer science, which owes a great deal to British scientist Alan Turing, revolutionized our society by providing mankind with one of the most powerful tools we've ever had : the computer.

Later, exciting interconnections started to develop between these fields. Questions about the quantity of classical information contained in quantum systems led to the development of the quantum counterpart of classical information theory: quantum information theory. An interesting result here is that when considering a communication protocol where the information is encoded in quantum states, the amount of information leaked during the transmission can be bounded thanks to fundamental quantum properties. Based on this idea, the first proposal of a quantum key distribution (QKD) protocol was submitted by Charles Bennett and Gilles Brassard in 1984 [1]. The goal of QKD protocols is to share a secret –the key– between distant parties in an adversarial setting, which has potential applications in the field of cryptography. The revolutionary aspect of QKD is that it constitutes a challenge to the security of classical key distribution techniques because the security of QKD does not involve any assumptions on the computing power of the adversary and hence permits to share a secret key with so-called *information-theoretic* security.

In the meantime, in 1981, Richard Feynman asked during a conference presentation [2] the question of how to simulate quantum systems and came to the conclusion that classical computers were not adequate to the task, because there is no succinct way to describe classically a quantum state of many particles. He then proposed to use a quantum computer to do this. Instead of functioning with bits, the quantum computer should perform operations on *qubits* which can be *entangled* with other qubits or in *superposition* of several states. Harnessing these properties, the amount of resources needed for the quantum computer to simulate quantum systems scales linearly with the size of the system to simulate, as opposed to exponentially for a classical computer. Feynman's talk undoubtedly played an important role in launching the field of quantum computing since it naturally spurred interest in the other tasks for which a quantum computer could outperform a classical computer.

In 1994, Peter Shor exhibited two problems for which a quantum computer had a significant ad-

vantage over a classical computer [3]. These are the factoring into prime numbers problem and the discrete-log problem. Since they are known to quickly become intractable for classical computers, these are currently used as the foundation for secure key distribution protocols in modern communications. Shor's results meant that current key distribution algorithms have an expiration date, and led cryptographers to refer to the creation of a quantum computer as the *quantum apocalypse.*

What about now ?

Thirty years later, building a large scale quantum computer still constitutes a remarkable challenge [4]. The core of the problem is that qubits collapse to classical states as they interact with the environment, hence quantum computers need to be strongly isolated from random interactions. At the same time though, we need to be able to interact with the qubits from the outside, in order to prepare the system in the desired state, apply quantum gates to the qubits to perform the quantum computation and then to read out the qubits so we can find the result of our computation. Building a quantum computer with all the desired features is a *very* difficult task.

Nonetheless considerable progress has been seen in the field, and today several large companies have developed quantum processors [5, 6, 7]. Even if these are still limited to a number of qubits around 200, this is sufficient for cryptographers to ring the alarm [8]. They typically need cryptographic algorithms to be safe for at least several years, sometimes several decades depending on the usage. This cannot be the case if a quantum computer that can implement Shor's algorithm is created in the next 10 or 20 years, because entities could potentially store encrypted communications today to break them then. Hence increasing attention is given to shifting vulnerable cryptographic primitives to quantum-safe primitives *i.e.* primitives for which a quantum computer should not in principle provide a considerable advantage over classical computers.

In particular it is the key distribution algorithms which are vulnerable to quantum computers and as such they are the primitives which require quantum-safe alternatives. Two are currently being developed in research teams. The first is to replace the vulnerable key distribution protocols by new protocols based on problems which remain difficult to solve even for quantum computers [9]. This field is called *post-quantum* cryptography and follows in the traditional way of considering cryptography in which the security of the protocol assumes that the adversary has limited classical and quantum resources. The second alternative is QKD, which regroups a wide range of protocols harnessing quantum mechanics to provide information-theoretic security on the shared key. As opposed to classical cryptographic algorithms, the security of QKD protocols is derived without any assumption on the computing power of the adversaries and therefore constitute future-proof key distribution protocols.

Focus on quantum key distribution.

The first conceptualisations of QKD, such as BB84, relied on single photons as the fundamental communication units. A photon is an elementary particle that is a quantum of the electromagnetic field and as such exhibits fundamental quantum properties enabling QKD. The information can be typically encoded in the polarisation or time-of-arrival of the photon. The main component of the detection apparatus in this case is the single-photon detector (SPD), which produces a "click" when one or several photons are successfully converted into a current. These protocols are referred to as "Discrete-Variable" (DV) QKD because of the discrete set of measurement results.

Later, it was also shown that QKD could be performed by encoding the information on the quadratures of weak coherent states [10]. This is particularly interesting because this is typically how information is transmitted in the field of classical telecommunications, therefore the hardware necessary to control and measure the quadratures of the electromagnetic field is well understood and readily available. These protocols are called "Continuous-Variable" (CV) QKD because of the continuous range of values that can be taken by the quadratures of the light.

The strong security guarantees of QKD are very exciting therefore the technology has received increasing sources of funding and has been experimentally deployed in many metropolitan fiber-networks [11, 12, 13, 14, 15]. However many challenges remain to be overcome before large scale implementation of QKD is possible. The main challenges are the point-to-point distance over which a secret key can be shared –since quantum states cannot be amplified– and the overall deployment costs of the technology.

Focusing on the latter, the by-far dominant cost of fiber-based communications is the deployment of the fiber-network infrastructure. Therefore if QKD could be deployed over the existing infrastructure used for classical communications, this would drastically cut the implementation costs and constitute a considerable step towards large-scale deployment. For this to be possible, the coexistence of the quantum states and the classical signal must be carefully orchestrated or else the fine measurement process required to detect quantum states will suffer from perturbations due to the classical signal, which will in turn jeopardize the ability of the QKD protocol to yield a secret key. Between DV- and CV-QKD, the latter is arguably better suited for this task because the coherent detection process used to measure the quadratures is spectrally selective, hence coherent receivers are less sensitive to Raman noise photons than SPDs. This constitutes an important practical advantage since Raman-induced noise is the dominant source of noise for QKD in wavelength multiplexed classical and quantum communication schemes[16].

Contributions and outline of the thesis.

In this thesis we investigated the question of the coexistence of CV-QKD with classical channels. Our approach was to study in what ways the coexistence could be beneficial for the CV-QKD protocol, rather than only detrimental because of the additional noise induced by the classical channels. Our work is divided in two projects.

Our first project is an experimental demonstration of a CV-QKD implementation where the phase and frequency recovery is performed on a classical channel which is multiplexed in polarisation and digitally frequency shifted relative to the quantum states. While this problem is traditionally addressed using pilot tones [17], our work shows that when designing hybrid quantum and classical communication systems, we can relax the need for pilot tones and perform the carrier recovery directly on a classical channel. We display positive key rates with two discrete modulation formats, one with 4 different quantum states, and one with 64 quantum states and a Gaussian-like probability distribution. In the asymptotic regime, our results are compatible with positive secret key rate over 40 km with reliable classical communication for the classical channel. Hence our work takes one step forward in the direction of hybrid communication systems.

In our second project we investigate how the noise generated by the classical channels can be harnessed to provide an interesting new kind of physical layer security, called *covertness*, to a CV-QKD protocol. The goal of covert communications is for the transmission between the legitimate parties to be indistinguishable from background noise for the adversary. This is achieved by reducing the power of the state transmitted over the channel below some threshold which scales as the inverse of the square-root of the total number of quantum states sent over the channel, due to the so-called "square-root law". We argue that covert CV-QKD is essentially impractical because of the square-root law and we propose to make some additional assumptions, which can be verified in a practical setting, in order to relax the square-root law and enable practical covert CV-QKD.

The rest of this manuscript is organised as follows.

Part I : From quantum theory to quantum key distribution

The objective of this first part is to define and understand CV-QKD, but also to position it with respect to the more general context of quantum-safe cryptography.

Chapter 1 : Quantum theory

In this chapter we give the formalism of quantum mechanics which will be the main language used to describe quantum systems in the rest of this work. We also give some important properties of quantum systems such as the no-cloning theorem and the uncertainty principle which are the foundations of quantum key distribution and therefore particularly relevant in this work. Then we will revisit the quantification of the electromagnetic field in order to derive the ladder operators which will then be used to define the quadrature operators. We continue by defining Gaussian states and Gaussian transformations from their covariance matrix. These play a central role in quantum information theory analogously to the Gaussian distribution in classical information theory. Finally, we describe the quantum mechanical effect of homodyne and heterodyne measurement on the covariance matrix of the quantum state

Chapter 2 : Classical and quantum information theory

We move on in the second chapter to study the most relevant quantity of communication systems: information. We define the notions of entropy and mutual information and give their quantum mechanical equivalent. Finally, we give Holevo's bound on the accessible classical information in a quantum system which will play a key role in the security proofs of CV-QKD.

Chapter 3 : Cryptography

This third chapter is meant to give some insight into the world of cryptography. We distinguish the computational and information-theoretic security models and then give an overview of important cryptographic primitives which are hashing functions, symmetric encryption throught AES and public-key encryption through RSA. Then we discuss in more detail the *quantum apocalypse* discussed above. We finish the chapter by detailing the outline of a generic QKD protocol, which we illustrate with BB84, and briefly review the different types of QKD protocols.

Chapter 4 : Quantum Key Distribution with Continuous-Variables

In the last chapter of the first part of this work, we focus on CV-QKD. We begin by giving some example of protocols, and give the expression of the secret key rate through the well-known Devetak-Winter formula. Then we show how to compute the key rate in several cases : when Alice employs a Gaussian modulation on the quadratures, when Alice employs a discrete modulation, when the receiver noise is considered "trusted" and in the finite-size regime. We finish this chapter with a comparison of DV- and CV-QKD solutions in term of key rate, achievable distance and potential for coexistence with classical channels.

Part II : Convergence of classical and quantum coherent communications.

In the second part of this manuscript we present the contributions that have been achieved during the course of this thesis.

Chapter 5 : Quantum and classical coherent communications

We begin with a general chapter on coherent communications which is necessary to understand the experimental implementations of coherent communications. We successively address the signal generation at Alice, the signal distortions during transmission, and signal measurement at Bob in coherent communications. Then we discuss how the sampled signal is processed to retrieve the information encoded in the field quadratures. Finally, we discuss some important challenges of quantum coherent communications and position the rest of our work.

Chapter 6 : Joint Classical and quantum coherent communications

We present here our experimental demonstration of CV-QKD and classical communications performed jointly where the quantum carrier recovery is performed on the classical channel. We begin by describing our experimental setup. Then we discuss the calibration in shot-noise units. We show our receiver is operated in the linear regime, where the shot-noise scales linearly with the LO power, and we discuss our precision in the shot-noise estimation. The following section focuses on the digital signal processing routine we used. In the final section, we discuss how we optimised our experimental parameters and give our results before discussing improvement perspectives and concluding this part of our work.

Chapter 7 : Covert quantum key distribution

Our second project is described in this chapter. We begin by giving a general introduction to covert communications and formally define covertness. Then we move on to deriving a threshold power for the quantum channel under which the quantum communication is covert. We show that without additional assumptions this bound makes covert CV-QKD essentially impractical because a negligible amount of covert and secret bits can be shared using the protocol because of the square-root law mentioned earlier. We move on to examining how a shared secret resource between Alice and Bob can be used to improve the performance on the protocol through a process we call *block-coherent encoding* but show that covert CV-QKD is still limited because of the square-root law. Then we derive two practical models in which we can relax the square-root scaling of the signal power which enables practical covert CV-QKD. We conclude this chapter with a discussion on covert CV-QKD.

Perspectives

We conclude this work in this final part. We attempt to give a general view of QKD in its current state, the challenges facing the technology and the contributions we made to the field.

Part I

From quantum theory to quantum key distribution

Chapter 1

Quantum theory

Contents

Giving a precise description of quantum systems can be challenging at first, since interesting phenomena appear in this regime which seem counter-intuitive by classical physics standards, that is based on what we can *see*. For example, the fact that the measurement result of a quantum particle is described by some set of probabilities is particularly odd compared to our macroscopic world where objects are well defined. Also quantum systems can be *entangled*, which means that by measuring one particle we can modify the measurement outcome probabilities of another. This was puzzling scientists at first since it goes against the principle of locality which states that an object is influenced only by its immediate surroundings. Thankfully, we have developed a mathematical formalism which permits describing such systems and exhibiting their unique properties. In this section we cover this formalism which will be needed to describe the QKD quantum states and their evolution during the QKD protocol.

1.1 Formalism of quantum mechanics

Let us begin with the mathematical formalism of quantum mechanics which we give below. These results constitute a brief overview and the interested reader is referred to [18] for a more thorough description.

1.1.1 The postulates of quantum mechanics

Quantum mechanics are built on a set of 6 postulates which enable an efficient description of quantum systems and their unique properties.

Postulate 1 (State space)**.** *The state of an isolated physical system at time t is represented by a state vector $|\psi\rangle$ belonging to a Hilbert space $\mathcal{H}$ called the state space.*

Basically the first postulate lets us write quantum states as complex vectors –sometimes infinite dimensional– which are called *kets* in the Dirac formalism. It is convenient to normalise the state vectors since we will see later that they are closely linked to probability distributions. A consequence of the first postulate is that all vectors of the Hilbert space are quantum states. Therefore if $|\psi\rangle$ and $|\phi\rangle$ are two possible states of the state space $\mathcal{H}$, then $|\varphi\rangle = \alpha\,|\psi\rangle + \beta\,|\phi\rangle$, with $|\alpha|^2 + |\beta|^2 = 1$ for normalisation, is also a possible state. This is known as the *superposition principle* because $|\varphi\rangle$ is is a superposition of states $|\psi\rangle$ and $|\phi\rangle$. The superposition principle is the fundamental resource behind the quantum advantage in computation.

All states that can be written in ket notation, such as $|\varphi\rangle$, $|\psi\rangle$ and $|\phi\rangle$, are called pure states and are part of the possible physical states of the system. Now suppose we need to describe a system that is a statistical mix –not a superposition– of several states. For example suppose we create and send quantum state $|\psi\rangle$ over a quantum channel with probability half, and state $|\phi\rangle$ the rest of the time. The average state sent on the channel is not a superposition of $|\psi\rangle$ and $|\phi\rangle$ and cannot be written as $|\varphi\rangle$. To descibe this statistical mix, we have to generalise the notion of state vector using the state density matrix. Any pure quantum system defined on $\mathcal{H}$ can also be defined by a density matrix $\hat{\rho}$ as:

$$\hat{\rho}^{\text{pure}} = |\psi\rangle\,\langle\psi|\,. \tag{1.1}$$

If we need to describe a statistical mix of n states $\{|\psi_k\rangle\}_{k=1}^n$ with the corresponding probabilities $\{p_k\}_{k=1}^n$, the quantum state is called a mixed state and is described by

$$\hat{\rho}^{\text{mixed}} = \sum_{k=1}^{n} p_k\,|\psi_k\rangle\,\langle\psi_k|\,. \tag{1.2}$$

The density matrix obeys the following properties :

$$\text{Tr}(\hat{\rho}) = 1, \tag{1.3}$$

$$\text{Tr}(\hat{\rho}^2) \leq 1, \tag{1.4}$$

with equality in the second line if and only if $\hat{\rho}$ is pure.

The next series of postulates define the formalism of measuring a quantum state.

Postulate 2 (Observable)**.** *Every measurable physical quantity $\mathcal{A}$ is described by a Hermitian operator $\hat{A}$ acting in the state space $\mathcal{H}$. The operator $\hat{A}$ is called an observable and its eigenvalues form a basis for the state space $\mathcal{H}$.*

The second postulate provides the way to address the physical quantities in a quantum system. Valid quantities for $\mathcal{A}$ are for example the position, momentum or energy of a quantum state.

Postulate 3 (Quantization)**.** *The only possible outcomes of the measurement of $\mathcal{A}$ are the eigenvalues of the operator $\hat{A}$.*

According to postulate 3 the outcomes of a measurement result are necessary discrete, which introduces the notion of quantization. This is for example the case for the energy of a quantum system, for which only discrete energy levels are possible.

Postulate 4 (Probability of a measurement outcome)**.** *When the physical quantity $\mathcal{A}$ is measured, the probability $\mathbb{P}(\lambda_i)$ of obtaining eigenvalue λ_i is given by the norm of the projection of the state vector $|\psi\rangle$ onto the corresponding eigenvector $|\lambda_i\rangle$*

$$\mathbb{P}(\lambda_i) = |\langle\lambda_i|\psi\rangle|^2. \tag{1.5}$$

If the spectrum is degenerate, then $\mathbb{P}(\lambda_i)$ is given by the norm of the projection of $|\psi\rangle$ onto the eigensubspace P_{λ_i} associated with λ_i

$$\mathbb{P}(\lambda_i) = \sum_{\lambda_i^k \in P_{\lambda_i}} |\langle\lambda_i^k|\psi\rangle|^2, \tag{1.6}$$

where the λ_i^k for an orthonormal basis of P_{λ_i}.

Thanks to the formalism of postulate 4, we can express the mean value of the observable $\hat{A}$ which is noted $\langle\hat{A}\rangle$ and is given by

$$\langle\hat{A}\rangle = \langle\psi|\hat{A}|\psi\rangle\,. \tag{1.7}$$

Also the variance of $\hat{A}$ can be expressed as :

$$(\Delta\hat{A})^2 = \langle\psi|\hat{A}^2|\psi\rangle - \langle\psi|\hat{A}|\psi\rangle^2\,. \tag{1.8}$$

Similarly, the measurement outcome probabilities can be computed from the density matrix representation. Let $\hat{\rho}$ be the density matrix of the quantum state. Then we have :

$$\mathbb{P}(\lambda_i) = \mathrm{Tr}(|\lambda_i\rangle\langle\lambda_i|\,\hat{\rho}) \tag{1.9}$$

and the mean value of operator $\hat{A}$ is given by :

$$\langle\hat{A}\rangle = \mathrm{Tr}(\hat{A}\hat{\rho}). \tag{1.10}$$

Postulate 5 (Effect of measurement)**.** *If the measurement of $\mathcal{A}$ on state vector $|\psi\rangle$ gives result λ_i, then the state of the system after the measurement is the normalized projection of $|\psi\rangle$ on eigensubspace P_{λ_i} associated with eigenvalue λ_i*

$$|\psi\rangle \xrightarrow[\lambda_i]{Measurement} \frac{\sum_{\lambda_i^k \in P_{\lambda_i}} \langle\lambda_i^k|\psi\rangle\,|\psi\rangle}{\sqrt{\mathbb{P}(\lambda_i)}}. \tag{1.11}$$

Postulate 5 explains that measurements affect the quantum state by projecting the state on the eigensubspace corresponding to the measurement result. Therefore measurements in quantum mechanics are projective, and modify the state.

Postulate 6 (Time evolution of a system)**.** *The time evolution of state vector $|\psi(t)\rangle$ obeys the Schrödinger equation*

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = H(t)\,|\psi(t)\rangle\,, \tag{1.12}$$

where H(t) is the observable associated with the total energy of the system and is called the Hamiltonian of the system.

1.1.2 Description of composed systems

Quantum systems can be more complex than just a quantum particle in a Hilbert space. Often, we will need to describe quantum systems shared by several parties, with each party holding a quantum state that is part of the full quantum system. Such system are described using the tensor product representation. Let $\{|\psi_i\rangle\}_{i=1}^n$ be n quantum states represented in their respective state space $\{\mathcal{H}_i\}_{i=1}^n$. The state space describing the quantum state composed of the n particles is given by the tensor product of the individual state spaces $\mathcal{H} = \otimes_{i=1}^n \mathcal{H}_i$.

Notice that the state space defined by $\text{Sep}_{\mathcal{H}} = \{(|\psi_1\rangle, ..., |\psi_n\rangle) \in \mathcal{H}_1 \times ... \times \mathcal{H}_n\}$ is of dimension $d_{sep} = \dim(\mathcal{H}_1) + ... + \dim(\mathcal{H}_n)$ while the dimension of the tensor product space $\mathcal{H}$ is $d = \Pi_{i=1}^n \dim(\mathcal{H}_i)$. Therefore it is impossible to describe composed systems using only quantum states in $\text{Sep}_{\mathcal{H}}$. Systems that can be described as such are called *separable*. On the other hands states in $\mathcal{H} \backslash \text{Sep}_{\mathcal{H}}$ cannot be defined by describing the individual states of the n particles but instead must be defined as a whole. Such systems are called *entangled*.

Example of entanglement. A maximally entangled two mode state is called a Bell state and is given by $|\Phi^+\rangle_{AB} = \frac{|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B}{\sqrt{2}}$ where states $|0\rangle$ and $|1\rangle$ represent for example the polarisation state of a photon. Now consider the polarisation of subsystem A is measured. The result will give either $|0_A\rangle$ or $|1_A\rangle$ each with probability half. Suppose the result is $|0_A\rangle$, then according to postulate 5 the bipartite state is projected onto the subspace $|0_A\rangle\langle 0_A|$ and becomes :

$$|\psi_{AB}\rangle = \frac{(\langle 0_A| \langle 0_B|) |\Phi^+\rangle}{1/\sqrt{2}} |0_A\rangle |0_B\rangle + \frac{(\langle 0_A| \langle 1_B|) |\Phi^+\rangle}{1/\sqrt{2}} |0_A\rangle |1_B\rangle \tag{1.13}$$

$$|\psi_{AB}\rangle = |0_A\rangle |0_B\rangle \tag{1.14}$$

Therefore particle B is projected onto polarisation state $|0\rangle_B$ as a result of the polarisation measurement of particle A. The particles A and B are *entangled*. Entanglement is a fundamental quantum resource which can be harnessed for quantum communications, and it is at the core of the security proofs of quantum key distribution protocols which we will discuss further in this manuscript.

Description of subsystems of a pure state. Consider a bipartite pure state $|\psi\rangle_{AB} = \sum_{i,j} \mu_{i,j} |a_i\rangle |b\rangle_j$ described over the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. The density matrix of the composed system is given by :

$$\hat{\rho}_{AB} = \sum_{i,j,k,l} \mu_{i,j} \mu_{k,l}^* |a_i\rangle \langle a_k| \otimes |b_j\rangle \langle b_l| . \tag{1.15}$$

Then we can give a description of the subsystem A (or B) by tracing out the other in the density matrix expression above. The resulting state will be the mixed state given by

$$\hat{\rho}_A = \text{Tr}_B(\hat{\rho}_{AB}) \tag{1.16}$$

$$= \text{Tr}_B\left(\sum_{i,j,k,l} \mu_{i,j} \mu_{k,l}^* |a_i\rangle \langle a_k| \otimes |b_j\rangle \langle b_l| \right) \tag{1.17}$$

$$= \sum_{i,j,k,l} \mu_{i,j} \mu_{k,l}^* |a_i\rangle \langle a_k| \quad \text{if} \quad \langle b_l | b_j \rangle = \delta_{i,j} \tag{1.18}$$

Purification. An important result of the formalism of quantum mechanics states that any mixed state can be expressed as a pure state in a larger Hilbert space. Let us formalise this result here. Consider for example $\hat{\rho}_A$ the density matrix of a pure state described in Hilbert space $\mathcal{H}_A$. Let $|\psi\rangle$ be a pure state in Hilbert space $\mathcal{H} \otimes \mathcal{H}_B$.

Definition 1 (Purification)**.** We say that $|\psi\rangle$ purifies $\hat{\rho}_A$ if

$$\hat{\rho}_A = \mathrm{Tr}_B\big(|\psi\rangle\langle\psi|\big). \tag{1.19}$$

Theorem 1. *For all mixed state described by density matrix $\hat{\rho}_A$ in some Hilbert space $\mathcal{H}_A$, there exists some Hilbert space $\mathcal{H}_B$ such that $\dim \mathcal{H}_B \geq \dim \mathcal{H}_A$ and such that there exists a pure state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ which purifies $\hat{\rho}_A$*

The notion of purification is particularly useful in QKD since we can express the bipartite mixed states exchanged by Alice and Bob as a pure tripartite state. The third party in this case is the eavesdropper, and purification results make it possible to compute the information leaked to the third party. However this is the object of another chapter and we leave this for later.

1.1.3 Quantum no-cloning theorem

The mathematical Hilbert space formalism of quantum mechanics comes with the crucial notion of *orthogonality*. As opposed to classical states, quantum states can be non orthogonal. When this is the case it is impossible to perfectly discriminate the states since they have some overlap. A direct consequence is the *no cloning theorem* :

Theorem 2 (No cloning theorem)**.** *It is impossible to create an independant and identical copy of an arbitrary unknown quantum state. Let $\mathcal{H}$ be a Hilbert space. The no cloning theorem translates as the following. There is no unitary U acting on $\mathcal{H} \otimes \mathcal{H}$ such that for all $|\psi\rangle \in \mathcal{H}$ and for any ancilla state $|0\rangle \in \mathcal{H}$:*

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle \tag{1.20}$$

Proof. We reason by contradiction. Suppose such a unitary exists. Then for any two states $(|\psi\rangle, |\phi\rangle) \in \mathcal{H}^2$ we have :

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle \tag{1.21}$$
$$U|\phi\rangle|0\rangle = |\phi\rangle|\phi\rangle \tag{1.22}$$

Then we can write :

$$\langle 0|\langle\psi|U^\dagger U|\phi\rangle|0\rangle = \langle\psi|\langle\psi|\phi\rangle|\phi\rangle \tag{1.23}$$
$$\text{thus } \langle\psi|\phi\rangle = \langle\psi|\phi\rangle^2 \tag{1.24}$$

Necessarily $\langle\psi|\phi\rangle = 0$ or $\langle\psi|\phi\rangle = 1$. Since the states are normalized, this means that either $|\psi\rangle$ and $|\phi\rangle$ are orthogonal, or we have some $\alpha \in [0, 2\pi]$ such that $|\psi\rangle = e^{i\alpha}|\phi\rangle$. In any case this is in contradiction with the assumption that the states $|\psi\rangle$ and $|\phi\rangle$ are chosen arbitrarily, which concludes the proof. □

The quantum no cloning theorem also play an important part in the security of quantum key distribution systems. As long as the communication quantum states are non-orthogonal, the adversary is prevented from creating replicate states to perform his measurement.

1.1.4 The Heisenberg uncertainty principle

Yet another principle of quantum mechanics is the Heisenberg uncertainty principle. It states that it is impossible to perfectly measure *complementary* physical quantities $\mathcal{A}$ and $\mathcal{B}$ of the same quantum state such as the position and momentum of a particle. The complementarity of two physical quantities is defined mathematically by the commutation relation of their respective observables.

Definition 2. Measurable physical quantities $\mathcal{A}$ and $\mathcal{B}$ are complementary if and only if their observables $\hat{A}$ and $\hat{B}$ do not commute, that is :

$$[\hat{A}, \hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A} \neq 0. \tag{1.25}$$

Follows from definition 2 the mathematical formalism of Heisenberg's uncertainty principle expressed as :

$$\Delta\hat{A} \cdot \Delta\hat{B} \geq \frac{1}{2} \left| \langle [\hat{A}, \hat{B}] \rangle \right|. \tag{1.26}$$

The principle can be interpreted as follows. Let $\hat{A}$ and $\hat{B}$ be two observables such that $[\hat{A}, \hat{B}] = k \neq 0$. Suppose state $|\psi\rangle$ is an eigenstate of $\hat{A}$ and $\hat{B}$ with eigenvalues a and b. Then we would have the two following equalities :

$$[\hat{A}, \hat{B}] |\psi\rangle = k |\psi\rangle , \tag{1.27}$$

$$\text{and} \quad [\hat{A}, \hat{B}] |\psi\rangle = (ab - ba) |\psi\rangle = 0, \tag{1.28}$$

which is impossible. Therefore no quantum state $|\psi\rangle$ can be an eigenstate of both observables $\hat{A}$ and $\hat{B}$. Necessarily $|\psi\rangle$ is a linear combination of eigenstates of either $\hat{A}$ or $\hat{B}$ which implies by postulate 3 that it cannot be exactly determined.

1.2 Quantization of the electromagnetic field

Now that we have given the formalism used to define our quantum systems and given a few key properties stemming from said formalism, we dive into the key components of the quantum theory of light which will be useful for CV-QKD. Here we begin by defining the ladder operators which are then used to define the quadrature operators of the quantum states. For further reading, see for example [19].

1.2.1 The ladder operators

Consider the position and momentum operators, which are linked to the quantum harmonic oscillator Hamiltonian by

$$\hat{H} = \frac{\hat{p}_m^2}{2m} + \frac{1}{2}\omega^2\hat{x}^2, \tag{1.29}$$

where $\hat{p}_m$ and $\hat{x}$ and the momentum and position operators. Since they are conjugate variables, they obey the canonical commutation relation :

$$[\hat{x}, \hat{p}_m] = i\hbar. \tag{1.30}$$

Definition of the ladder operators. In quantum mechanics, the dimensionless creation $\hat{a}^\dagger$ and annihilation $\hat{a}$ operators are conveniently used to express the Hamiltonian. They are also referred to as the *ladder* operators and they are defined as

$$\hat{a} = \frac{1}{\sqrt{2m\hbar\omega}}(m\omega\hat{x} + i\hat{p}_m), \tag{1.31}$$

$$\hat{a}^\dagger = \frac{1}{\sqrt{2m\hbar\omega}}(m\omega\hat{x} - i\hat{p}_m), \tag{1.32}$$

such that the position and momentum operators are :

$$\hat{x} = \sqrt{\frac{\hbar}{2m\omega}}(\hat{a}^\dagger + \hat{a}), \tag{1.33}$$

$$\hat{p}_m = i\sqrt{\frac{m\hbar\omega}{2}}(\hat{a}^\dagger - \hat{a}). \tag{1.34}$$

It follows from equations 1.31 and 1.32 that

$$\hat{a}\hat{a}^\dagger = \frac{1}{2m\hbar\omega}(m^2\omega^2\hat{x}^2 + \hat{p}_m^2 + im\omega(\hat{p}_m\hat{x} - \hat{x}\hat{p}_m)), \tag{1.35}$$

$$= \frac{1}{\hbar\omega}(\hat{H} + \frac{1}{2}\hbar\omega), \tag{1.36}$$

$$\hat{a}^\dagger\hat{a} = \frac{1}{\hbar\omega}(\hat{H} - \frac{1}{2}\hbar\omega). \tag{1.37}$$

Therefore the Hamiltonian can be written as :

$$\hat{H} = \hbar\omega(\hat{a}^\dagger\hat{a} + \frac{1}{2}), \tag{1.38}$$

and the operators $\hat{a}$ and $\hat{a}^\dagger$ obey the commutation relation

$$[\hat{a}, \hat{a}^\dagger] = 1. \tag{1.39}$$

Effect on energy eigenstates. Consider the energy eigenstates of the quantum system, which form an orthonormal basis of the Hilbert space called the *Fock basis*. We denote by $|n\rangle$ the energy eigenstate with eigenvalue E_n. By definition we have $\hat{H}|n\rangle = E_n|n\rangle$ and by multiplying both expressions by $\hat{a}^\dagger$ via the left hand side we obtain

$$\hat{a}^\dagger\hat{H}|n\rangle = E_n\hat{a}^\dagger|n\rangle. \tag{1.40}$$

Using expression 1.38 and commutation relation 1.39 we find that 1.40 becomes

$$\hat{H}\hat{a}^\dagger|n\rangle = (E_n + \hbar\omega)\hat{a}^\dagger|n\rangle. \tag{1.41}$$

Proceeding similarly with the operator $\hat{a}$ we find that

$$\hat{H}\hat{a}|n\rangle = (E_n - \hbar\omega)\hat{a}|n\rangle. \tag{1.42}$$

Therefore $\hat{a}^\dagger|n\rangle$ and $\hat{a}|n\rangle$ are also eigenstates of the Hamiltonian. The operators $\hat{a}^\dagger$ and $\hat{a}$ are called the *creation* and *annihilation* operators because they can be seen as increasing or decreasing the energy level of a quantum state by one energy increment $\hbar\omega$. Note they do not correspond to measurable quantities since they are not Hermitian and therefore do not satisfy the condition to be observables. We use the notation

$$E_{n+1} = E_n + \hbar\omega \tag{1.43}$$

$$E_{n-1} = E_n - \hbar\omega, \tag{1.44}$$

to designate the $n+1$ and $n-1$ energy levels. If we now consider the ground state of the system, noted $|0\rangle$, we have that $\hat{a}|0\rangle$ is also an eigenstate of the Hamiltonian of energy $E_0 - \hbar\omega$. Since there is by definition no state with lower energy than the ground state, necessarily we have

$$\hat{a}\,|0\rangle = 0. \tag{1.45}$$

Then we can find the energy of the ground state by computing $\hat{H}\,|0\rangle = \frac{\hbar\omega}{2}\,|0\rangle = E_0\,|0\rangle$ which gives the energy levels of the system

$$E_0 = \frac{1}{2}\hbar\omega \tag{1.46}$$

$$E_n = (n + \frac{1}{2})\hbar\omega. \tag{1.47}$$

Since $\hat{H}\,|n\rangle = E_n\,|n\rangle$ we can deduce that

$$\hat{a}^\dagger\hat{a}\,|n\rangle = n\,|n\rangle\,. \tag{1.48}$$

We note $\hat{n} = \hat{a}^\dagger\hat{a}$ the *number* operator. The energy eigenstates are also eigenstates or the number operator. Let us denote by $|n+1\rangle$ and $|n-1\rangle$ the eigenstates corresponding to the energy levels $n+1$ and $n-1$. We showed that the ladder operators applied to $|n\rangle$ are proportional to $|n+1\rangle$ and $|n-1\rangle$. Thus there exists complex numbers A_n and C_n such that

$$\hat{a}^\dagger\,|n\rangle = C_n\,|n+1\rangle \tag{1.49}$$

$$\hat{a}\,|n\rangle = A_n\,|n-1\rangle\,. \tag{1.50}$$

We prefer using normalised states therefore we find the values A_n and C_n such that the states $|n\rangle$ are of orthonormal. We have

$$\langle n|\hat{a}\hat{a}^\dagger|n\rangle = |C_n|^2\,\langle n+1|n+1\rangle = |C_n|^2 \tag{1.51}$$

$$\langle n|\hat{a}^\dagger\hat{a}|n\rangle = |A_n|^2\,\langle n-1|n-1\rangle = |A_n|^2. \tag{1.52}$$

Equation 1.48 gives that $A_n = \sqrt{n}$ and using the commutation relation 1.39 we find that $C_n = \sqrt{n+1}$ such that

$$\hat{a}^\dagger\,|n\rangle = \sqrt{n+1}\,|n+1\rangle \tag{1.53}$$

$$\hat{a}\,|n\rangle = \sqrt{n}\,|n-1\rangle\,. \tag{1.54}$$

1.2.2 The quadrature operators

In particular for this work in which we focus on quantum key distribution protocols, the quantization is considered at the level of the photon. Then the number operator $\hat{n}$ has for eigenvalues the mean number of photons of the quantum state. Any optical quantum state $\hat{\rho}$ can be represented in the *Fock* basis, using the density matrix formalism :

$$\hat{\rho} = \sum_{n,m} \hat{\rho}_{n,m}\,|n\rangle\,\langle m|\,. \tag{1.55}$$

The Fock basis is infinite-dimensional which can make it difficult to represent states in this basis. For example coherent states, which we will discuss in the next section, are difficult to represent in the Fock basis because they are superpositions of all the number states. Therefore it is convenient to introduce the *quadrature* operators $\hat{p}$ and $\hat{q}$ to represent the quantum states in phase space. We define them as

$$\hat{p} = \frac{1}{2}(\hat{a}^\dagger + \hat{a}) \tag{1.56}$$

$$\hat{q} = \frac{i}{2}(\hat{a}^\dagger - \hat{a}), \tag{1.57}$$

such as the ladder operators are

$$\hat{a} = \frac{1}{2}(\hat{p} + i\hat{q}) \tag{1.58}$$

$$\hat{a}^\dagger = \frac{1}{2}(\hat{p} - i\hat{q}) \tag{1.59}$$

The quadrature operators are Hermitian since $\hat{p}^\dagger = \hat{p}$ and $\hat{q}^\dagger = \hat{q}$ therefore they satisfy the condition for observable quantities of the quantum system. The commutation relation can be computed as

$$[\hat{p}, \hat{q}] = \frac{i}{2}, \tag{1.60}$$

therefore we can deduce the Heisenberg uncertainty relation on the quadrature operators

$$\Delta\hat{p} \cdot \Delta\hat{q} \geq \frac{1}{4}. \tag{1.61}$$

1.3 Gaussian states

An important category of quantum states is the group of Gaussian states. These have nice properties, especially from an information theory point of view. In addition, they are easy to describe since they are uniquely defined from their first and second moments. We define these states here and discuss their properties.

1.3.1 Wigner's function

The Wigner function is typically used to represent the probability distribution of the quadratures of a quantum state. It is defined in the general case from the density matrix of the quantum state by

$$W(p, q) = \frac{1}{\pi\hbar} \int_{-\infty}^{\infty} e^{-i\frac{qp'}{\hbar}} \langle p + p' | \hat{\rho} | p - p' \rangle \, dp'. \tag{1.62}$$

Since the quadratures are conjugate variables, the Heisenberg uncertainty principle prevents us from precisely defining the joint probability distribution $Pr(p, q)$. However it is possible to define the marginal distributions $Pr(p)$ and $Pr(q)$. The Wigner function is a good probability distribution approximation for quantum states since it gives the marginal probability distributions as :

$$Pr(p_0) = \int_{-\infty}^{\infty} W(p_0, q) dq. \tag{1.63}$$

The Wigner function is called a *quasiprobability* density function because it can take some negative values in small regions for quantum states which have no classical representation.

1.3.2 Gaussian states

Gaussian states are quantum states for which the Wigner function is a Gaussian such that each marginal probability distribution is also Gaussian. The probability distribution of the quadrature operators of a Gaussian state can be written as

$$\hat{p} \sim \mathcal{N}(\mu_p, \sigma_p^2), \tag{1.64}$$

$$\hat{q} \sim \mathcal{N}(\mu_q, \sigma_q^2). \tag{1.65}$$

This definition can be extended to an n mode Gaussian state which is entirely defined by its first and second moments. The first moment of an n mode quantum state is the displacement vector $\vec{d}$ given by the mean values of the quadratures in each mode

$$\vec{d} = (\langle \hat{p}_1 \rangle, \langle \hat{q}_1 \rangle, ..., \langle \hat{p}_n \rangle, \langle \hat{q}_n \rangle). \tag{1.66}$$

The second moment is given by the covariance matrix Γ with the matrix coefficients

$$\Gamma_{i,j} = \frac{1}{2}\{\Delta\hat{c}_i, \Delta\hat{c}_j\}, \tag{1.67}$$

where $\hat{c} = (\hat{x}_1, \hat{p}_1, ..., \hat{x}_n, \hat{p}_n)$ and $\{,\}$ is the anti-commutator defined by $\{\hat{x}, \hat{p}\} = \hat{x}\hat{p} + \hat{p}\hat{x}$. Therefore the covariance matrix is in the form of

$$\Gamma = \begin{pmatrix} (\Delta\hat{p}_1)^2 & \frac{1}{2}\{\Delta\hat{p}_1, \Delta\hat{q}_1\} & ... & \frac{1}{2}\{\Delta\hat{p}_1, \Delta\hat{q}_n\} \\ \frac{1}{2}\{\Delta\hat{q}_1, \Delta\hat{p}_1\} & (\Delta\hat{p}_1)^2 & ... & \frac{1}{2}\{\Delta\hat{q}_1, \Delta\hat{q}_n\} \\ ... & ... & & ... \\ \frac{1}{2}\{\Delta\hat{q}_n, \Delta\hat{p}_1\} & \frac{1}{2}\{\Delta\hat{q}_n, \Delta\hat{p}_2\} & ... & (\Delta\hat{q}_n)^2 \end{pmatrix}, \tag{1.68}$$

and is a real valued symmetric matrix. The covariance matrix will later play a central role when considering the informational quantities in joint quantum systems.

Coherent states. The most important class of Gaussian states for this work are called coherent states. They are the quantum representation of the light emitted by a laser source such as those employed in our continuous-variable quantum key distribution experiment. They are referred to by a complex number α and are defined as the eigenstates of the annihilation operator such that coherent state $|\alpha\rangle$ obeys

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle\,. \tag{1.69}$$

Coherent states can be decomposed over the Fock basis as a superposition of all Fock states with decreasing probability at higher energy levels. In particular, the number of photons in a coherent state follows a Poisson distribution as

$$|\alpha\rangle = e^{\frac{-|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\,. \tag{1.70}$$

We can easily check that the coherent states are unitary *i.e.* $\langle\alpha|\alpha\rangle = 1$ and are also non orthogonal since for all $(\alpha, \beta) \in \mathbb{C}^2$,

$$\langle\alpha|\beta\rangle = e^{-\frac{1}{2}(|\alpha|^2 + |\beta|^2 - 2\alpha\bar{\beta})} \neq 0. \tag{1.71}$$

A consequence of this non-orthogonality is that is it impossible to perfectly discriminate between coherent states, which is fundamental for the security of quantum key distribution. Moving on we give some properties of coherent states. The mean value of the quadrature operators for coherent state $|\alpha\rangle$ is

$$\begin{aligned}\langle\hat{p}\rangle &= \frac{1}{2}\langle\alpha|\hat{a}^\dagger + \hat{a}|\alpha\rangle\,,\\ &= \frac{1}{2}(\langle\alpha|\hat{a}^\dagger|\alpha\rangle + \langle\alpha|\hat{a}|\alpha\rangle),\\ &= \frac{1}{2}(\alpha + \alpha^*),\\ &= \mathrm{Re}(\alpha),\end{aligned} \tag{1.72}$$

and similarly

$$\langle\hat{q}\rangle = \mathrm{Im}(\alpha). \tag{1.73}$$

The quadratures of the coherent state $|\alpha\rangle$ are the real and imaginary part of the complex amplitude, thus coherent states are sometimes defined with respect to their quadratures as $|p + iq\rangle$. The quadrature operators variances are computed as

$$\begin{aligned}(\Delta\hat{p})^2 &= \langle\alpha|\hat{p}^2|\alpha\rangle - \langle\alpha|\hat{p}|\alpha\rangle^2\,,\\ &= \frac{1}{4}\langle\alpha|\hat{a}^{\dagger 2} + \hat{a}^\dagger\hat{a} + \hat{a}\hat{a}^\dagger + \hat{a}^2|\alpha\rangle - \mathrm{Re}(\alpha)^2,\\ &= \frac{1}{4}((\alpha^*)^2 + |\alpha^2| + |\alpha|^2 + 1 + \alpha^2) - \mathrm{Re}(\alpha)^2,\\ &= \frac{1}{4}(4\,\mathrm{Re}(\alpha) + 1) - \mathrm{Re}(\alpha),\\ &= \frac{1}{4},\end{aligned} \tag{1.74}$$

and proceeding similarly on the $\hat{q}$ quadrature gives

$$(\Delta\hat{q})^2 = \frac{1}{4}. \tag{1.75}$$

Therefore the coherent states minimise the Heisenberg uncertainty relation in equation 1.61. Finally the number operator applied to $|\alpha\rangle$ gives

$$\langle\hat{n}\rangle = \langle\alpha|\hat{a}^\dagger\hat{a}|\alpha\rangle \tag{1.76}$$

$$= |\alpha|^2 \tag{1.77}$$

We say that coherent state $|\alpha\rangle$ has mean photon number $|\alpha|^2$.

Two-mode squeezed Gaussian states. Two-mode Gaussian states are of particular interest for the security proofs of quantum key distribution. In this picture one mode is measured by Alice and the other is sent through the quantum channel to Bob for him to measure. Among two mode Gaussian states, an important class of states are the *two-mode squeezed states* for which the quadratures in each mode are perfectly correlated. The covariance matrix of two-mode squeezed states is of the form

$$\Gamma_{\mathrm{TMSV}} = \begin{pmatrix}\cosh 2r\mathbb{1}_2 & \sinh 2r\sigma_z\\ \sinh 2r\sigma_z & \cosh 2r\mathbb{1}_2\end{pmatrix}, \tag{1.78}$$

where we have

$$\sigma_z = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}. \tag{1.79}$$

A two-mode squeezed state is a pure state which is the continuous-variable counterpart to the maximally entangled Bell state in the discrete-variable picture. Therefore these states are called *EPR* states. They are represented in the Fock basis as

$$|\text{TMSV}\rangle = \frac{1}{\cosh r} \sum_{n=0}^{\infty} \tanh^n r \, |n, n\rangle \,, \tag{1.80}$$

1.3.3 Gaussian transformations

The set of Gaussian transformations is the set of unitary transformations which transform a Gaussian state into another Gaussian state. They will often be the transformations that affect the quantum states transitioning over the quantum channel during the QKD protocol.

Symplectic transformations. An important subset of Gaussian transformations called the symplectic transformations group. It is the set of transformations that are linear in the creation and annihilation operators and preserves their commutation relations. For an n mode Gaussian state, the symplectic transformations are defined by a $2n \times 2n$ symplectic matrix S such that :

$$S\Omega S^T = \Omega, \text{ where } \Omega = \bigoplus_{i=1}^{n} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \tag{1.81}$$

where the direct sum is defined on matrices A and B by

$$A \bigoplus B = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}. \tag{1.82}$$

A symplectic transformation on a Gaussian state is entirely defined by its effect on the first and second moments as

$$\vec{d}_{out} = S\vec{d}_{in} \tag{1.83}$$

$$\Gamma_{out} = S\Gamma_{in}S^T. \tag{1.84}$$

In particular for continuous-variable quantum key distribution we will consider Gaussian states with zero mean. Then the first moment is zero and the full description of the state is given by its covariance matrix.

Theorem 3 (Williamson's theorem)**.** *Every positive-definite real matrix of even dimension can be put in diagonal form by a symplectic transformation. In particular this can be applied to an n mode Gaussian state covariance matrix* Γ *where for some symplectic matrix S, the following holds*

$$\Gamma^{\oplus} = S\Gamma S^T, \text{ with } \Gamma^{\oplus} = \bigoplus_{i=1}^{n} \begin{pmatrix} \nu_i & 0 \\ 0 & \nu_i \end{pmatrix}. \tag{1.85}$$

The n coefficients ν_i *are called the symplectic eigenvalues of* Γ *and are the eigenvalues of the matrix* $-\Omega\Gamma\Omega\Gamma$

Williamson's theorem is a powerful tool to analyse Gaussian states and plays a central part in quantum information theory on with these states.

Examples of symplectic transformations We give here some of the most common symplectic transformations on optical modes which we will use in further analyses.

Phase rotation : a phase rotation by an angle θ of a single mode state is described by the symplectic matrix R_θ given by

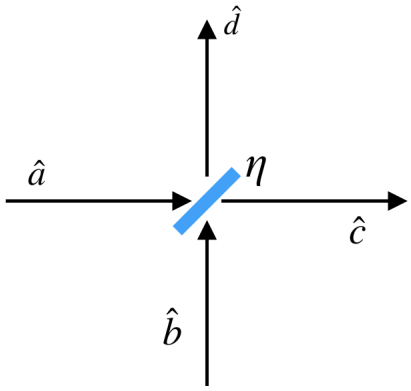


Figure 1.1: Representation of the beamsplitter with two input spatial modes $\hat{a}$ and $\hat{b}$ and two output spatial modes $\hat{c}$ and $\hat{d}$

$$R_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \tag{1.86}$$

Beamsplitter : the beamsplitter with transmissivity η is described on the creation and annihilation operators of two input modes $(\hat{a}, \hat{b})$ and two output modes $\hat{c}, \hat{d}$ such that

$$\hat{c} = \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{b}, \tag{1.87}$$
$$\hat{d} = -\sqrt{1-\eta}\hat{a} + \sqrt{\eta}\hat{b}. \tag{1.88}$$

Then the relation between the four input quadratures and the four output quadratures is

$$\begin{pmatrix} \hat{p}_c \\ \hat{q}_c \\ \hat{p}_d \\ \hat{q}_d \end{pmatrix} = \begin{pmatrix} \sqrt{\eta} & 0 & \sqrt{1-\eta} & 0 \\ 0 & \sqrt{\eta} & 0 & \sqrt{1-\eta} \\ -\sqrt{1-\eta} & 0 & \sqrt{\eta} & 0 \\ 0 & -\sqrt{1-\eta} & 0 & \sqrt{\eta} \end{pmatrix} \begin{pmatrix} \hat{p}_a \\ \hat{q}_a \\ \hat{p}_b \\ \hat{q}_b \end{pmatrix} \tag{1.89}$$

We refer to the matrix representation of the beamsplitter of transmittance η applied to modes A and B as $B_{AB}(\eta)$. The covariance matrix of a two mode Gaussian state after the beamsplitter is

$$\Gamma_{out} = B_{AB}(\eta)\Gamma_{in}B_{AB}^T(\eta) \tag{1.90}$$

The beamsplitter is very convenient to model channel losses as a unitary process in quantum key distribution protocols. The first input mode $\hat{a}$ is the signal mode at Alice while $\hat{b}$ is taken as the vacuum state of the environment. The output mode $\hat{c}$ is the signal mode at Bob's and mode $\hat{d}$ is the environment mode after transmission. We will discuss this more in section 4.3 when computing the Holevo information leaked to the environment during the quantum key distribution protocol.

1.4 Measurement of the quantum states

In a continuous-variable quantum key distribution protocol the information is encoded on the quadratures of coherent states. The quadrature operators are observables, meaning they correspond to a physical quantity we can estimate. In particular for CV-QKD, we will need to express the post-measurement state shared between Alice and Bob. Hence we develop here the formalism of the

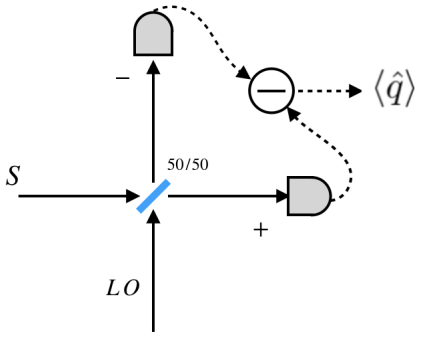


Figure 1.2: Homodyne detection scheme. The signal mode is mixed with a strong laser called the Local Oscillator on a 50/50 beamsplitter. The intensity on both outputs of the beamsplitter is measured and subtracted to constitute the homodyne measurement.

quadrature measurement process. This is called *coherent detection* since it involves mixing the signal state with a strong reference signal called *local oscillator* (LO) on a balanced beamsplitter. The measurement result then depends on the relative phase between the signal and LO. Coherent detection can be divided into homodyne detection and heterodyne detection depending on whether a single or both quadratures are measured. Note that these terms used by the QKD community have a different meaning for the telecom industry, so we make clear that the terms used here are taken in the sense of the QKD community.

1.4.1 Homodyne detection

Homodyne detection permits the measurement of one quadrature of the light, as opposed to heterodyne detection for which both quadratures are measured.

Quadrature measurement. The homodyne detection scheme is represented in the figure 1.2. The signal mode, denoted by S, is mixed with the LO on a 50/50 beamsplitter. Two detectors placed at the $+$ and $-$ outputs of the beamsplitter produce photocurrents I^+ and I^- proportional to the mean photon number in the corresponding mode. The quadrature measurement is given by subtracting the I^+ and I^- currents. According to the beamsplitter model we can write the photon number operators in each mode as

$$\hat{n}_+ = \hat{a}_+^\dagger \hat{a}_+ = \frac{1}{2}(\hat{a}_S^\dagger + \hat{a}_{LO}^\dagger)(\hat{a}_S + \hat{a}_{LO}), \tag{1.91}$$

$$\hat{n}_- = \hat{a}_-^\dagger \hat{a}_- = \frac{1}{2}(-\hat{a}_S^\dagger + \hat{a}_{LO}^\dagger)(-\hat{a}_S + \hat{a}_{LO}). \tag{1.92}$$

The operator for the difference in photocurrents $\hat{I}_\Delta$ is proportional to

$$\begin{aligned}\hat{I}_\Delta &\propto \hat{n}_+ - \hat{n}_- \\ &\propto \hat{a}_S^\dagger \hat{a}_{LO} + \hat{a}_{LO}^\dagger \hat{a}_S,\end{aligned} \tag{1.93}$$

where the proportionality factor depends on the characteristics of the photodectectors. Since the local oscillator is a classical field with energy levels much larger than one quantum unit, hence we can assume that applying the creation and annihilation operators does not change the state. Therefore we can use the classical field assumption and replace $\hat{a}_{LO}$ and $\hat{a}_{LO}^\dagger$ by the classical field amplitude

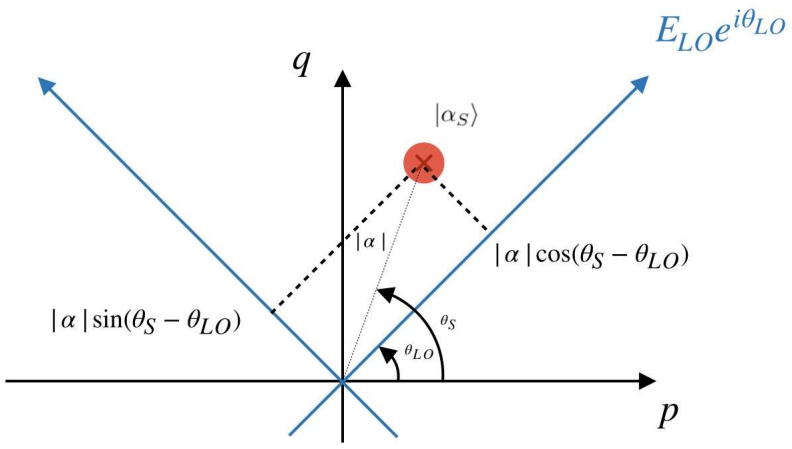


Figure 1.3: The homodyne detection amounts to computing the amplitude of the projection of the quantum state $|\alpha_S\rangle$ on the vector defined by the local oscillator amplitude and phase.

$E_{LO}e^{\pm i\theta_{LO}}$ with θ_{LO} the phase of the local oscillator. Then the mean value of operator $\hat{I}_\Delta$ when the signal state is coherent state $|\alpha_S\rangle = ||\alpha|e^{i\theta_S}\rangle$ is

$$\begin{aligned}\langle \hat{I}_\Delta \rangle &\propto \langle \alpha_S | \hat{a}_S^\dagger \hat{a}_{LO} + \hat{a}_{LO}^\dagger \hat{a}_S | \alpha_S \rangle \\ &\propto E_{LO}(\alpha_S^* e^{i\theta_{LO}} + \alpha_S e^{-i\theta_{LO}}) \\ &\propto 2E_{LO}\,\mathrm{Re}(\alpha_S e^{-i\theta_{LO}}) \\ &\propto 2E_{LO}|\alpha|\cos(\theta_S - \theta_{LO}),\end{aligned} \tag{1.94}$$

which is the quadrature of the coherent state $|\alpha_S\rangle$ in phase with the local oscillator. By shifting the local oscillator phase by $\pi/2$ we have that

$$\hat{I}_\Delta^{\pi/2} \propto 2E_{LO}|\alpha|\sin(\theta_S - \theta_{LO}), \tag{1.95}$$

which is the quadrature of $|\alpha_S\rangle$ in quadrature with the local oscillator. Therefore by controlling the phase of the local oscillator we can chose to measure an arbitrary quadrature of the signal. Equivalently homodyne detection can be seen as a projection of the signal on the quadrature of the local oscillator as is depicted in figure 1.3

Shot-noise. Consider the variance of the quadrature measurement. It is given by

$$(\Delta \hat{I}_\Delta)^2 = \langle \hat{I}_\Delta^2 \rangle - \langle \hat{I}_\Delta \rangle^2, \tag{1.96}$$

where the first term is

$$\langle \hat{I}_\Delta^2 \rangle \propto E_{LO}^2 \langle \alpha_S | (\hat{a}_S^\dagger)^2 e^{i2\theta_{LO}} + \hat{a}_S^2 e^{-i2\theta_{LO}} + \hat{a}_S^\dagger \hat{a}_S + \hat{a}_S \hat{a}_S^\dagger | \alpha_S \rangle \tag{1.97}$$

$$\propto E_{LO}^2((\alpha_S^*)^2 e^{i2\theta_{LO}} + (\alpha_S)^2 e^{-i2\theta_{LO}} + 2|\alpha|^2 + 1) \tag{1.98}$$

$$\propto E_{LO}^2\big(2|\alpha|^2(2\cos^2(\theta_S - \theta_{LO}) - 1\big) + 2|\alpha|^2 + 1), \tag{1.99}$$

$$\propto 4E_{LO}^2|\alpha|^2\cos^2(\theta_S - \theta_{LO}) + E_{LO}^2 \tag{1.100}$$

and we have

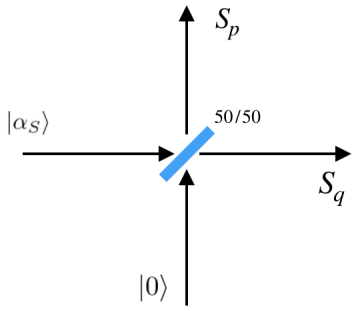


Figure 1.4: For heterodyne detection, the signal is mixed with vacuum when split on a 50/50 beamsplitter

$$\langle \hat{I}_\Delta \rangle^2 \propto 4E_{LO}^2 |\alpha|^2 \cos^2(\theta_S - \theta_{LO}) \tag{1.101}$$

We used the commutation relation of the ladder operators to go from 1.97 to 1.98 and a trigonometric formula of the cosine to go from 1.98 to 1.99. Since the proportionality factors are the same in the expressions of $\langle \hat{I}_\Delta^2 \rangle$ and $\langle \hat{I}_\Delta \rangle^2$ we can write the variance of the observable as

$$(\Delta \hat{I}_\Delta)^2 = N_0 \propto E_{LO}^2. \tag{1.102}$$

The variance of the homodyne measurement comes from the quantum commutation relation between the ladder observables and is proportional the local oscillator intensity. This variance is called the *shot-noise* and is noted N_0 in this manuscript. It plays a significant role in quantum key distribution protocol because it is a normalisation value which is used to calibrate experiments. We will discuss this further in the next chapter.

Heterodyne detection. Both $\hat{p}$ and $\hat{q}$ quadratures of a coherent state $|\alpha_S\rangle$ can be measured by splitting the signal on a 50/50 beamsplitter and performing a double homodyne measurement, one on each branch. In that case it is called a *heterodyne* measurement. The splitting of the signal in mode S in the two modes S_p and S_q induces an additional vacuum contribution because splitting the signal on a beamsplitter mixes the state with vacuum. Thus we have

$$\hat{a}_{Sp,q} = \frac{1}{\sqrt{2}}(\hat{a}_S \pm \hat{v}),$$

where $\hat{v}$ is the annihilation operator of the vacuum. By substituting this expression to $\hat{a}_S$ in the case of homodyne detection, we find that

$$\langle \hat{I}_\Delta \rangle_{\text{het}} = \frac{1}{\sqrt{2}} \langle \hat{I}_\Delta \rangle_{\text{hom}}. \tag{1.103}$$

However the variance of the operator is given by

$$\langle \Delta \hat{I}_\Delta \rangle_{\text{het}}^2 = 2 \langle \Delta \hat{I}_\Delta \rangle_{\text{hom}}^2 \tag{1.104}$$

because there is the additional commutation relation of the vacuum ladder operators in equation 1.97.

1.4.2 Effect of homodyne detection on the covariance matrix

Since Gaussian states are uniquely defined by their first and second moments, it is sufficient to know how transformations affect these moments to define the transformed state. In particular it will be interesting to know the effect of a homodyne or heterodyne measurement of one mode on the covariance matrix of the bipartite state. The interested reader can refer to reference [20] for more details.

Homodyne detection. Consider the two-mode state defined by the covariance matrix

$$\Gamma = \begin{pmatrix} \gamma_A & \gamma_C \\ \gamma_C^T & \gamma_B \end{pmatrix} \tag{1.105}$$

where all matrices γ_i are in $\mathbb{R}^2$ and A, B denote the covariance matrices of the modes A and B while C is the correlations between modes A and B. A homodyne measurement on mode B will destroy the mode and transform mode A depending on the quadrature that is measured. This is described on the covariance matrix $\gamma_{A|B}$ of mode A after measurement by

$$\gamma_{A|B} = \gamma_A - \gamma_C(\Pi_{p,q}\gamma_B\Pi_{q,p})^{-1}\gamma_C^T, \tag{1.106}$$

where $\Pi_{p,q}$ is the projector on the p or q quadrature of mode B and is given by

$$\Pi_p = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ and } \Pi_q = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \tag{1.107}$$

The matrix $\gamma_C(\Pi_{p,q}\gamma_B\Pi_{q,p})^{-1}\gamma_C^T$ is not invertible, but it is diagonal. The notation $^{-1}$ denotes the Moore-Penrose pseudoinverse, which is the corresponding matrix where all non-negative eigenvalues are inverted. The expression in 1.106 simplifies as

$$\gamma_{A|B}^{\text{hom}} = \gamma_A - \frac{1}{(\Delta\hat{p},\hat{q})^2}\gamma_C\Pi_{p,q}\gamma_C^T \tag{1.108}$$

Heterodyne detection. In the case of heterodyne detection the mode B is first split on a balanced beamsplitter which mixes the mode with a vacuum state and is described on the covariance matrix by

$$\Gamma = B_{B,v}(1/2)\begin{pmatrix} \gamma_A & \gamma_C & 0 \\ \gamma_C^T & \gamma_B & 0 \\ 0 & 0 & \mathbb{1}_2 \end{pmatrix} B_{B,v}(1/2)^T, \tag{1.109}$$

where

$$B_{B,v}(1/2) = \begin{pmatrix} \mathbb{1}_2 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}}\mathbb{1}_2 & \frac{1}{\sqrt{2}}\mathbb{1}_2 \\ 0 & -\frac{1}{\sqrt{2}}\mathbb{1}_2 & \frac{1}{\sqrt{2}}\mathbb{1}_2 \end{pmatrix}. \tag{1.110}$$

We compute the covariance matrix after a heterodyne measurement which is a homodyne measurement on the p quadrature of one mode and q measurement of the other. The result yields

$$\gamma_{A|B}^{\text{het}} = \gamma_A - \gamma_c(\gamma_B + \mathbb{1}_2)^{-1}\gamma_C^T. \tag{1.111}$$

This concludes our first chapter. Here we introduced the Hilbert space formalism which permits to describe quantum states and reviewed some important quantum mechanical properties in the no-cloning theorem and the uncertainty principle. We also defined the quadrature operators and the class of coherent states which will be used in the rest of this manuscript. Finally, we described the effect of heterodyne or homodyne detection on the quantum states which will be useful to compute the post-measurement information of the adversary during the QKD protocol. To do this, we first need to define information and give some insights on how to compute it. We do this in the next chapter.

Chapter 2

Classical and quantum information theory

Contents

In this chapter, we define and study the information that is contained in classical variables and in quantum states. We aim to give the tools to define and quantify the information shared between Alice and Bob during a communication protocol –such as QKD– as well as the information leaked to Eve.

2.1 Classical information theory

The founding father of modern information theory is undoubtedly the American engineer Claude Shannon with his article published in 1948 *A Mathematical Theory of Communications*. We will review in this section the core principles of Shannon's information theory.

2.1.1 Introduction to information theory

Definition 3. A random variable X is defined by a set of possible outcomes $\mathcal{X}$ and a set of corresponding probabilities $\{p_X(x)|x \in \mathcal{X}\}$. The outcomes $\mathcal{X}$ can be discrete or continuous and the following relations hold :

$$\forall x \in \mathcal{X}, \quad p_X(x) \in [0,1], \tag{2.1}$$

$$\text{if } \mathcal{X} \text{ is discrete, } \sum_{x\in\mathcal{X}} p_X(x) = 1, \tag{2.2}$$

$$\text{if } \mathcal{X} \text{ is continuous, } \int_{\mathcal{X}} p_X(x)dx = 1. \tag{2.3}$$

When $\mathcal{X}$ is continuous, p_X is called the probability density function. In the rest of this section we will consider $\mathcal{X}$ is discrete. Note the results hold in the continuous case by substituting integrals to the sums.

The mean value of the random variable X, noted $\langle X \rangle$, and its variance noted $\mathrm{var}(X)$, are given by

$$\langle X \rangle = \sum_{x \in \mathcal{X}} p_X(x) \cdot x, \tag{2.4}$$

$$\mathrm{var}(X) = \langle X^2 \rangle - \langle X \rangle^2 . \tag{2.5}$$

A fundamental question answered by Shannon is *how much information* is contained in a realisation of X. Conceptually, if the result of X is certain i.e. $p(X = x) = 1$, then the realisation of X does not provide any information since we can predict with certainty the result. On the contrary a very improbable realisation of X carries a lot of information, since the result was nearly unpredictable. Thus the information provided by the realisation of a random variable depends on the probability of the realisation. With this in mind a natural candidate to quantify information is the $-\log$ function since when the result is certain $-\log(1) = 0$ and this quantity increases as the result becomes less probable.

Definition 4. The information gained by the realisation x of a random variable X is given by :

$$I(x) = -\log_2 p_X(x), \tag{2.6}$$

where the logarithm is taken in base 2 and therefore the information is expressed in bits. The average information provided by the random variable X is called *entropy* and is defined as follows.

Definition 5. The entropy of a random variable X quantifies the average information provided by X. It is noted $H(X)$ and equal to :

$$H(X) = -\sum_{x \in \mathcal{X}} p_X(x) \log_2 p_X(x). \tag{2.7}$$

Notice the entropy does not consider the realisations of the random variable but only their probabilities. The joint entropy of two random variables X and Y quantifies the average information gained by the joint realisations of X and Y. It is computed over the set of outcomes $\mathcal{X}$ and $\mathcal{Y}$ as :

$$H(X,Y) = -\sum_{x \in \mathcal{X}, y \in \mathcal{Y}} p(x,y) \log_2 p(x,y). \tag{2.8}$$

The joint entropy can be generalised to any number of random variables by considering the joint probability distribution of all variables. In general the joint entropy of X and Y is not equal to the sum of the entropies. This is because when they are considered jointly, X and Y can have some information that is redundant. We characterise the remaining uncertainty on variable Y (X) when X (Y) is known with the conditional entropy :

$$H(Y|X) = H(X,Y) - H(X), \tag{2.9}$$

$$= -\sum_{x \in \mathcal{X}, y \in \mathcal{Y}} p(x,y) \log_2 p(y|x), \tag{2.10}$$

$$\text{and } H(X|Y) = H(X,Y) - H(Y), \tag{2.11}$$

$$= -\sum_{x \in \mathcal{X}, y \in \mathcal{Y}} p(x,y) \log_2 p(x|y). \tag{2.12}$$

$$\tag{2.13}$$

The entropy obeys the following relations :

- $H(X) \geq 0$: a random variable X carries information greater or equal to 0, with equality if and only if X is deterministic.
- $H(X) \leq \log_2 |\mathcal{X}|$: the maximum of the entropy of random variable X is $\log_2 |\mathcal{X}|$ with equality if and only if X is uniformly distributed over $\mathcal{X}$ i.e. $\forall x \in \mathcal{X}$, $p_X(x) = \frac{1}{|\mathcal{X}|}$.
- $H(X,Y) \leq H(X) + H(Y)$ with equality if and only if the random variables are independant such that $p(y|x) = p(y)$ and $p(x|y) = p_X(x)$ thus $H(Y|X) = H(Y)$ and $H(X|Y) = H(X)$.

Finally an important measure in the field of communications is the mutual information $I_{X,Y}$ shared between two random variables X and Y.

Definition 6. The mutual information $I_{X,Y}$ between random variables X and Y is a measure of the common information in both variables. It is given by :

$$\begin{aligned} I_{X,Y} &= H(X) + H(Y) - H(X,Y), \\ &= H(X) - H(X|Y), \\ &= H(Y) - H(Y|X). \end{aligned} \tag{2.14}$$

The mutual information plays a central role in communications since it quantifies how many bits X and Y have in common. Therefore if distant parties hold random variable X on one hand and Y on the other, such as when X is a random variable corresponding to the state sent by Alice and Y is be Bob's measurement result, they can extract $I_{X,Y}$ shared bits.

2.1.2 Information theory with Gaussian variables

An important category of random variables for is Gaussian random variables, that is when X and Y follow a Gaussian distribution. Such distributions hold a central role in classical communications since they maximise the amount of information that can be shared. We discuss the information theory quantities in this case here.

A Gaussian random variable $X \sim \mathcal{N}(\mu, \sigma^2)$ is entirely defined on the set of real number $\mathbb{R}$ by its first two moments, that is its mean value μ and variance σ^2. The density probability of the random variable X is given by :

$$p_X(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \cdot e^{-\frac{(x-\mu)^2}{2\sigma^2}}. \tag{2.15}$$

The entropy of a Gaussian random variable $X \sim \mathcal{N}(\mu, \sigma^2)$ is

$$H(X) = -\int_{\mathbb{R}} p_X(x) \log_2 p_X(x) dx, \tag{2.16}$$

$$= \frac{1}{2} \cdot \log_2(2\pi e \sigma^2). \tag{2.17}$$

Note that for a given variance σ^2, the Gaussian distribution is the distribution which maximises the entropy. We can further define the joint probability distribution of Gaussian random variables $X \sim \mathcal{N}(\mu_X, \sigma_X^2)$ and $Y \sim \mathcal{N}(\mu_Y, \sigma_Y^2)$ as :

$$p_{X,Y}(x,y) = \frac{1}{2\pi\sqrt{\sigma_X^2\sigma_Y^2 - \langle XY \rangle^2}} \cdot \exp\left[\frac{x^2\sigma_Y^2 + y^2\sigma_X^2 - 2xy\langle XY \rangle}{2(\sigma_X^2\sigma_Y^2 - \langle XY \rangle^2)}\right]. \tag{2.18}$$

Similarly than for a single Gaussian variable, a joint distribution of Gaussian variables X and Y is entirely defined by its first two moments $\langle XY \rangle$, σ_X^2 and σ_Y^2. Therefore for centered variables, the covariance matrix K_{XY} defined by

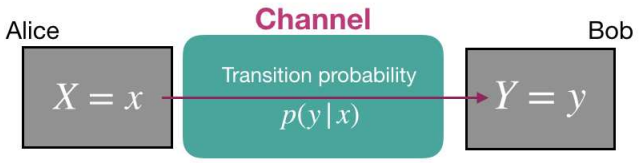


Figure 2.1: Channel representation

$$K_{XY} = \begin{bmatrix} \sigma_X^2 & \langle XY \rangle \\ \langle XY \rangle & \sigma_Y^2 \end{bmatrix}, \tag{2.19}$$

is sufficient to describe the joint distribution of the two Gaussian random variables X and Y. In addition, the entropy and mutual information quantities can be computed from the covariance matrix as we show below. The joint and conditional entropies of X and Y are found by plugging the appropriate density functions in equations 2.8 and 2.9:

$$H(X,Y) = \frac{1}{2}\log_2\big((2\pi e)^2 \cdot \det K_{XY}\big), \tag{2.20}$$

$$H(Y|X) = \frac{1}{2}\log_2\left(2\pi e \cdot \frac{\det K_{XY}}{\sigma_X^2}\right), \tag{2.21}$$

and the mutual information is given by :

$$I_{XY} = \frac{1}{2}\log_2\left(\frac{\sigma_X^2 \sigma_Y^2}{\det K_{XY}}\right). \tag{2.22}$$

2.1.3 Communication over a noisy channel

The information theory quantities we've discussed above are used to describe communication protocols over noisy channels. In such protocols the transmitter, Alice, sends a realisation $x \in \mathcal{X}$ of X to the receiver, Bob, who receives realisation $y \in \mathcal{Y}$ of Y. The goal of the communication is for Alice and Bob to share information -or bits- via the protocol, which is given by the mutual information I_{XY} between the random variables X and Y. The channel model is represented in figure 2.1.

Note the channel is entirely defined by the transition probabilities $p(y|x)$ between random variables X and Y. Then an important subcategory of channels is the *memoryless* channels, for which $p(y|x)$ does not depend on previous events. The maximal amount of bits that can be shared by sending one symbol for memoryless channels is called the *channel capacity* and is given by Shannon's second theorem.

Theorem 4 (Channel coding theorem)**.** *Let a sender, Alice, send realisation x of random variable X over a memoryless channel to the receiver, Bob, who measures realisation y of random variable Y. The maximal amount of bits that can be shared by this scheme is called the channel capacity and is given by :*

$$C = \max_{\{p_X(x)\}} I_{X,Y}. \tag{2.23}$$

Essentially Shannon's channel coding theorem states that there is some distribution of X which enables Alice to send an average of C bits per symbol to Bob without errors. Reversely if Alice tries to send more than C bits per symbol the transmission will contain errors.

The AWGN channel. The main channel model for classical communications and quantum key distribution protocols with continuous variables is the additive white Gaussian noise (AWGN) channel. It is defined by the following relation between variables X and Y :

$$Y = X + Z, \tag{2.24}$$

where $Z \sim \mathcal{N}(0, \sigma_Z^2)$. Z is called noise because it is added to the signal X and contains no information. It is obviously additive and we say it is *white* because it is assumed to be the same for each frequency. The opposite of a white noise is a colored noise which is not equal over all frequencies. The transition probabilities of AWGN channels are Gaussian density probabilities given by

$$p(y|x) = \frac{1}{\sqrt{2\pi\sigma_Z^2}} \cdot e^{-\frac{(y-x)^2}{2\sigma_Z^2}}. \tag{2.25}$$

Theorem 5 (Capacity of the AWGN channel)**.** *The capacity of the AWGN channel is given by :*

$$C_{AWGN} = \frac{1}{2} \cdot \log_2\left(1 + \frac{\sigma_X^2}{\sigma_Z^2}\right), \tag{2.26}$$

where σ_X^2 is the variance of the random variable X.

Proof. We have :

$$\begin{aligned} I_{X,Y} &= H(Y) - H(Y|X), && (2.27)\\ &= H(Y) - H(X + Z|X), && (2.28)\\ &= H(Y) - H(Z), && (2.29)\\ &= H(Y) - \frac{1}{2} \cdot \log_2\left(2\pi e \sigma_Z^2\right). && (2.30) \end{aligned}$$

For a fixed variance σ_Y^2, $H(Y)$ is maximal when Y is Gaussian i.e. when X is Gaussian. In this case we have $\sigma_Y^2 = \sigma_X^2 + \sigma_Z^2$ and $H(Y) = \frac{1}{2} \cdot \log_2\left(2\pi e \sigma_Y^2\right)$. Substituting $H(Y)$ in the mutual information expression above gives the capacity C_{AWGN} which concludes the proof. □

The fraction $\frac{\sigma_X^2}{\sigma_Z^2}$ is called the *signal-to-noise ratio*, or SNR, and represents the signal power relative to the noise power. The capacity of the AWGN channel is sometimes noted $C_{AWGN} = \frac{1}{2} \cdot \log_2(1+\text{SNR})$

2.2 Quantum information theory

The information-related quantities defined in the first section can be extended, thanks to the quantum formalism, to the quantum domain. This is particularly interesting since it becomes possible to bound the information accessible to an eavesdropper during a quantum communication.

2.2.1 The Von Neumann Entropy

The extension of the notion of entropy to quantum states is called the *Von Neumann* entropy.

Definition 7 (Von Neumann Entropy)**.** Any mixed or pure quantum state $\hat{\rho}$ can be written as $\hat{\rho} = \sum_i \lambda_i |\phi_i\rangle \langle\phi_i|$ where the $|\phi_i\rangle$ are orthonormal vectors and $\sum_i |\lambda_i|^2 = 1$. The Von Neumann entropy of $\hat{\rho}$ is the generalisation of the notion of entropy to quantum state $\hat{\rho}$. It is noted $S(\hat{\rho})$ and is defined by

$$S(\hat{\rho}) = -\sum_i \lambda_i \log_2 \lambda_i. \tag{2.31}$$

To not have to write the explicit eigenvalues of $\hat{\rho}$ the Von Neumann entropy is more conveniently noted :

$$S(\hat{\rho}) = -\mathrm{Tr}\big[\hat{\rho}\log_2\hat{\rho}\big]. \tag{2.32}$$

The Von Neumann entropy quantifies the average information that can be obtained by a measurement of state $\hat{\rho}$. It has properties similar to the classical entropy :

- For all $\hat{\rho}$, $S(\hat{\rho}) \geq 0$ with equality if and only if $\hat{\rho}$ is a pure state, which would be the classical equivalent of a deterministic state.
- If $\hat{\rho}$ is a quantum state in a Hilbert space of dimension d, $S(\hat{\rho})$ is bounded by $S(\hat{\rho}) \leq \log_2 d$ with equality if and only if $\hat{\rho} = \mathbb{I}/d$.
- If $\hat{\rho}_{AB}$ is the density matrix of a composed system that is a pure state, then the Von Neumann entropy of each subsystem is equal i.e. $S(\hat{\rho}_A) = S(\hat{\rho}_B)$ where $\hat{\rho}_A$ and $\hat{\rho}_B$ are the density matrices obtained by tracing out subsystem B and A respectively.
- $S(\hat{\rho})$ is constant under any unitary transformation i.e. for any unitary U, $S(U\hat{\rho}U^\dagger) = S(\hat{\rho})$.

For a system composed of subsystems A and B we can also define the following entropy values :

- *The conditional entropy* : $S(A|B) = S(AB) - S(B)$.
- *The quantum mutual information* : it is the quantum counterpart to the mutual information and is given by $I(A,B) = S(A) + S(B) - S(AB)$.

Von Neumann entropy of Gaussian states

When $\hat{\rho}$ is an n-mode Gaussian state, the Von Neumann entropy can be computed from the symplectic eigenvalues of the state covariance matrix as

$$S(\hat{\rho}) = \sum_{i=1}^{n} G\left(\frac{\lambda_i - 1}{2}\right), \tag{2.33}$$

where the symplectic eigenvalues are defined in 1.85 and the function G is given by $G(x) = (x+1)\log_2(x+1) - x\log_2(x)$.

2.2.2 Accessible information

Suppose a setting where Alice communicates *classical information* with Bob using quantum states, which is the case during our QKD experiment. Similarly to classical communications, Alice holds a random variable X which can take for example n values $\{0, ..., n\}$ with probabilities $\{p_1, .., p_n\}$. Based on the realisation of X, Alice prepares quantum state $\hat{\rho}_X$ chosen from a set $\{\hat{\rho}_1, ..., \hat{\rho}_n\}$ and gives the state to Bob. By performing a measurement M on the state $\hat{\rho}_X$, Bob obtains a classical random variable Y_M which depends on X and the measurement.

Definition 8 (Accessible information)**.** The accessible information is the maximal amount of classical information that can be extracted from a quantum system when the information is encoded using a particular ensemble of quantum states, and is given by

$$I^{\mathrm{acc}}_{X,\hat{\rho}} = \max_M I_{X,Y_M}. \tag{2.34}$$

Therefore the accessible information computes the maximum of I_{X,Y_M} optimized over the set of all possible measurements performed by Bob. We do not have an explicit formula to the accessible information in this case, but it is possible to give an upper-bound.

Theorem 6 (Holevo's bound)**.** *In the setting described above, the accessible information on variable X from the quantum state $\hat{\rho}$ is*

$$I^{\text{acc}}_{X,\hat{\rho}} \leq S(\hat{\rho}) - \sum_{i=1}^{n} p_i S(\hat{\rho}_i), \tag{2.35}$$

where $\hat{\rho} = \sum_{i=1}^{n} p_i \hat{\rho}_i$ is the mixed state sent to Bob. The right hand side of the inequality is called the Holevo information of state $\hat{\rho}$ and is noted $\chi(\hat{\rho}, X)$

The Holevo bound is tight if $\hat{\rho} = \mathbb{1}/n$, that is if the $\{\hat{\rho}_i\}$ form an orthonormal basis of the n dimensional Hilbert space and are equiprobable, i.e. $p_i = 1/n \ \forall i$. Then we can write the state $\hat{\rho}$ in the form :

$$\hat{\rho} = \frac{1}{n} \sum_{i=1}^{n} |i\rangle \langle i| , \tag{2.36}$$

where $\langle i|j\rangle = \delta_{i,j}$. Since the quantum states sent by Alice are orthogonal, Bob can discriminate between the n quantum states with probability 1 by applying the projective measurements $\{E_i = |i\rangle \langle i|\}_{i=1}^{n}$. Then we have $Y = X$ and we can compute the mutual information between X and Y :

$$I_{X,Y} = \log_2 n. \tag{2.37}$$

which is also the Holevo information since the $\hat{\rho}_i$ are pure states $S(\hat{\rho}_i) = 0$ and $S(\hat{\rho}) = \log_2 n$.

This concludes this relatively short chapter where we covered the very basics on information theory. We refer the interested reader to [21] for further exploration of the field. Here, we introduced the notion of information for classical and quantum variables and gave some interesting behaviors of the information quantities. The important results for this work moving forward are how to compute the Von Neumann entropy of Gaussian states from the symplectic eigenvalues as in equation 2.33 and Holevo's bound. These will play a central role during the CV-QKD protocol, which we will discuss further in chapter 4. Before this however, we cast aside the quantum world –just for a bit– in the next chapter to discuss some basic notions of cryptography.

Chapter 3

Cryptography

Contents

In this thesis we focus on quantum key distribution (QKD), protocols which enable two distant parties to share a secret key which is guaranteed secure by the laws of physics. But before we can discuss these protocols and our contributions to the field, it is crucial to understand the stakes of key sharing between distant parties and why QKD is an interesting protocol to achieve this goal. The answers to these questions require understanding of the cryptographic world. We provide an introduction to the field in this chapter and discuss the paradigm shift induced by a potential future quantum computer.

3.1 Principle of cryptography

Cryptography is an ancient science -dating back to antiquity- which initially aims at securing the contents of a message such that only the intended receiver can retrieve its original content. In our digital era, insuring confidential communications is paramount for user privacy and safeguarding of sensitive data, but other security guarantees are also desirable. We discuss in this section the different security guarantees required for modern communications, and the security models available.

3.1.1 Secure communication

The context in which we analyse secure communications is one where a transmitter wants to send a message $M \in \{0,1\}^n$, also called *plaintext*, to a receiver without revealing its contents if it were to fall

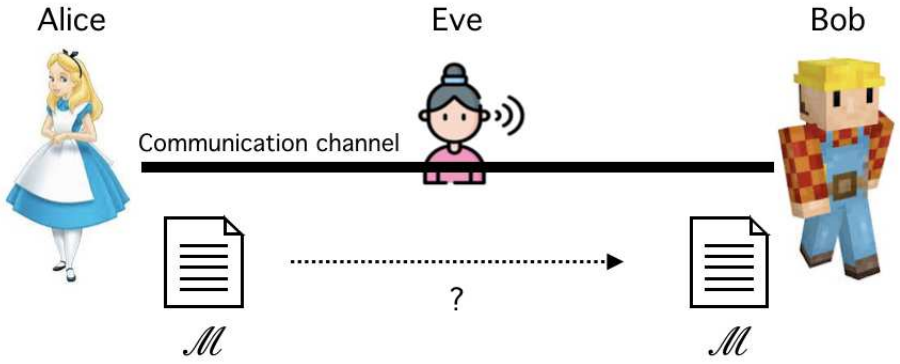


Figure 3.1: The setting is the following. Alice needs to send M to Bob over a communication channel, but Eve can intercept the message and Alice must insure that she does not learn the contents of M.

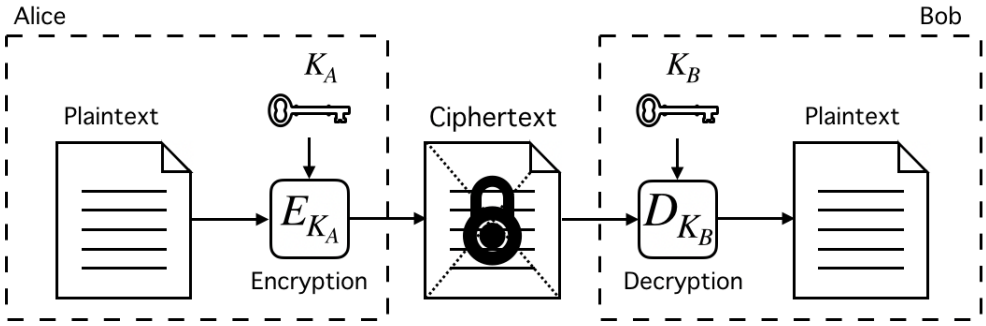


Figure 3.2: Depiction of the encryption of the plaintext and decryption of the ciphertext using the keys K_A and K_B.

in the hands of a malevolent adversary. It is customary in the cryptographic world to give names to the different roles played during the communication process. We will respect these conventions here and denote the transmitter, the receiver and the adversary by Alice, Bob and Eve respectively. We depict the setting of the further analysis in the figure 3.1.

Confidentiality. The security service sought by Alice and Bob is called *confidentiality*. To insure this, Alice performs a reversible transformation of M before sending it to Bob. The transformation process is indexed by a secret K_A held by Alice. It is called *encryption* and denoted E_{K_A}. The encrypted plaintext is called the *ciphertext* and is denoted $C = E_{K_A}(M)$. Bob can retrieve the plaintext from the ciphertext because he has a secret K_B which provides the inverse transformation, called *decryption* and noted D_{K_B} such that $D_{K_B}(C) = M$. The security of the encryption lies in the fact that it is not possible to perform the decryption process without knowledge of K_B. The secrets K_A and K_B are called the *keys*. The encryption and decryption process is depicted in the figure 3.2.

We will discuss further in this chapter the two big families of cryptographic primitives which are symmetric and asymmetric cryptography. In the first, $K_A = K_B = K$ and the keys must remain unknown to all but Alice and Bob. In the latter $K_A \neq K_B$ and only K_B must remain secret, K_A can be public which enables anyone to encrypt messages for Bob.

Security primitives beyond confidentiality. If confidentiality is crucial to insure secure communication over public channels, it is not sufficient in itself to guarantee secure communications.

Three other security primitives are also necessary and play a central part in modern communications :

- **Authentication.** Alice and to Bob must be given guarantees that they are communicating with each other and not with Eve, or else Eve could perform a so-called *Man-in-the-middle* attack where she impersonates Alice to Bob and Bob to Alice.
- **Integrity.** The message received by Bob must be guaranteed unaltered by Eve.
- **Non-repudiation.** Individuals should not be able to deny actions such as signing a contract online.

In the next section we will see how modern cryptographic primitives insure the four security services discussed above, but first we discuss different security models for cryptosystems.

3.1.2 Security model : information-theoretic vs computational

There are different security models associated with encryption processes. These provide guarantees with different levels of strength, but also different levels of complexity.

Information-theoretic security. This type of security, also called perfect secrecy, is achieved if the a priori probability of the message $p(M)$ and the a posteriori probability of the message conditioned on the knowledge of the ciphertext $p(M|C)$ coincide from Eve's perspective.

An example of perfect secrecy is the *One-time pad* (OTP) scheme. It is a symmetric encryption protocol for which the ciphertext is obtained by performing the XOR operation between the message and the key of the same length than the message. Importantly, the key must be chosen at random such that for all K we have $p(K) = 2^{-n}$. The encryption and decryption give

$$C = E_K(M) = M \oplus K, \tag{3.1}$$
$$M = D_K(C) = C \oplus K. \tag{3.2}$$

We can prove the OTP scheme has perfect secrecy using Bayes rule. For all M and K we have

$$p(M|C) = \frac{p(M)p(C|M)}{p(C)}, \tag{3.3}$$

and we have that $p(C|M) = p(K)$ and $p(C) = p(K)$ which proves the point.

An important implication of perfect secrecy is that the key must be of the same length than the message which can be difficult to implement in practice. Also the secret key cannot be re-used, or Eve can guess information on the secret key and perfect secrecy is lost. To see this, consider two messages M_1 and M_2 giving ciphertexts C_1 and C_2. Then we have that

$$C_1 \oplus C_2 = M_1 \oplus M_2, \tag{3.4}$$

Eve can therefore obtain the bitwise parity of the messages. Because of the difficulty of sharing a unique key of the same length than the message for each communication, usual cryptosystems do not employ perfect secrecy but rely on a relaxed security assumption : computational security

Computational security. In this security model the key is generally of (much) smaller size than the message to be encrypted. Hence for a given ciphertext the number of possible messages -which matches the number of possible keys- is greatly reduced compared to the perfect secrecy model. The security in this view lies in the fact that the adversary has bounded computing capabilities, therefore he cannot crack the encryption scheme in a *reasonable amount of time*. This concept relates to how long it takes a computer to perform a task and is quantified in the average number of operations for completing the task. Therefore the security in this view is dependant on :

- The current relation between computing power and cost. The security is defined against a certain level of computing power which has to be estimated based on current technology and foreseeable advances. As technology progresses and computing power becomes more readily available, encryption conventions can evolve by imposing longer keys and more resilient encoding algorithms.

- The best known attacks to crack the encryption. Although unlikely, it is always possible someone finds a flaw in an encryption algorithms which can be exploited to reduce the number of operations required to crack the code.

Obviously using cryptography in a computational security model is much easier than for an information-theoretic security model since one key of fixed length can be used to encode arbitrary messages and also be used more than once without decreasing the security. This is why modern cryptography is designed to provide security in this security model. In the next section we review the relevant cryptographic protocols used today in order to discuss in the following section how a quantum computer can impose a paradigm shift on some current cryptosystems.

3.2 Modern cryptography

Modern cryptography is built on a set of cryptographic primitives, basic building blocks which are used in more complex protocols to provide the desired security service. Three important kind of primitives are hashing functions, symmetric cryptography and asymmetric cryptography. Together they can provide the set of security services discussed in subsection 3.1.1.

3.2.1 Hashing functions

A hashing function h is a function which maps data $M \in \{\{0,1\}^n\}_{n=1}^{\infty}$ of an arbitrary size n to fixed-size values $h(M) \in \{0,1\}^k$ which are called hash values. Since the cardinality of inputs is much larger than the cardinality of outputs, there are necessarily *collisions* : two (or more) inputs M_1 and M_2 can give the same output by h. A good hashing function is a function for which these collisions are very difficult to find.

Interesting hash functions are key-based hash functions. They are basically hash functions indexed by a secret key which determines the behavior of the hash function. Hash functions and key-based hash functions play a central role in communications because the hash values are a fingerprint of the message which can be used to provide authentication and integrity. We illustrate this in an example below.

Application example. Consider the previous context in which Alice encodes her message M into the ciphertext C before sending it to Bob. However this time she wants to guarantee that she sent the message and that it was not altered, i.e. guarantee authentication and the integrity of her message. To do this she also computes the hash value of C using a key based hash function and outputs $h_K(C)$, also called a keyed-hash message authentication code (HMAC). She sends C and $h_K(C)$ to Bob who computes the HMAC of the ciphertext he received. If his value coincides with $h_K(C)$, he is assured of the authenticity and integrity of the message.

3.2.2 Symmetric cryptography

In symmetric cryptography the encryption and decryption key are the same and must be kept secret. Until 2001 the standard encryption algorithm was DES -for Data Encryption Standard- functioning with 58 bits keys. Labelled as too weak because of the short size of the key, DES has been replaced with AES -the Advanced Encryption Standard- with keys of length 128, 192 or 256 bits.

AES. The AES encryption is a *block cipher algorithm*. This means that the plaintext is divided into block of equal length, 128 bits here, and each block is independently encrypted by the algorithm using the secret key. The principle is as follows. The 128 bits plaintext is written in the shape of a 4×4 byte matrix, then a series of transformations is iterated on the matrix to provide encryption. Each iteration requires a different secret key to determine the specific transformations of that iteration. To do this, a set of subkeys are first generated from the symmetric key using a deterministic key expansion algorithm. We give the different steps of AES encryption below.

1. Generate subkeys from the symmetric key $\mathcal{K}$
2. XOR plaintext M and symmetric key $\mathcal{K}$
3. Iterate N times operations below :
   (a) SubBytes : permutation of the matrix bytes based on the Rijndael S-box (permutation table).
   (b) ShiftRows : circular shift of the rows of the 4×4 matrix by respectively 0, 1, 2 and 3 increments to the right.
   (c) MixColumns : each byte is transformed into a linear combination of the bytes in the same column.
   (d) AddRoundKey : XOR resulting matrix with the corresponding subkey.
4. Final iteration, the MixColumns step is skipped : SubBytes, ShiftRows, AddRoundKey.

The number of iterations N depends on the length of the secret key. For keys of length 128, 192 and 256 bits we have N equal to 9, 11 and 13 respectively. To this day, the best known attack on AES encryption requires testing an average of $2^{124.9}$ keys. It is estimated this would take longer than the age of the universe for the most advanced supercomputers in the world.

Usage. Symmetric cryptography such as AES are used to provide confidentiality. They are particularly well suited to encode large volumes of data since there is no limit to the length of the input message. We can freely increase or decrease the length of the message which will only result in more or less blocks to be encoded for the block cipher algorithm.

An important prerequisite for symmetric cryptography is for Alice and Bob to share a secret key before starting the protocol. This is know as the key distribution problem and can be solved using the other family of cryptographic protocols : asymmetric cryptography.

3.2.3 Asymmetric cryptography

Contrary to symmetric cryptography, in asymmetric cryptography the encryption and decryption keys are different. Such protocols are also referred to as public-key cryptography because the encryption key is public while the decryption key -or private key- is kept secret. Then each user in a network can have their own set of public/private keys allowing all members of the network to encrypt messages intended to them.

RSA. The RSA encryption scheme, named after its inventors Rivest, Shamir and Adleman, is an asymmetric encryption scheme based on algebraic properties. Each user (e.g. Alice) of the RSA encryption scheme has a public key composed of two integers (e, n) and a private key d. These must obey specific rules in order for the encryption/decryption to function :

1. Alice chooses two large prime integers p and q to compute $n = pq$.
2. Alice computes Euler's totient function of n which is in this case $\phi(n) = z = (p-1)(q-1)$.

3. Alice chooses an integer e smaller than n such that e is relatively prime with z.

4. Alice computes $d = e^{-1} \bmod(z)$ such that $de = 1 \bmod(z)$. The value e exists by construction of z and d thanks to algebraic properties we do not develop further in this work.

Arithmetic theorems give that if 4. holds, then for all $a \in \mathcal{Z}/n\mathcal{Z}$, $a^{ed} = a \bmod(n)$. Using this we can construct asymmetric encryption and decryption schemes using e and d :

$$C = M^e \bmod(n) \tag{3.5}$$

$$M = C^d \bmod(n) \tag{3.6}$$

Since (e, n) is public, anyone can encrypt data to send to Alice. On the other hand she is the only person who knows d therefore she is the only one who can decipher those messages.

The security of the RSA encryption scheme is based on the fact that it is very difficult, given (e, n), to compute the private key d. Actually the only way to do this is to find p and q from n. This is called the *factoring problem* and no efficient way of achieving this has been found yet using classical computing methods.

Usage. By nature RSA cannot be used on messages of arbitrary length since the space of possible messages of cardinality n. In addition since the encryption and decryption processes are slow due to the operations on large numbers, it is not suited to encrypt large volumes of data. However public-key cryptography is particularly useful for other reasons :

- *Sharing symmetric keys.* A key interest in public key cryptography is that it can enable two parties to share a secret key, which would later allow them to use symmetric cryptography to encode large quantities of data between them.

- *Digital signature.* An interesting feature of public-key cryptography is that one can also sign messages. This is achieved by «encrypting» the message with the private key : the user is the only one able to do this since he is the only one with knowledge of his private key. However anyone can verify the signature using the public key. The digital signature provides authentication, integrity and non-repudiation.

3.3 Cryptography in a quantum world

For the last 40 years or so, starting from Feynman's 1981 conference talk [2], research efforts were directed towards harnessing quantum mechanical systems for computing purposes. The holy grail of the field is to build a universal quantum computer using *qubits* as basic building blocks. As opposed to classical bits, qubits must be described by quantum mechanics and as such can be in superposition of different states. Harnessing this, quantum computers can perform some tasks much faster than classical computers, which is an exiting idea for many applications but can pose security threats if the hard problems at the core of cryptographic primitives become tractable. This forces us to review our cryptographic landscape in this new context.

3.3.1 Threats to cryptography posed by the quantum computer

Quantum algorithms -running on a quantum computer- are interesting when they can solve a particular task faster than a classical computer. Relevant examples of such algorithms are Shor's and Grover's algorithms, named after their discoverers.

- **Shor's algorithm.** Solves the factoring and discrete logarithm problem in polynomial time as opposed to super polynomial time for the best classical algorithm. Can be used to break RSA encryption rendering this cryptographic primitive obsolete in a quantum world.

Algorithm	Key length	Security level for classical computer	Security level for quantum computer
RSA-1024	1024	80 bits	∼0 bits
RSA-2048	2048	112 bits	∼0 bits
AES-128	128	128 bits	∼64 bits
AES-256	256	256 bits	∼128 bits

Table 3.1: Comparison of the security levels provided by RSA and AES against a classical and quantum computer. Table taken from [22].

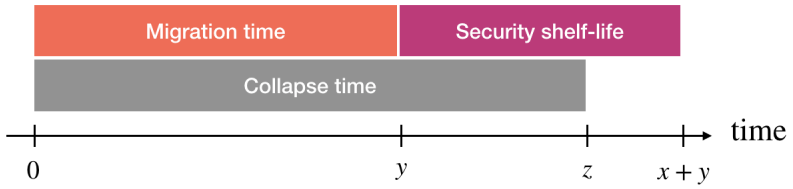


Figure 3.3: Encrypted data should be guaranteed safe during a reasonable period of time x. Until we have completed the migration towards quantum-safe solutions, at time y, encryption will be performed using quantum-vulnerable solutions. Thus if the collapse time z when a quantum computer becomes available is smaller than $x + y$, we cannot guarantee the security shelf-life x.

- **Grover's algorithm.** Searches an unstructured database with N entries for a specific entry with complexity $O(\sqrt{N})$ compared to $O(N)$ for the best classical algorithm. Can be used to speedup the search for symmetric keys to break AES encryption, thus larger key sizes will be necessary in a quantum world.

To illustrate the impact of these algorithms we represent in the table 3.1 the effective key lengths of commonly used RSA and AES encryptions for a quantum computer. The cryptographic primitives harshly impacted by the future quantum computer are the public-key cryptography solutions such as RSA, which are crucial to share symmetric keys.

Action must be taken now. A question that is raised by the possibility of a quantum computer is the following : when do we adapt our cryptographic systems to this new context ? Since the quantum computer is still in early stages of development, this question is legitimate.

To answer this question, one must consider three quantities defined in [8] which are the following :

- *Security shelf-life.* How long we need our encryptions to remain secure. Let us denote this duration by x.
- *Migration time.* How long we need to transpose all cryptographic primitives to quantum-safe solutions. Let us denote this duration by y.
- *Collapse time.* How long until we can expect a large-scale quantum computer capable of cracking current encryption. Let us denote this duration by z.

A «theorem» discussed is [8] answers the question above : « If $x + y > z$, then worry ! ». The idea is that until we have transitioned the full infrastructure towards quantum-safe solutions, soon-to-be obsolete cryptographic primitives will continue to be used, hence an adversary could perform a « store-now, decrypt later » attack and wait for the development of the quantum computer.

With the development of the quantum computer picking up the pace, it is absolutely necessary to begin the transition as soon as possible. We discuss the solutions explored in the next subsection.

3.3.2 Quantum-safe cryptography

Quantum-safe cryptography seeks to develop cryptographic primitives which are safe even if an attacker has access to a quantum computer. The field is divided in the two complementary fields of post-quantum cryptography (PQC) and quantum key distribution (QKD).

Post-quantum cryptography. The first solution consists in developing cryptographic primitives based on problems for which a quantum computer does not provide a sensible advantage over a classical computer. Quantum-safe cryptography research is mainly focused on public-key cryptography because, as far as we know, these are the primitives which we know will become obsolete against an adversary owning a quantum computer.

Let us provide some examples of PQC algorithms which are investigated to replace current public-key algorithms. Some interesting candidates for post-quantum public key cryptography are for example code-based cryptography [23], multivariate cryptography [24], lattice-based cryptography [25] and supersingular elliptic curve isogenies [26].

PQC is a solution applied to the software level, hence is easily implementable on current machines. These solutions will follow in the approach of modern cryptography in the sense that they will be secure on the condition the attacker has limited computing power, and that no algorithm will be found to crack the encryption with a considerable speedup. Moreover, PQC algorithms will need to be adapted if the available computing power increases drastically, as was the case when we migrated from DES to AES.

Quantum key distribution. QKD is a type of key distribution protocol. It is based on the exchange of quantum states over a communication channel during a communication phase. Then, by harnessing the no-cloning theorem and the effect of projective measurements, QKD enables Alice and Bob to quantify the information leaked to Eve during a post-processing phase. Ultimately a QKD protocol produces a secret key shared by Alice and Bob with the guarantee that any adversary has no information on the key.

Compared to PQC, QKD requires an implementation on the physical layer which supposes suitable communication channels and the necessary hardware. The compensation for the experimental challenges of QKD -which will be discussed in the rest of this manuscript- lies with the strong security guarantee on the key. The fact that the adversary has no information on the secret key means that his best strategy is a random guess, which is independant from future developments of computing power or of algorithm performance. We review QKD more specifically in the next section.

3.4 Quantum key distribution

In this section we discuss the principles of quantum key distribution and give an example of protocol. Then we review the different types of QKD existing today.

3.4.1 Principle

A generic QKD protocol is built on the assumption that two requirements are met. We begin by discussing these requirements, then move on to giving the main steps of the generic QKD protocol.

Prerequisites. The setting for a generic QKD protocol is represented in the figure 3.4. There are two prerequisites for any QKD protocol which must be verified.

The first is the basic assumption that Alice and Bob are connected by an untrusted quantum channel in order to exchange quantum states. The quantum channel is said to be untrusted because it is assumed to be Eve in the sense that she can intercept all the quantum states output from Alice's lab and that all distortions taking place on the channel are her doing.

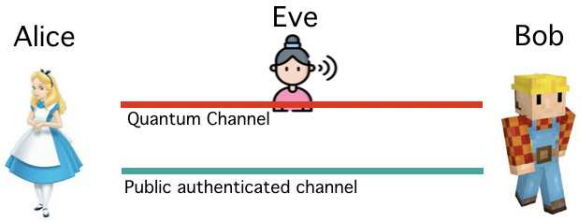


Figure 3.4: Setup of a generic QKD protocol. The two prerequisites are that Alice and Bob are connected via 1) an untrusted quantum channel which is assumed to be Eve and 2) a public authenticated classical channel.

The second assumption is that Alice and Bob are also linked by a public authenticated channel to perform the post-processing. The authentication of the classical channel is crucial to prevent any man-in-the-middle attack which would result in the loss of any security provided by the protocol. In this attack Alice and Bob think they are performing a QKD protocol with each other while in fact they are both talking to Eve, hence Eve generates a secret key shared between her and Alice and between her and Bob, and can always decipher messages from one to the other before encrypting them again with her second key to go unnoticed.

Contrarily to the first assumption the authentication between Alice and Bob is not trivial to realise and it must be done carefully. Importantly, it cannot be achieved via public key algorithms since the interest of QKD lies in the scenario where the adversary has a quantum computer and these algorithms are not secure anymore. Therefore the authentication must be performed using quantum resistant algorithm such as key-based hash functions described in subsection 3.2.1. Since these require Alice and Bob share a secret key, QKD is technically a key *expansion* protocol rather than a key *distribution* protocol, but the term QKD is well established and we will continue to use it in the rest of this work for clarity.

Before moving on let us briefly discuss the impact of the authentication on the global security of the protocol. The question is legitimate since we will use a computationally safe algorithm to authenticate Alice and Bob, therefore what about the unconditional security of QKD ? Well, consider that it is irrelevant for Eve to break the authentication scheme after the QKD protocol has taken place since it will be too late to perform the man-in-the-middle attack. Therefore she must do so *during* the protocol which will be very challenging. Ultimately this means that she cannot use future computing power to jeopardize the security of the protocol, but that some limited computational assumption must be made on her current computing power for the authentication to be secure.

The phases of a generic QKD protocol. A QKD protocol is composed of different steps followed by Alice and Bob which we review here.

1. *Quantum communication.* They exchange and measure quantum states sent over the quantum channel. After this phase, the rest of the communication occurs on the public classical channel.

2. *Sifting.* They agree on a subset of measurements they keep, and discard the rest.

3. *Parameter estimation.* They reveal some of their measurement results to estimate relevant parameters to quantify the action of the eavesdropper. These are determined by the type of QKD protocol employed.

4. *Keymap.* If their results during the parameter estimation phase are compatible with sharing a secret key, they map their measurement results to a bit string. At this stage, this bit string can be different for Alice and Bob.

5. *Error correction.* They perform error correction so they agree on the same bit string called the raw key. Eve potentially has some information on the raw key.

6. *Privacy amplification.* They apply the same random hash function to the raw key. The strength of the hash function, quantified by the reduction of length of the raw key, is determined by the results of the parameter estimation phase. Information theory guarantees that Eve knows nothing of the resulting key shared between them.

3.4.2 An example of protocol : BB84

In order to illustrate the QKD principles discussed above let us review the functioning of perhaps the most famous QKD protocol, named BB84 after its inventors -Benett and Brassard- and the year of the publication detailing said protocol -1984. This particular example will help understand how the security of QKD protocols is captured.

Quantum communication. During a run of the BB84 protocol, Alice encodes a sequence of classical bits on the polarisation of single-photons. For this she uses one of two bases, either the vertical-horizontal ($\rightarrow$ and $\uparrow$) basis or the diagonal-antidiagonal ($\nearrow$ and $\nwarrow$) basis, mapping bits 0 and 1 to the states $(\rightarrow, \nearrow)$ and $(\uparrow, \nwarrow)$ respectively.

Bob measures the state of polarisation by splitting the incoming photons on a polarising beam splitter (PBS) and placing a single photon detector (SPD) on each path. The inclination of the PBS determines Bob's measurement basis. Quantum measurement theory stipulates that if Bob chooses the same basis as the one used by Alice, he will perfectly separate quantum states encoding bits 0 and bits 1. In the case where he chooses the other basis, the quantum states will be routed to a random SPD with probability half. The vertical-horizontal and diagonal-antidiagonal bases are called *mutually unbiased bases* because measurement in one basis does not give any information on a state encoded in the other.

Sifting. After all the quantum states have been exchanged Alice and Bob publicly reveal their measurement bases. They discard any measurement result for which Alice and Bob did not use the same basis, as the results in those bases would be random.

Parameter estimation. Alice reveals a subset of the bit string she sent to Bob and he reveals the corresponding bit sequence he measured. They aim to quantify the quantum binary error rate (QBER) from their data, which is the number of quantum states which yielded an erroneous measurement result at Bob's over the total number of transmitted quantum states. The data shared by Alice and Bob at this stage is is represented in the figure 3.5.

The QBER is a useful metric which quantifies the actions of Eve during the communication of the quantum states. To see this, consider the goal of Eve is to gain knowledge of the secret key and the only way she can do this is through the quantum states since she does not have access to Alice and Bob's laboratories. Thanks to the no-cloning theorem 2 she cannot replicate the non-orthogonal quantum states and therefore can only measure the quantum states transiting over the quantum channel to gain knowledge. By doing so, she will necessarily introduce errors between Alice and Bob according to the measurement postulate 5. Consider for example a basic intercept-resend attack, depicted in the figure 3.6. The attack consists in Eve measuring each quantum state exiting Alice's lab and sending to Bob a quantum state polarised according to her result. On average Eve will measure Alice's states in the wrong basis half of the time, and when she does she will introduce a bit flip half of the time. Hence an intercept-resend attack will asymptotically generate a QBER of 0.25.

Error correction and privacy amplification. Alice and Bob perform error correction to agree on a raw key, then use the same random hash function to insure Eve is completely uncorrelated from their resulting key.

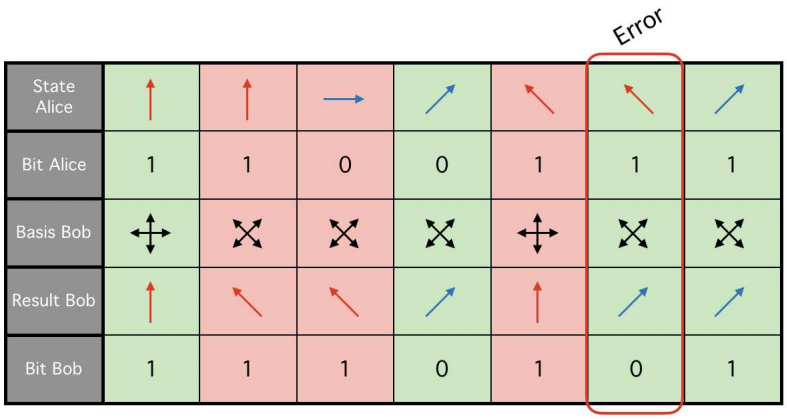


Figure 3.5: Representation of the successive states sent by Alice and the measurement performed by Bob during a BB84 protocol. For the columns in green Alice and Bob used the same basis and conserve their data for this state. For the columns in red, Alice and Bob used a different basis therefore they discard that measurement. The color of the arrows represents the bit associated to that symbol, red for 1 and blue for 0. Even when Bob chooses the correct basis, errors can occur. Alice and Bob estimate the error rate during the parameter estimation phase.

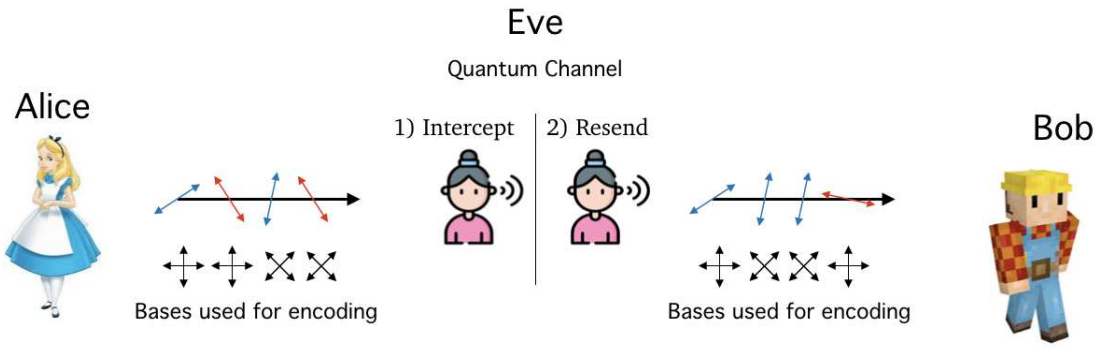


Figure 3.6: Depiction of an explicit intercept-resend attack by Eve.

3.4.3 Types of protocols

Since its inception by Charles Bennett and Gilles Brassard in 1984, QKD has come a long way and a multiplicity of different protocols has been developed. Today QKD protocols can be categorized by the techniques used to encode and measure the quantum states and by the assumptions made on the devices during the protocol. We review these here.

Discrete-variables and continuous-variables. QKD protocols can be divided by the technique used to detect the quantum states. The first type of protocol relies on single photon detectors (SPDs) to measure the phase or polarisation of quantum states. Since the measurement result produced is a detector "click" the outcome can only take a discrete set of values, hence these protocols are referred to as discrete-variable (DV)-QKD. The second type of protocol is called continuous-variable (CV) QKD and uses coherent detection to detect the quadratures of the electromagnetic field. This time the measurement result can take a continuous set of values hence the name of the type of protocol.

Fundamental differences between CV- and DV-QKD will be discussed in **??**.

Entanglement-Based and Prepare-and-Measure. In order to generate a secret key Alice and Bob need to first share correlations during the quantum communication phase of the protocol. In general, QKD protocols can be fundamentally differentiated by whether Alice generates a bimodal entangled state and measures her particle or if she simply encodes classical information on a quantum state. In the first case the protocol is called *entanglement-based* (EB) and *prepare-and-measure* (PM) in the other. They are described in the following manner

- *Entanglement based.* Alice generates in her lab a two-mode entangled state $|\Phi\rangle_{AA'}$. She keeps the particle denoted by register A and sends the other particle to Bob over the quantum channel, which can be defined by the map $\mathcal{N}_{A'\to B}$, such that the state shared by Alice and Bob is written

$$\hat{\rho}_{AB} = \mathcal{N}_{A'\to B}\big(|\Phi\rangle\langle\Phi|_{AA'}\big). \tag{3.7}$$

- *Prepare and measure.* Alice prepares a quantum state $|\psi_k\rangle$ with a probability p_k, where the indexes k can range over a discrete or infinite set of values. The state generated by Alice is represented by the density matrix $\hat{\rho}_A = \sum_k p_k \hat{\rho}_k$ where $\hat{\rho}_k = |\psi_k\rangle\langle\psi_k|$. After transition on the quantum channel, the state received by Bob is written

$$\hat{\rho}_B = \mathcal{N}_{A\to B}\big(\hat{\rho}_A\big). \tag{3.8}$$

Device independent QKD. The security proofs of QKD bounding the information leaked to Eve rely on the implicit assumption that Alice and Bob's devices function correctly and according to a given model. This can create security loopholes known as *side-channel attacks* when an attacker can exploit some component which is not accounted for in the security proof in order to gain an advantage.

Multiple side-channel attacks have been detected and patched for both DV- [27, 28, 29] and CV-QKD [30, 31, 32] systems, but it is not possible to claim new attacks will not be discovered in the future. In an attempt to escape this hack-and-patch cycle, a new type of protocol was developed which does not make any assumptions on the type of devices used during the experiment. These protocols are known as *device-independent* (DI) QKD.

In order to understand DI-QKD we need to introduce the notion of Bell inequalities. These were first introduced in the paper by John Bell [33] answering the Einstein-Podolsky-Rosen (EPR) paradox paper [34] claiming that quantum-mechanics were necessarily incomplete since it is not possible to predict with certainty the outcome of a quantum system. For Einstein, Podolsky and Rosen there were necessarily some hidden variables which would make quantum systems deterministic if accounted for. In his paper, Bell shows that this is not the case by repeating an experiment multiple times and considering the statistics of the measurement outcomes. He shows that if the hidden-variable theory

were true, some inequality can be derived from the statistics. Since this inequality can be violated for entangled quantum states, the hidden variable theory is false and some quantum systems are naturally unpredictable.

DI-QKD harnesses this concept to generate a secret key. Alice generates an entangled pair of photons and sends one pair to Bob. They measure their respective photons either in a random basis from a given set or in a predetermined basis. The measurements in the random bases are used to verify that their measurement statistics violate Bell inequalities and therefore that they share entanglement and randomness. Since this is the case, their measurements in the predetermined basis are perfectly correlated and they use these to distill a secret key.

Measurement-device independant QKD. DI-QKD is particularly interesting from a theoretical point of view because it requires no assumptions on the devices used during the experiment. The downside is that is necessitates sharing entanglement over large distances in order to violate Bell inequalities, which is experimentally challenging and at the moment the reported key rates of DI-QKD systems are very limited.

A more practical version of DI-QKD is measurement-device independant (MDI) QKD [35, 36] which makes no assumption on the detection apparatus but assumes Alice and Bob can generate their desired quantum states perfectly. Typically during an MDI-QKD protocol Alice and Bob encode bits on orthogonal quantum states in one of two bases. Then they send their state to a central receiver, possibly Eve, who performs a Bell measurement and outputs the result. When they used the same basis, they know based on the measurement announced if they sent the same state or not, hence they can deduce the bit encoded by the other party.

Beyond the increased security provided by MDI-QKD, it is interesting because the measurement is performed outside of Alice and Bob's laboratory. In particular this makes MDI-QKD a promising candidate for QKD networks where all users can be connected to a central measurement node, while no security assumptions must be made on said node.

Satellite QKD. Satellite QKD is particularly interesting because it can potentially achieve QKD over larger distances that fiber-based protocols. The reason behind this is that the losses in the fiber are the main limitation for QKD protocols, and the losses in space are zero. Hence satellite based quantum-communications can reach ground stations thousands of km apart and the only losses affecting the quantum signal will be those of the ~ 10 km of atmosphere between the satellite and the ground station. We refer the interested reader to reference [37] for a review of satellite-based QKD.

Fundamental limit to any QKD protocol. It is interesting to investigate if there is a fundamental limit to the secret key rate that can be shared using QKD. This quantity is the two-way secret key capacity, noted $C(T)$, and depends on T, the channel transmittance. This question was tackled in reference [38], where the authors derived $C(T)$ regardless of the type of QKD protocol considered. The authors find that the following relation holds :

$$C(T) = -\log_2(1-T), \tag{3.9}$$

which is known as the PLOB bound, named after the authors.

We conclude this chapter here. We have given some insight to the functioning of current cryptographic systems used for secure communications and have highlighted the need for quantum-safe cryptography. One of these solutions, QKD, is based on the fundamental properties of quantum states and produces a shared key with information-theoretic security. As we have discussed above, many different kinds of QKD protocols exist, but in this work we will focus specifically on CV-QKD. In the next section we take a closer look to this particular type of QKD protocol.

Chapter 4

Quantum Key Distribution with Continuous-Variables

Contents

In the last chapter we discussed the role of QKD in the current cryptographic landscape and we illustrated the outline of a generic QKD protocol through the famous BB84 protocol. Then we gave different types of QKD protocols. In our work we focus on CV-QKD protocols, hence we provide a more detailed analysis of these protocols in this chapter. We begin in the first section by describing relevant CV-QKD protocols and how some protocols can be shown to be equivalent to each other for anyone outside Alice's lab. This will prove convenient to extend the security analysis from theoretical to implementation-friendly protocols. In the second section we discuss the different attack models for Eve and give the corresponding secret key rate. We will also provide tools to adapt the key rate to the practical setting. First we discuss how realistic assumptions can reduce the power of the eavesdropper and second we consider the impact of imperfect parameter estimation and privacy amplification due to the finite-size effects. The third section is dedicated to the explicit derivations of the key rate based on the protocol and protocol parameters. In the last section, we compare CV- and DV-QKD protocols to understand the strengths and challenges for each technology.

4.1 CV-QKD protocols

4.1.1 Examples of protocols

We begin this chapter by giving a few examples of CV-QKD protocols, 1 EB protocol and 2 PM protocols. From an experimental point of view it is much easier to implement PM protocols since in this case the quantum state generation closely resembles the symbol generation of classical telecommunications. In comparison, it is difficult to generate entangled states since this involves taking other steps which are not useful in telecom systems, hence are less widely used.

Unfortunately the security proofs for quantum key distribution are built on the EB picture of protocols, as we will see in the next section. It is however possible to transition from one picture to the other to extend the security proofs in the EB picture to PM protocols, as is shown for example in [39]. Although this is not always trivial, it works particularly well for the GG02 protocol described in the following. In that case we can show that from Bob and Eve's perspective, the PM version of the protocol is indistinguishable from an EB protocol in which Alice generates two-mode squeezed states and measures one mode before sending the other over the channel.

That being said lets describe 3 relevant CV-QKD protocols for this rest of this work.

EPR states. The first propositions for CV-QKD [40, 41] were EB protocols using the continuous variable equivalent of EPR states. They consisted in Alice generating the two-mode squeezed vacuum states described by

$$|\mathrm{TMSV}\rangle_{AA'} = \frac{1}{\cosh r} \sum_{n=0}^{\infty} \tanh^n r \, |n\rangle_A \, |n\rangle_{A'} \, . \tag{4.1}$$

Note that considering only particle A' by tracing out subsystem A we obtain a thermal state such that

$$\begin{aligned} \hat{\rho}_{A'} &= \mathrm{Tr}_A \Big(|\mathrm{TMSV}\rangle \langle \mathrm{TMSV}|_{AA'} \Big), \\ &= \frac{1}{\cosh^2(r)} \sum_{n=0}^{\infty} \tanh^{2n}(r) \, |n\rangle \langle n| \, . \end{aligned} \tag{4.2}$$

The mean photon number of this thermal state is given by $\bar{n} = \sinh^2(r)$.

GG02. The GG02 protocol [10], named after its founders Grosshans and Grangier, was the first protocol to make use of weak coherent states. For the state generation, in this protocol Alice generates coherent state $|\alpha\rangle$ according to a complex Gaussian distribution where each quadrature has variance V_A. The probability of sending each state in this case depends only on the state amplitude and is given by $p_\alpha = \frac{1}{2\pi V_A} e^{-\frac{|\alpha|^2}{2V_A}}$. On the detection side, Bob randomly chooses to measure the p or q quadrature using homodyne detection. Later this protocol was improved into a so-called *no-switching protocol* [42, 43] where Bob performs a heterodyne detection of both quadratures.

At first the GG02 protocol suffered from a 3-dB limit for the channel losses. This was because beyond this limit Eve would systematically have more information than Bob on the quantum state. This problem was later solved by introducing reverse-reconciliation [44] where Alice would map her raw key to Bob's.

What is particularly interesting in the GG02 protocol is that the average state sent by Alice is described by the mixture of coherent states

$$\hat{\rho}_A = \int_{\alpha \in \mathbb{C}} p_\alpha \, |\alpha\rangle \langle \alpha| \, d\alpha, \tag{4.3}$$

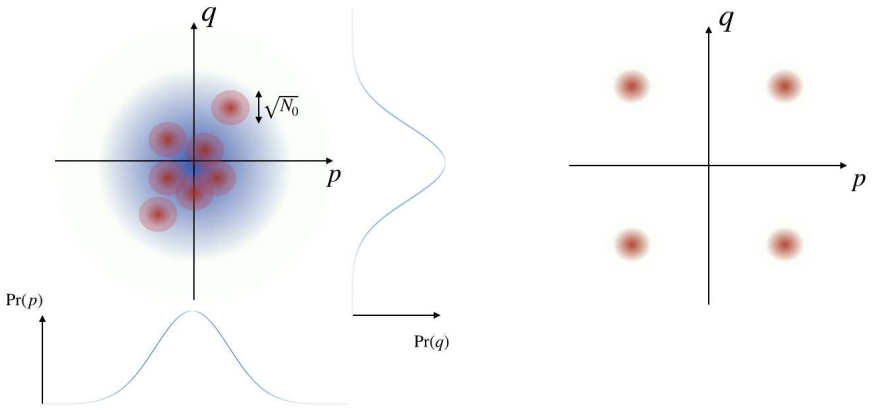


Figure 4.1: Schematic representation in phase space of the quantum states sent by Alice during a CV-QKD protocol. On the left we represent the Gaussian modulation, where each quadrature has a centered Gaussian probability distribution. On the right we represent the discrete Quadrature Phase-Shift Keying (QPSK) modulation. Each point has a thickness due to the shot-noise.

which can be shown to be the thermal state with mean photon number $\bar{n} = \frac{V_A}{2}$. Hence the statistical description of the state exiting Alice's lab is the same in the GG02 protocol than for the EPR states protocol. Therefore it is impossible for anyone but Alice to distinguish between the two protocols, and we can implement the PM version while analysing the security of the EB protocol.

Discrete modulated coherent states. Generating a Gaussian modulation for Alice can be experimentally challenging because she needs a true random number generator to determine the quadrature value to be encoded on the light. In addition, the keymap can be quite involved for Gaussian variables compared to DV-QKD or classical telecom using a finite set of states to encode bits. For this reason it is desirable to perform QKD using some finite set of states, as in classical telecommunications. In this work we have used both the four state protocol as well as a normalized random walk distribution with 64 states. The state preparation in each case is described below.

- *Four state protocol.* Here Alice chooses at random coherent state $|\alpha_k\rangle = ||\alpha|e^{i\frac{(2k+1)\pi}{4}}\rangle$ for $k \in \{1, 2, 3, 4\}$. It is the quantum equivalent of the Quadrature Phase-Shift Keying (QPSK) modulation used in classical telecommunications.

- *Normalized random walk distribution.* The coherent states $|\alpha_{k,\ell}\rangle$ of the normalized random walk distribution with m^2 states are defined by the amplitude

$$\alpha_{k,\ell} = \frac{\alpha\sqrt{2}}{\sqrt{m-1}}\left(k - \frac{m-1}{2}\right) + i\frac{\alpha\sqrt{2}}{\sqrt{m-1}}\left(\ell - \frac{m-1}{2}\right), \tag{4.4}$$

  and the set of probabilities

$$p_{k,\ell} = \frac{1}{2^{2(m-1)}}\begin{pmatrix} m-1 \\ k \end{pmatrix}\begin{pmatrix} m-1 \\ \ell \end{pmatrix}. \tag{4.5}$$

4.2 Security of CV-QKD

The security proofs for QKD protocols in general aim to bound the amount of information that has potentially been leaked to Eve during the protocol. For this, we must make some assumptions which will condition the security of the protocol on their veracity. We discuss this below.

4.2.1 Security assumption

Any kind of security is based on some basic assumptions. A trivial example is that we must assume Eve is not in Alice's or Bob's laboratory during the QKD protocol, or she could simply read out the secret key on their devices. Here we are interested in the assumptions which allow us to bound the information leaked to Eve during the protocol.

Attacks. The first relevant assumption relates to the power of the attacker. We consider three types of attacks Eve can perform to obtain information on the quantum states transiting on the quantum channel.

1. *Individual attacks.* Individual attacks are the less powerful type of attack a quantum adversary can perform. Here Eve is permitted to probe the quantum states transmitted on the channel one by one and store them in an individual quantum memory. She is restricted to measurements on the individual states, but she can chose to perform her measurement after learning of the full information communicated on the public channel.

2. *Collective attacks.* Collective attacks are similar to individual attacks except for the measurement performed by Eve. Here she is allowed to perform a collective measurement on all the quantum states stored in her memory. The measurement operator is therefore described on the Hilbert spanned by the tensor product of all the quantum states.

3. *Coherent attacks.* Coherent attacks are the most general type of attack performed by Eve. Here she can probe the entirety of the quantum communication using an ancilla state in a large Hilbert space. She can then perform a measurement on the full state. The state cannot in general be written as n copies of the same state.

Ideally we would like to bound Eve's information in the general case of coherent attacks. However this is a particularly difficult problem and we only know how to derive a bound in the regime of collective attacks. However in some cases we can extend the security in this regime to the case of general attacks. We discuss this further in the following.

Asymptotic regime or finite-size regime. In order to compute the secure key rate, it is convenient to suppose we are in the *asymptotic regime* where Alice and Bob communicate an infinite number of quantum states. This allows us to a) neglect the states discarded during parameter estimation and also b) suppose we can compute perfect estimators because of the infinite amount of samples.

Of course this is not the case in reality where necessarily the number of states sent over the channel are finite. We will see how to derive the impact of the finite-size effects on the asymptotic key rate in the dedicated subsection 4.3.4.

Trusted versus untrusted receiver model. The transformation of the state between Alice and Bob's laboratory are used to quantify the action of Eve. However some effects occur in Bob's laboratory and as such cannot contribute to the information gained by Eve since she is assumed to only operate on the channel. This assumption is called the *trusted receiver model* and is particularly interesting since it considerably increases the performances of CV-QKD protocols. This model will be discussed further in the dedicated subsection 4.3.3.

This work. In this work we will focus on protocols using a discrete modulation because of their experimental simplicity. We will derive the security of our protocol against collective attacks in the

asymptotic regime. Also, we will focus on protocols using heterodyne detection, and consider we are in the trusted receiver model.

Unfortunately, security proofs do not yet permit to derive the security against coherent attacks or in the finite-size regime. For other protocols however, such as BB84 and GG02, we have been able to derive security in the general case by using a similar approach. In both cases, the security was first derived against collective attacks, following which a de Finetti reduction [45, 46] shows that this implies security against general attacks with a reasonable loss and that this is compatible with finite-size effects. We will discuss this further in subsection 4.3.4. It remains to be shown that this is also possible for protocols with discrete modulation, but this issue is outside the scope of this thesis. Hence we will limit ourselves to collective attacks and deal with the finite-size effects with a simple approach by computing the worst-case estimator for the excess noise.

4.2.2 Secret key rate

The secret key rate is given by the formula

$$K = f \times r, \tag{4.6}$$

where f is the symbol rate and r is the secret fraction *i.e.* the number of secret bits per symbol. The secret fraction in the case of collective attacks is given by a modified version of the Devetak-Winter formula [47] given by

$$r = \beta I(X,Y) - \sup_{\mathcal{N}_{A'\to B}} \chi(E,Y), \tag{4.7}$$

where $I(X,Y)$ is the mutual information between the classical variables X and Y resulting from Alice and Bob's measurements. $\chi(E,Y)$ is the Holevo information between Eve's subsystem and Bob's result and the supremum is taken over all possible channels from Alice to Bob compatible with the data observed by Alice and Bob. The prefactor β represents the imperfect reconciliation between Alice and Bob and is typically taken equal to 0.95 [48].

Mutual information. The mutual information term depends on the distributions of X and Y. In the GG02 no-switching protocol these both follow a complex Gaussian distributions such that the mutual information is given by

$$I(X,Y) = \log_2(1 + \mathrm{SNR}). \tag{4.8}$$

Here the term SNR is the signal-to-noise ratio given by $\mathrm{SNR} = \frac{TV_A}{2(1+\xi_{tot})}$, where V_A is the modulation variance used by Alice on her quadratures, T is the channel transmittance and ξ_{tot} is the total noise above the shot-noise. Note this expression is normalized by the value of the shot-noise, which explains the presence of the unity contribution in the denominator.

For protocols using a discrete set of states, the mutual information is different. However in the low SNR regime, which is the case for quantum communications, the Gaussian mutual information is a good approximation. Hence we will use this expression for the mutual information in our protocol.

Holevo information. To compute the Holevo information term, it is convenient to assume that Eve holds a purification of the state $\hat{\rho}_{AB}$ shared by Alice and Bob. Eve's register is introduced by the isometric representation of the quantum channel $\mathcal{U}_{A'\to BE}$ in the EB scenario such that we can write the tripartite state $\hat{\rho}_{ABE}$ shared between Alice Bob and Eve as

$$\hat{\rho}_{ABE} = \left(\mathrm{id}_A \otimes \mathcal{U}_{A'\to BE}\right)\left(|\Psi\rangle\langle\Psi|_{AA'}\right). \tag{4.9}$$

Then we use a very useful tool known as the *extremality property of Gaussian states* [49] which states that the supremum in equation 4.7 is upper bounded by the Holevo information computed for the Gaussian state $\hat{\rho}^G_{ABE}$ with the same covariance matrix then the state $\hat{\rho}_{ABE}$. We note $\chi^G(E,Y)$

this value. Since Eve holds an arbitrary purification of $\hat{\rho}_{AB}$, this means that Holevo information we want to compute is bounded by a function of the covariance matrix of the bipartite state $\hat{\rho}_{AB}$.

We compute the Holevo information using a universal purification analysis which stems from the fact that since Eve holds a purification of $\hat{\rho}_{AB}$, the Von Neumann entropy of her subsystem matches the Von Neumann entropy of Alice and Bob's subsystem (see properties of the Von Neumann entropy in chapter 2). Hence we can write that

$$\begin{aligned} S(\hat{\rho}_E) &= S(\hat{\rho}_{AB}), \\ S(\hat{\rho}_{E|Y}) &= S(\hat{\rho}_{A|Y}). \end{aligned} \tag{4.10}$$

In the next section, we derive the Holevo information for the GG02 protocol and for discrete modulations using this second technique. The first technique will come in use later when we will discuss the trusted noise model.

4.3 Derivation of the Holevo information

The Holevo information only depends on the covariance matrix of the state $\hat{\rho}_{AB}$ in the EB version of the protocol. Since we implement the PM version experimentally, we need to find the covariance matrix Γ_{AB}^{EB} from the measured covariance matrix Γ_{AB}^{PM}. We know how to do this easily in the case of the GG02 protocol, since it is indistinguishable from the EB protocol using two-mode squeezed vacuum states. However, we will see that this problem is more involved for discrete modulations.

4.3.1 The GG02 protocol

A nice property of the GG02 protocol is that Gaussian attacks are optimal for Eve [50]. This implies that the channel $\mathcal{N}_{A'\to B}$ can be taken as the Gaussian channel, here with transmittance T and noise ξ_{tot}. This allows us to explicitly compute the covariance matrix of Alice and Bob which is given in the PM scenario with heterodyne detection by

$$\Gamma_{AB}^{PM} = \begin{pmatrix} V_A \mathbb{1}_2 & \sqrt{\frac{T}{2}} V_A \mathbb{1}_2 \\ \sqrt{\frac{T}{2}} V_A \mathbb{1}_2 & \left(\frac{T}{2} V_A + 1 + \frac{\xi_{tot}}{2}\right) \mathbb{1}_2 \end{pmatrix}. \tag{4.11}$$

On the other hand the covariance matrix of the equivalent EB protocol where Alice prepares a two-mode squeezed vacuum state is

$$\Gamma_{AB}^{EB} = \begin{pmatrix} V \mathbb{1}_2 & \sqrt{T}\sqrt{V^2-1}\sigma_z \\ \sqrt{T}\sqrt{V^2-1}\sigma_z & \left(T(V-1) + 1 + \xi_{tot}\right) \mathbb{1}_2 \end{pmatrix} = \begin{pmatrix} a\mathbb{1}_2 & c\sigma_z \\ c\sigma_z & b\mathbb{1}_2 \end{pmatrix}, \tag{4.12}$$

where $V = V_A + 1$. The components of Γ_{AB}^{PM} are computed during the parameter estimation phase of the GG02 protocol following what the covariance matrix Γ_{AB}^{EB} is inferred. Then $S(\hat{\rho}_{AB})$ can be computed from equation 2.33 and the symplectic eigenvalues Γ_{AB}^{EB} given by

$$\lambda_{1,2} = \frac{1}{2}[\sqrt{(a+b)^2 - 4c^2} \pm (b-a)]. \tag{4.13}$$

The second term of the Holevo information $S(\hat{\rho}_{A|Y})$ is computed from the covariance matrix of the state held by Alice conditioned by Bob's measurement. We note this matrix $\Gamma_{A|Y}$ which we compute using equation 1.111 in the case of heterodyne detection. In this case the post-measurement covariance matrix is given by

$$\Gamma_{A|Y} = a\mathbb{1}_2 - \frac{c^2}{b+1}\mathbb{1}_2. \tag{4.14}$$

The symplectic eigenvalue of this matrix is

$$\lambda_3 = a - \frac{c^2}{b+1}. \tag{4.15}$$

Finally the Holevo information can be computed as

$$\chi^G(E,Y) = G\left(\frac{\lambda_1 - 1}{2}\right) + G\left(\frac{\lambda_2 - 1}{2}\right) - G\left(\frac{\lambda_3 - 1}{2}\right). \tag{4.16}$$

4.3.2 Discrete modulations

Discussion. The GG02 protocol is very convenient because it is easy to link the prepare-and-measure version of the protocol to an equivalent entanglement-based version used to derive the security of the protocol. In addition the optimality of Gaussian attacks allows us to suppose that $\mathcal{N}_{A'\to B}$ is the Gaussian channel allowing us to explicit the covariance matrix Γ_{AB}^{EB}. Unfortunately transitioning from the PM to the EB picture for protocols using a discrete modulation is more difficult, and since Gaussian attacks are not known to be optimal we cannot in general write the covariance matrix Γ_{AB}^{EB} and bound the key rate.

New security proofs have solved this issue by formulating the problem as a semidefinite program (SDP) [51, 52], where some convex function is minimized over the set of all possible quantum states compatible with the observations made in the PM protocol. Such numerical methods can provide reliable bounds on the key rate at the cost of intensive computations which scale with the number of discrete states used in Alice's modulation. Hence computing key rates when using 64 states in the random walk distribution seems complicated.

Recently, the work in [48] has developed an analysis of their semidefinite program to provide an analytical bound to the numerical optimisation problem, circumventing the need for the numerical optimisation and therefore providing bounds to the keyrate for any modulation format.

A question remains in the case of the four state protocol of why the explicit rate derived in [48] is much more pessimistic than the numerical results of [52]. Surely the differences in the objective functions used in the respective SDPs plays a role, and perhaps the explicit bound in reference [48] is not tight in this case. Nonetheless the authors argue that the explicit bound converges towards the Gaussian key rate as the number of states in the random walk distribution increases, and provides the Gaussian key rate when Alice employs a Gaussian modulation, hence their explicit formula is necessarily tight for higher order modulations.

Our approach. In this work we will present two protocols implementing respectively the four state protocol and the protocol with 64 states in the random walk distribution. We began with the four-state protocol based on the results of [52] which yielded positive key rates in our case. Following this the work of [48] showed the advantage on the key rate of using higher order modulations and gave an explicit bound to compute it. Unfortunately their pessimistic results for the four-state protocol meant the key rate in our protocol collapsed to 0 using their proof.

Since we have two ways of deriving the key rate in the case of the four state protocol, we will be picky and use the results of [52] which is advantageous compared to [48]. However we will use the explicit key rate formula of [48] when scaling up to the random walk distribution. In the following, we will transpose the results of reference [48] to derive the explicit key rate, and we will briefly compare the results of both references for the four state protocol.

Explicit key rate for discrete modulation formats. The approach of [48] is to consider the covariance matrix of the bipartite state after transmission over the channel as

$$\Gamma_{AB} = \begin{pmatrix} V\mathbb{1}_2 & Z\sigma_z \\ Z\sigma_z & [T(V-1)+1+\xi_{tot}]\mathbb{1}_2 \end{pmatrix}, \tag{4.17}$$

where the covariance term Z is not known in general. Since the Holevo information is inversely proportional to Z, we can bound the Holevo information by minimizing Z. Before we give the result derived in [48], a few quantities need to be defined, which we do in the following.

We begin by writing the density matrix of the state generated by Alice, rebranded to τ from $\hat{\rho}_A$ to stick with the notations of [48]. Hence we have

$$\tau = \sum_{k=1}^{M} p_k \left|\alpha_k\right\rangle \left\langle\alpha_k\right|. \tag{4.18}$$

where $M = m^2$ is the number of states in the modulation, equal to 64 for us. Then a purification of the state τ is given by

$$\left|\Phi\right\rangle_{AA'} = \sum_{k=1}^{M} \sqrt{p_k} \left|\psi_k\right\rangle \left|\alpha_k\right\rangle, \tag{4.19}$$

where the states $\left|\psi_k\right\rangle$ are defined by

$$\left|\psi_k\right\rangle = \sqrt{p}_k \bar{\tau}^{-1/2} \left|\bar{\alpha}_k\right\rangle. \tag{4.20}$$

Here $\bar{\tau}^{-1/2}$ denotes the square-root of the Moore-Penrose pseudo-inverse of $\bar{\tau}$. One can check that the $\left|\psi_k\right\rangle$ form an orthonormal basis and that tracing out Alice subsystem in $\left|\Phi\right\rangle_{AA'}$ collapses the state to τ. Finally we define an operator a_τ which will be useful in the following and is given by

$$a_\tau = \tau^{1/2} \hat{a} \tau^{-1/2} \tag{4.21}$$

Lower bound on Z. We now state the main result of [48]. A lower bound to Z, denoted Z^*, is given by

$$Z^* = 2c_1 - 2\sqrt{w\left(n_B - \frac{c_2^2}{\langle n\rangle}\right)}, \tag{4.22}$$

where the two terms w and $\langle n\rangle$ are defined by modulation used by Alice and c_1, c_2 and n_B are determined by Bob's measurement results. These parameters are defined by

$$w = \sum_{k=1}^{M} p_k \left(\left\langle\alpha_k\right| a_\tau^\dagger a^\tau \left|\alpha_k\right\rangle - \left| \left\langle\alpha_k\right| a_\tau \left|\alpha_k\right\rangle \right|^2 \right), \tag{4.23}$$

$$\langle n\rangle = \sum_{k=1}^{M} p_k |\alpha_k|^2, \tag{4.24}$$

$$n_B = \mathrm{Tr}[\hat{\rho}_{AB} \hat{b}^\dagger \hat{b}], \tag{4.25}$$

$$c_1 = \frac{1}{2} \mathrm{Tr}\left[\hat{\rho}_{AB} \Big(\sum_{k=1}^{M} \left\langle\alpha_k\right| \bar{a_\tau} \left|\alpha_k\right\rangle \left|\psi_k\right\rangle \left\langle\psi_k\right| \otimes \hat{b} + \mathrm{h.c.} \Big) \right], \tag{4.26}$$

$$c_2 = \frac{1}{2} \mathrm{Tr}\left[\hat{\rho}_{AB} \Big(\sum_{k=1}^{M} \bar{\alpha}_k \left|\psi_k\right\rangle \left\langle\psi_k \otimes \hat{b}\right| + \mathrm{h.c.} \Big) \right], \tag{4.27}$$

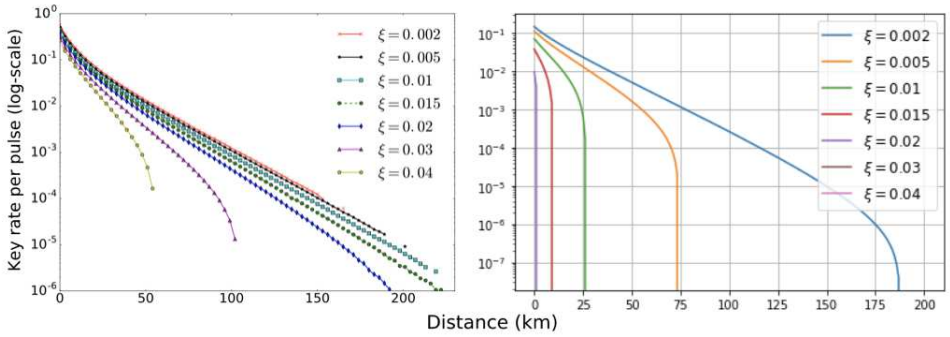


Figure 4.2: Secret key rates versus the distance for the four state protocol. (left) Results taken from [52] where the authors solve the SDP they define numerically. (right) Key rates obtained using the explicit lower bound to the covariance term defined in [48]. For both plots the value of α was optimized.

where the term h.c. in the last two expressions denotes the hermitian conjugate. Let us discuss these values. First w only depends on the state prepared by Alice in the PM version of the protocol. The mean value $\langle n \rangle$ is the mean photon number sent by Alice. The third term n_B is the variance of Bob's state. Finally, the terms c_1 and c_2 are linked to the first moment of the state measured by Bob. The values n_B, c_1 and c_2 can be determined experimentally in the following way.

During the protocol, for each state $|\alpha_k\rangle$ sent by Alice, Bob measures N complex values $\beta_{k,i}$ for $i \in \{1, .., N\}$. Let us note β_k the first moment of Bob's state defined by

$$\beta_k = \mathrm{Tr}[\hat{\rho}_k \hat{b}], \tag{4.28}$$

where $\hat{\rho}_k = \mathcal{N}_{A' \to B}(|\alpha_k\rangle \langle \alpha_k|)$. Bob builds the estimators for β_k and n_B as

$$\hat{\beta}_k = \frac{1}{N} \sum_{i=1}^{N} \beta_{k,i}, \qquad \hat{n}_B = \frac{1}{N} \sum_{k,i} p_k |\beta_{k,i}|^2 - 1. \tag{4.29}$$

In the limit of large N, we have that $\hat{\beta}_k \xrightarrow[N \to \infty]{} \beta_k$ and $\hat{n}_B \xrightarrow[N \to \infty]{} n_B$. Finally the values c_1 and c_2 are given by

$$c_1 = \mathrm{Re}\left(\sum_{k=1}^{M} p_k \overline{\langle \alpha_k \, |a_\tau| \, \alpha_k \rangle} \beta_k \right), \tag{4.30}$$

$$c_2 = \mathrm{Re}\left(\sum_{k=1}^{M} p_k \bar{\alpha}_k \beta_k \right). \tag{4.31}$$

and can be computed using the estimator $\hat{\beta}_k$ instead of β_k. Once the 5 values have been computed and Z^* determined, we bound the Holevo information by computing $\chi^G(E, Y)$ in the same way than for the GG02 protocol.

Comparison of the key rates in references [52] and [48]. In the figure 4.2, we show on the left plot the key rates obtained numerically via the SDP defined in reference [52]. On the right we plot the key rates obtained using the method of [48] described above and with the same parameters.

Note that the excess noise parameter ξ is defined at the channel input rather than at the channel output, hence the value ξ_{tot} we used in our analysis is related to the parameter ξ as $\xi_{tot} = T\xi$ where T is the channel transmittance.

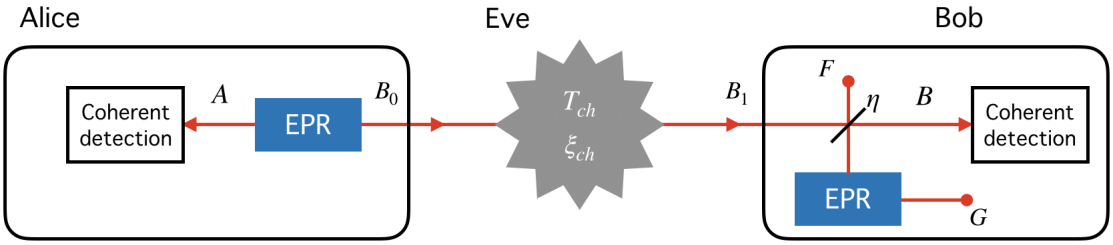


Figure 4.3: Trusted receiver model. The detection losses and noise are modelled by mixing an EPR states with Bob's mode in his laboratory.

It is clear from the comparison that the key rates obtained in [52] are more advantageous : a positive key rate over 50 km is possible with $\xi = 0.04$ while using the explicit bound method the maximal distance is about 7 km when $\xi = 0.015$. Hence we will use their results for our four state protocol implementation.

4.3.3 Trusted receiver model

The Holevo information leaked to Eve increases as the excess noise increases and as the transmittance of the channel decreases. This can be intuitively understood as the fact that the excess noise quantifies the interaction of the eavesdropper on the quantum states, and that all the losses are given to Eve so that she can gain information.

In a real experiment however, there are some constant noise sources and losses that occur in Bob's lab and therefore cannot be caused by Eve. This is the case for the losses in Bob's detection apparatus and the electronic noise in Bob's detectors. In addition the electronic noise is the dominant excess noise contribution and greatly deprecates the key rate when assumed to be caused by the actions of Eve.

Therefore it is interesting to define a model taking into account the fact that Eve cannot have induced the receiver losses and noise. In this scenario we want to rewrite the excess noise and the transmittance as :

$$T = T_{ch}\eta, \tag{4.32}$$

$$\xi_{tot} = \eta\xi_{ch} + \nu_{el}, \tag{4.33}$$

where T_{ch} and ξ_{ch} are the transmittance and excess noise of the channel, *i.e.* caused by Eve, and η and ν_{el} are the the transmittance and noise of the receiver. We call this the trusted receiver model and explain how to compute the Holevo information in this new setting.

Universal purification analysis In the trusted receiver scenario the receiver noise and losses are not due to Eve, hence do not contribute to the Von Neumann entropy $S(\hat{\rho}_E)$ of Eve's subsystem in the pure tripartite state after the channel transmission $\hat{\rho}_{AB_1E}$. They will however impact Bob's measurement result and therefore Eve's Von Neumann entropy $S(\hat{\rho}_{E|Y})$ conditioned on Bob's result. We model this by attributing the receiver noise and losses to the mixing of one mode of an EPR state of variance W_{rec} with the mode B_1 incoming to Bob's laboratory on a beamsplitter of transmissivity η. This is depicted in figure 4.3. We denote by $\hat{\rho}_{F'G}$ the EPR state in Bob's lab modelling receiver noise and $\hat{\rho}_{AB_1}$ the state shared by Alice and Bob after transmission and before Bob's detection apparatus. The total state at this point can be written as a tensor product of two states

$$\hat{\rho}_{AB_1F'G'} = \hat{\rho}_{AB_1} \otimes \hat{\rho}_{F'G}, \tag{4.34}$$

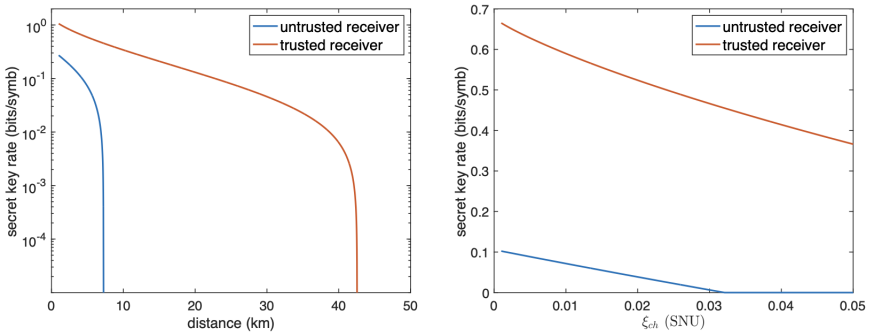


Figure 4.4: We compare the key rates obtained in the trusted receiver scenario compared to the "paranoid" model for the GG02 protocol. (left) key rate versus distance with $\xi_{ch} = 0.01$. (right) key rate versus ξ_{ch} at 5 km. Other parameters were taken equal to : $V_A = 5$, $\nu_{el} = 0.1$, $\eta = 0.9$.

and the total covariance matrix is given by the direct sum $\Gamma_{tot} = \Gamma_{AB_1} \oplus \Gamma_{F'G}$. Since Eve hold a purification of $\hat{\rho}_{AB_1}$ we have that $S(\hat{\rho}_E) = S(\hat{\rho}_{AB_1}$ which is computed from the covariance matrix of Alice and Bob's subsystem given by

$$\Gamma_{AB_1} = \begin{pmatrix} V\mathbb{1}_2 & \frac{Z}{\sqrt{\eta}}\sigma_z \\ \frac{Z}{\sqrt{\eta}}\sigma_z & [T_{ch}(V-1)+1+\xi_{ch}]\mathbb{1}_2 \end{pmatrix}, \tag{4.35}$$

where the symplectic eigenvalues are computed following equation 4.13. In Bob's detection apparatus his mode B_1 is mixed on a beamsplitter $B_{B_1F'}(\eta)$ of transmissivity η with the mode F' of the EPR state modelling the receiver noise. The covariance matrix of the resulting state $\hat{\rho}_{ABFG}$ is given by

$$\Gamma_{ABFG} = \big(\mathrm{id}_A \oplus B_{B_1F'}(\eta) \oplus \mathrm{id}_G\big)\Gamma_{AB_1F'G}\big(\mathrm{id}_A \oplus B^T_{B_1F'}(\eta) \oplus \mathrm{id}_G\big). \tag{4.36}$$

We will omit writing explicitly the covariance matrix since it is rather bulky. Looking at the variance V_B of Bob's mode we find the value of W_{rec} compatible with the receiver losses η and noise ν_{el} given by

$$W_{rec} = \frac{\nu_{el}}{1-\eta} + 1. \tag{4.37}$$

In order to derive the post-measurement covariance matrix, we rearrange Γ_{ABFG} so that Bob's mode is on the bottom right which gives a matrix of the form

$$\Gamma_{AFGB} = \begin{pmatrix} \Gamma_{AFG} & \Gamma_C \\ \Gamma_C^T & V_B \end{pmatrix}. \tag{4.38}$$

Then the post heterodyne measurement covariance matrix is given by equation 1.111 as

$$\Gamma_{AFG|Y} = \Gamma_{AFG} - \frac{1}{V_B+1}\Gamma_C\Gamma_C^T. \tag{4.39}$$

The term $S(\hat{\rho}_{E|Y})$ is given by the symplectic eigenvalues of this covariance matrix following equation 2.33. In figure 4.4 we compare the key rates obtained in the paranoid model where the receiver is not trusted and in the case where the receiver is trusted. These plots illustrate how the trusted receiver model can greatly increase the performances of the protocols, and is almost systematically considered valid in CV-QKD experiments.

4.3.4 Finite-size effects

To discuss the finite-size regime, we must first define the notion of composable security.

Composable security. The notion of *composable-security* was introduced in the field of QKD by Renner [53] based on the framework developed by Canetti [54] for classical cryptography. The idea is view the protocol as completely-positive trace-preserving map taking as input state an arbitrary input state $\hat{\rho}_{A^N B^N}$ composed of N quantum systems and outputting a state $\hat{\rho}_{S_A S_B E}$ composed of Alice and Bob's final key and of Eve's subsystem. Then the security of the protocol is derived by quantifying the security of the protocol by the distance of the real protocol to the ideal protocol. This term is denoted ϵ and in the context of QKD is taken as the trace distance between the two protocols. Then the protocol is said to have ϵ-*security*. Note the security in this framework is said to be composable because if two protocols with security parameters ϵ_1 and ϵ_2 are used together, the resulting protocol will have security $\epsilon \leq \epsilon_1 + \epsilon_2$.

In our case, the ideal protocol can be seen as the state $\hat{\tau} \otimes \hat{\rho}_E$ where $\tau = \frac{1}{2^\ell} \sum_{s \in \{0,1\}^\ell} |s, s\rangle \langle s, s|_{AB}$ describes a uniformly chosen secret key of length ℓ shared by Alice and Bob and the tensor product shows that Eve is completely decorrelated from Alice and Bob's system. Then the security parameter of the protocol is given by bounding the trace distance

$$\frac{1}{2} || \hat{\rho}_{S_A S_B E} - \hat{\tau}_{SS} \otimes \hat{\rho}_E || = \epsilon, \tag{4.40}$$

for any input state $\hat{\rho}_{A^N B^N}$. Composable security is particularly relevant when considering finite-size effects because the security definition takes into account the number N of states exchanged by Alice and Bob. The approach to prove the finite-size security of QKD is to compare three key rates which are

- $r_\epsilon(N)$: the secret key rate of the protocol with ϵ-security against general attacks, *i.e.* for an arbitrary input state $\hat{\rho}_{A^N B^N}$.
- $r_\epsilon^{\text{coll}}(N)$: the secret key rate of the protocol with ϵ-security against collective attacks, *i.e.* for an input states of the form $\hat{\rho}_{AB}^{\otimes N}$.
- r : the secret key rate computed with the Devetak-Winter formula, which we used for the GG02 protocol and the discrete modulation format protocol. This amounts to computing the key rate for collective attacks in the asymptotic regime.

The idea behind the security proofs of CV-QKD in the finite-size setting is to first compute r, then show that we have $r_{\epsilon'}(N) \approx r_\epsilon^{\text{coll}}(N) \approx r$ for some reasonable value of N and some security parameters ϵ and ϵ'. This has been done for the GG02 protocol in reference [46].

Simple approach to finite-size effects. Here we will adopt the approach derived in reference [55] to deal with the finite-size effects in the case of the GG02 protocol. We begin by defining the security parameter

$$\epsilon = \epsilon_{\text{PE}} + \epsilon_{\text{EC}} + \epsilon_{\text{PA}} + \bar{\epsilon}, \tag{4.41}$$

which is the sum of the security parameters of the different steps of the protocol. Here PE refers to the parameter estimation, EC to the error correction, and $\epsilon_{\text{PA}} + \bar{\epsilon}$ are virtual parameters linked to the privacy amplification. The key rate in the finite-size regime is given by

$$r_\epsilon^{\text{coll}}(N) = \frac{n}{N} \big(\beta I_{AB} - \chi^G_{\epsilon_{\text{PE}}}(E, Y) - \Delta(n) \big). \tag{4.42}$$

The terms in this expression are the following. N is the total number of states exchanged during the protocol and n is number of states used to derive the key, $\chi^G_{\epsilon_{\text{PE}}}(E, Y)$ is the maximum of the Holevo information compatible with the data except for probability ϵ_{PE} and $\Delta(n)$ is the penalty from the privacy amplification step. These two last terms are computed as follows.

- $\chi^G_{\epsilon_{\rm PE}}(E,Y)$ is computed by using the worst case estimator for the excess noise ξ_{tot}. To derive this term we must consider how the excess noise is estimated during the protocol. Consider $\mathrm{Var}(P_B, Q_B)$ is the variance of Bob's P or Q quadrature which can be written as

$$\mathrm{Var}(P_B, Q_B) = \frac{T}{2} V_A + 1 + \xi_{tot}. \tag{4.43}$$

Taking the conditional variance of Bob's data given the state sent by Alice we obtain

$$\mathrm{Var}(P_B, Q_B|(P_A, Q_A)) = 1 + \xi_{tot} = \sigma^2. \tag{4.44}$$

During the protocol we build an estimator $\hat{\sigma}^2$ for σ^2 the precision of which depends on the number of states $m = N - n$ used in the parameter estimation phase. We can compute the worst case estimator for σ^2, except with probability $\epsilon_{\rm PE}$, from the estimator $\hat{\sigma}^2$ as

$$\sigma^2_{\max} \approx \hat{\sigma}^2 + z_{\epsilon_{\rm PE}/2} \frac{\hat{\sigma}^2\sqrt{2}}{\sqrt{m}}, \tag{4.45}$$

where $z_{\epsilon_{\rm PE}/2}$ obeys the relation $1 - \mathrm{erf}\left(z_{\epsilon_{\rm PE}/2}/\sqrt{2}\right)/2 = \epsilon_{\rm PE}/2$ and the erf function is given by

$$\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt. \tag{4.46}$$

The worst case estimator for the excess noise is $\hat{\xi}_{tot,max}$ is computed as $\sigma^2_{max} - 1$, and is increased by a factor $\Delta\xi = z_{\epsilon_{\rm PE}/2} \frac{\hat{\sigma}^2\sqrt{2}}{\sqrt{m}}$ compared to the excess noise estimator $\hat{\xi}_{tot}$.

- The penalty term $\Delta(n)$ is given by

$$\Delta(n) = 7\sqrt{\frac{\log_2(2/\bar{\epsilon})}{n}} + \frac{2}{n}\log_2\left(1/\epsilon_{\rm PA}\right), \tag{4.47}$$

where $\bar{\epsilon}$ and $\epsilon_{\rm PA}$ should be optimized but still satisfy equations (4.41) and (4.47). In the limit of large n we see that the penalty is dominated by the square-root term, thus

$$\Delta n \approx 7\sqrt{\frac{\log_2(2/\bar{\epsilon})}{n}}. \tag{4.48}$$

4.4 Comparison with DV-QKD

In this section we discussed in depth CV-QKD protocols. We derived their secret key rate in the asymptotic limit against collective attacks, and gave some insight as to how the security in a realistic setting again general attacks could be derived. A question that remains is to know how does this technology compare to DV-QKD. We discuss the relevant comparison points in this section in order to shed light on the respective strengths of DV- and CV-QKD.

4.4.1 Security proof

In comparison with CV-QKD, DV-QKD protocol have more mature security proofs. For CV-QKD, we can only prove the full security in the general setting of the GG02 no-switching protocol. Other PM protocols, such as those using discrete modulation formats, do not yet have a security proof in the full setting and this remains an open question in the field. On the other hand full security proofs for DV-QKD protocols have been found for a while now [56, 45].

Moreover, even when considering the GG02 protocol, the correction term giving the key rate $r_\epsilon(N)$ from r is lower for DV-QKD protocols. Therefore they occur less penalty than CV-QKD protocols in the finite-size regime. This is because the correction term is greatly correlated to the security proof used to extend the security to the general setting, and a more mature security proof is available for DV-QKD. Note however that we can observe similar trends in both CV- and DV-QKD as is explained in reference [48]. In DV-QKD the first security proofs for the general setting were first based on a de Finetti theorem [56], then on a de Finetti reduction [45], then on the entropic uncertainty principle [57] and finally on the entropy accumulation theorem [58]. The security proofs of the GG02 no-switching protocols have followed a similar trend where first a de Finetti theorem was found [59] then a de Finetti reduction [46]. It is therefore tempting to believe that the CV-QKD security proofs will continue to improve and that they will apply to discrete modulation formats.

4.4.2 Rate versus distance

DV-QKD protocols champion the point-to-point communication distance, where secure key rates have been obtained over the incredible distance of 421 km [60] using ultralow-loss fiber, and other works have consistently demonstrated positive key rates beyond 250km [61, 62, 63] using regular fiber. On the other hand CV-QKD protocols have been shown to provide secret keys up to a record distance of 202 km [64] using ultralow-loss fiber, doubling the previous record of 100 km [65].

This is partly explained because the key rate expression for DV-QKD protocols depends only on the QBER. Mostly errors in DV protocols are caused by the combination of a photon loss and a dark count in the SPDs, but these are typically reduced by cooling the detectors to low temperatures ranging from -30°C for avalanche photodiode (APD) SPDs [61] to 4 K for superconducting nanowire (SN) SPDs[66, 62], which enables long distance key distillation. On the other hand the losses in CV-QKD protocols directly contribute to Eve's information as can be intuitively seen from the entangling cloner attack, for which higher channel losses amount to a more aggressive probing of the quantum states by Eve.

Concerning the secret key rate, the main limitations for DV-QKD is detector dead time, the time after detection of a photon during which the detector cannot detect another. State of the art dead time is found in SNSPDs cooled to cryogenic temperatures which can achieve a $\sim$ 10 ns dead time corresponding to a maximal detection rate of 100 MHz. On the other hand the electronics of CV-QKD systems closely resembles the technology used for classical telecommunications for which symbol rates of over 50 Gbaud can be detected. The main challenge for receivers designed for CV-QKD is to allow for high rates while having enough gain to detect the weak coherent states and sufficiently small receiver noise. At the moment, CV-QKD experiments have already been demonstrated with symbol rates of 1 Gbaud [67] and recently shot-noise limited balanced receivers with 20 GHz bandwidth have been built [68]. Therefore it is certain that over short-distances CV-QKD protocols will outperform DV-QKD protocols.

Choosing DV- or CV-QKD solutions should be done as to maximise the secret key rate for the desired application which greatly depends on the distance of communication. A rule of thumb considering the current state of the art is that CV-QKD protocols will be preferred over shorter distances ($<$25 km) while DV-QKD protocol will perform over longer distances where CV protocols cannot. However the field of QKD is constantly improving and it will be interesting to monitor how CV- and DV-QKD overcome their respective limitations.

4.4.3 Cost

For QKD technology to be deployed in real world applications it is necessary to design cost-effective systems. In this scope CV-QKD hardware is typically cheaper because it can be operated at room temperature.

Other efforts in this direction have led to investigating the coexistence of QKD systems with classical channels. The reason behind this is because dark fiber that can be dedicated to QKD is scarce and very expensive. On the other hand, the classical telecom network composed of lit fibers is readily available as most metropolitan homes enjoy internet access via optical fibers and data centers a typically linked by optical fibers.

An review of experimental QKD systems deployed over classical wavelength division multiplexing (WDM) channels is given in [16]. By nature, CV-QKD protocols are more resilient to adjacent classical channels because of the coherent detection process, which is spectrally selective [69]. Hence CV-QKD has been shown to tolerate more noise than DV-QKD systems [70] and to coexist with up to 100 classical channels carrying data a rate 18.3 Tbit/s [71] although only over 10 km. In comparison DV-QKD systems are more sensitive to classical channels because the SPDs can produce random clicks -and generate errors- because of the noise photons from the classical channels. DV-QKD systems therefore require strong filtering techniques in order to coexist with WDM channels and for the moment this has, to the best of our knowledge, only been done with a launch power below the nominal launch power of 0 dBm for classical systems [72].

It remains an interesting engineering challenge to enable QKD systems over a distance equivalent to the typical optical fiber span, *i.e.* 80 km, alongside classical channels at nominal launch power. Positive results would greatly contribute to large scale deployment of QKD.

This marks the end of this chapter and also of the first part of this manuscript. Here we gave here an in-depth view of CV-QKD protocols. We covered the security proofs of the GG02 protocol as well as the more recent results for discrete modulation formats, which will be used later for our CV-QKD protocol implementation. We also discussed the different security assumptions when the receiver noise is trusted and when only a finite number of quantum states are exchanged between Alice and Bob. In the second part of this work we will begin with a general chapter on coherent communications before diving into the core of the work accomplished during this thesis.

Part II

Convergence of classical and quantum coherent communications

Chapter 5

Quantum and classical coherent communications

Contents

We begin the second part of this manuscript with a general chapter on the topic of coherent communications in practice. We will covert the experimental aspects of signal generation, propagation and detection. Then we will discuss the digital signal processing routine which translates the sampled signal into the set of measured symbols. In general the notions developed in this chapter apply to both classical and quantum coherent communications. In the last section, we will discuss some implementation challenges facing specifically quantum coherent communications and position our work relative to the issues raised here.

5.1 Symbol generation

The first part of any coherent communication protocol is to be able to generate the desired signal at the transmitter. We describe how this is done here.

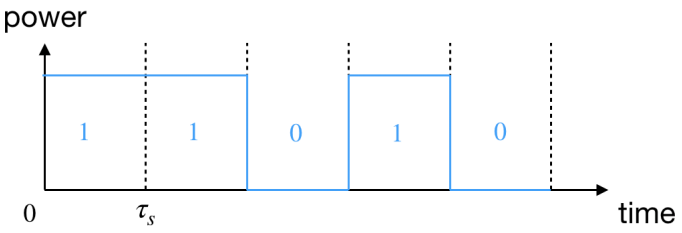


Figure 5.1: Temporal representation of the OOK modulation. The bits 0 and 1 are encoded by the absence or the presence of light. The duration of a symbol is noted τ_s

5.1.1 Mapping bits to symbols

The principle of a communication protocol is to transfer a sequence of bits $B = \{b_i\}_{i=1}^{N_{bits}}$ from an transmitter, Alice, to a receiver, Bob. For this the sequence B is mapped to a sequence of symbols $S = \{\alpha_k\}_{k=1}^{N_{symb}}$ that will be transmitted over the channel. The symbols in S are drawn from an ensemble C whose cardinality determines the number of bits that are encoded in one symbol. This number is given by $\log_2 |C|$, therefore we have $N_{symb} = N_{bits}/\log_2 |C|$. The symbols are encoded on a *carrier*, a sine wave, which is the light emitted by a laser in the context of optical communications. The process of encoding the symbols on the carrier is called the *modulation*.

Example : On-Off Keying. The most basic form of modulation is On-Off Keying (OOK), where the bit 1 and 0 are encoded by the presence or absence of light respectively. A temporal representation of an OOK modulation is represented in the figure 5.1. The "light" and "no light" events are respectively mapped to the bits 1 and 0.

Using the phase to encode more bits per symbol. We can increase the number of bits per symbol, and thus the data rate, by using more complex modulation formats where the information is encoded on the amplitude and the phase, or equivalently on both quadratures, of the electromagnetic field. Such modulation formats are called Quadrature Amplitude Modulation (QAM). Compared to the OOK modulation format where a simple photodetector is enough to detect the signal, a coherent receiver is needed in the case of QAM modulation in order to recover both quadratures.

Typically the QAM modulations refer to the number of unique symbols in the ensemble C, such as 4-QAM (also called Quadrature Phase-Shift Keying or QPSK), 16-QAM or 64-QAM. For these modulation formats, the ensemble C is called the *constellation*. We represent different QAM constellations in the figure 5.2. We adopt in this section the notations of classical communications where the quadratures are noted I and Q for the in-phase and quadrature components respectively.

Probability constellation shaping. We discussed in chapter 4 the specific modulation format referred to as the random walk distribution. This type of format is inspired from probability constellation shaping QAM modulation formats (PCS-QAM) used in classical communications. The bit-to-symbol mapping in this case is not trivial since we want to be able to communicate any bit sequence using this format and it seems like the probability distribution of each symbol will affect the probability of given bit sequences associated to that symbol. Actually PCS-QAM modulations use a so-called *distribution matcher* which maps a long sequence of bits into a sequence of QAM symbols with the desired probability distribution. However this is outside the scope of this thesis and we will simply generate a QAM constellation with the desired probability distribution when we use these formats. We provide a representation of the probability distribution of the symbols in a PCS 64-QAM format with the random walk distribution in figure 5.3.

Choice of modulation format for classical and quantum coherent communications. In

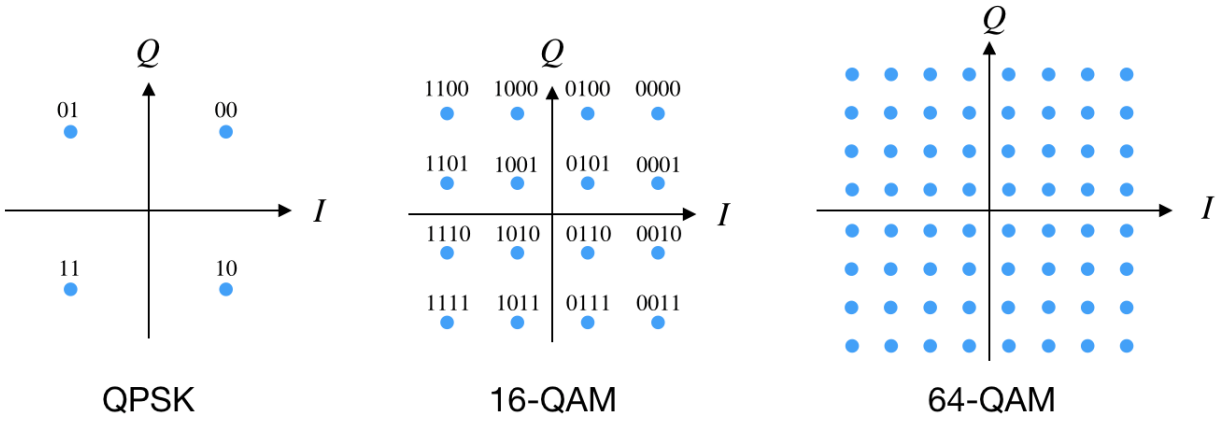


Figure 5.2: Different QAM constellations with the corresponding bit encoding for QPSK and 16-QAM

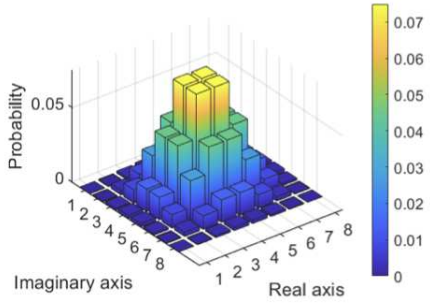


Figure 5.3: Representation of the probability of occurence of the symbols in a PCS 64-QAM format with a random walk distribution

classical coherent communications the choice of modulation format depends on the power that can be transmitted from Alice to Bob. Since higher order QAM modulation formats require more power to distinguish the symbols, QPSK modulation will be preferred for long-haul transmissions in the undersea cables while 64-QAM will be used over shorter distances such as WiFi applications. The OOK modulation is used for its simplicity on the optical fiber available to the public for internet connection.

For CV-QKD, the objective is to maximize the secret key rate and therefore to chose the modulation format which yields the highest key rate. This is then put in perspective with the implementation challenges of each format, and based on recent results the PCS-QAM format seems like a promising candidate for high key rates and simple processing.

5.1.2 The I/Q modulator

Once the mapping of bits to symbol is determined the next step is to physically modify the quadratures of the electromagnetic field to generate the desired symbol sequence. This is achieved by converting electrical signals generated on a device called an arbitrary waveform generator (AWG) into a modification of the light field using devices exploiting the Pockels effect. This effect appears in crystals lacking inversion symmetry such as lithium niobate ($LiNbO_3$) and gallium arsenide (GaAs) and consists in

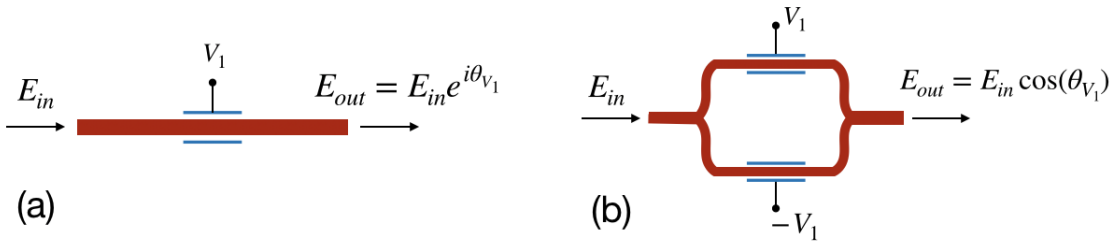


Figure 5.4: (a) The Pockels effect permits to modify the phase of the light by a factor θ_{V_1} proportionally to the voltage V_1 applied to the medium. (b) The Mach-Zehnder modulator is an inteferometer for which the amplitude of the output signal can be piloted by applying a voltage to the device.

the modification of the refractive index of a medium proportional to the electric field applied to the medium, therefore the phase of the output signal can be piloted by the voltage applied. We illustrate in figure 5.4.a how the Pockels effect modifies the phase of the signal by a phase θ_{V_1} proportional to the voltage V_1 applied to the medium.

Based on this the Mach-Zehnder modulator (MZM), depicted in figure 5.4.b, enables amplitude modulation of the input signal. In the MZM, the input signal is split on a 3-dB coupler and voltage $\pm V_1$ is applied to each branch. The signals in each branch interferes when they are recombined such that the output field E_{out} is related to the input field E_{in} by $E_{out} = E_{in}\cos(\theta_{V_1})$. It is common to denote by V_π the voltage difference between the two branches of the MZM for which the signal in each branch is dephased by a factor π. Then the input-output relation of the MZM is

$$E_{out} = E_{in}\cos\left(\frac{\pi}{2}\frac{V_1}{V_\pi}\right), \tag{5.1}$$

where we clearly see how tuning V_1 will modify the amplitude of the output signal.

Controlling the I and Q components of the light is done in the IQ modulator (IQM) depicted in figure 5.5.a. The input signal is split in two branches fed into two MZM with applied voltages V_1 and V_2. The signal on the second branch is shifted by a phase of $\pi/2$ such that the output of the IQM is given by

$$E_{out} = \frac{E_{in}}{2}\left(\cos(\frac{\pi}{2}\frac{V_1}{V_\pi}) + i\cos(\frac{\pi}{2}\frac{V_2}{V_\pi})\right). \tag{5.2}$$

Generally, we can write that $V_{1/2} = V_{\text{dc}} + V_{\text{mod},I/Q}$ where V_{dc} is a voltage bias applied to the IQ modulator and $V_{\text{mod},I/Q}$ is the voltage generated by the AWG on the I and Q optical paths. The voltage bias is set to V_π such that we have

$$E_{out} = \frac{E_{in}}{2}\left(\sin(\frac{\pi}{2}\frac{V_{\text{mod},I}}{V_\pi}) + i\sin(\frac{\pi}{2}\frac{V_{\text{mod},Q}}{V_\pi})\right). \tag{5.3}$$

For small $V_{\text{mod},I/Q}$ compared to V_π, we have that

$$E_{out} \propto \frac{E_{in}}{2}(V_{\text{mod},I} + iV_{\text{mod},Q}), \tag{5.4}$$

such that the quadratures of the output field are proportionnal to the applied voltage on their corresponding optical path.

Finally, dual-polarisation IQ modulator (DP-IQM) depicted in figure 5.5.b allows to pilot the I and Q components of the X and Y polarisation of the input light.

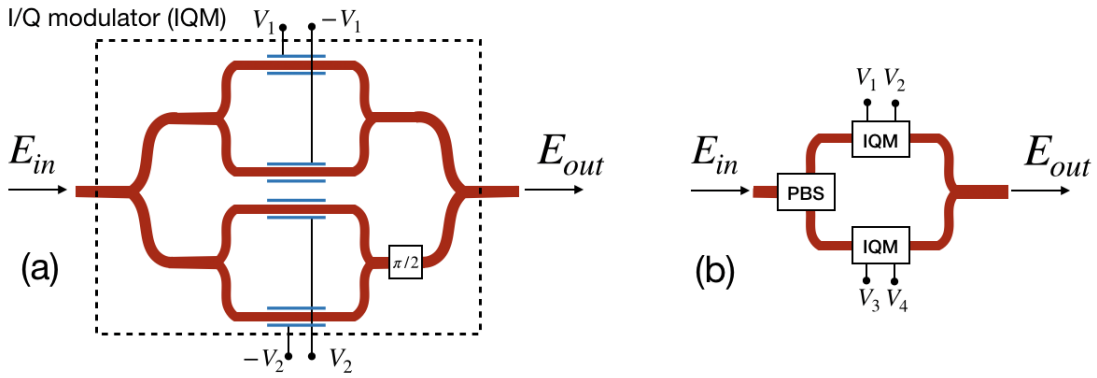


Figure 5.5: (a) The IQ modulator controls the amplitude of the real and imaginary parts of the light. The signal is split in two branches each fed to a MZM controlling the amplitude of the corresponding quadrature. The phase in the second path is shifted by $\frac{\pi}{2}$ to constitute the Q component. (b) A dual polarisation IQM first splits the incoming signal on a polarising beam splitter (PBS), then each polarisation is fed to an IQM.

5.1.3 Pulse shaping

Pulse shaping refers to the modification of the temporal and spectral distribution of the generated symbols in order to optimise the transmission over the channel. To see how this can be useful, let us consider the temporal signal corresponding the sequence S which can be written as

$$s(t_n) = \sum_{k=1}^{\infty} \alpha_k \Pi\left(\frac{t_n - kT_s}{T_s}\right), \tag{5.5}$$

where T_s is the duration of one symbol and Π is the door function defined by

$$\Pi(t_n) = \begin{cases} 0, & \text{if } |t_n| > \frac{1}{2} \\ \frac{1}{2}, & \text{if } |t_n| = \frac{1}{2} \\ 1, & \text{if } |t_n| < \frac{1}{2} \end{cases}. \tag{5.6}$$

The spectral representation of the signal is given by the Fourier transform of $s(t_n)$ and is given by the function $S(f) = \text{sinc}(fT_s) = \frac{\sin(\pi f T_s)}{\pi f T_s}$. The spectrum is represented in figure 5.6.

Notice the signal in this case spans over an infinite bandwidth which presents a couple drawbacks :

- The signal is not bandwidth efficient, and signals propagating at different frequencies will overlap. This can generate additional noise when signals are multiplexed in frequency.
- The detectors have a finite bandwidth therefore part of the signal will not be retrieved. Additionally the detection process will apply a spectral filter to the signal which can introduce inter-symbol interference (ISI).

Therefore it is desirable to apply some filter to the signal to reduce its bandwidth. By doing so, we will modify the time-domain representation of the signal thus one must verify that we do not introduce ISI. ISI occurs when several symbols overlap in the time domain and introduces noise. The criteria for mitigating ISI is the Nyquist criterion.

Definition 9 (Nyquist ISI criterion)**.** If the channel impulse response of the channel is $h(t_n)$, then the condition for mitigating ISI is :

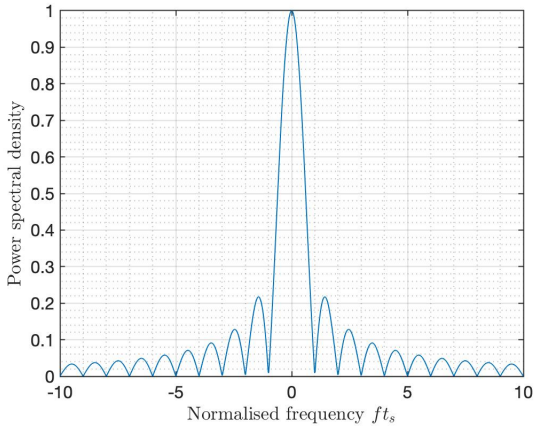


Figure 5.6: Power spectral density of QAM signals. The power spectral density is normalised by its maximum value in this plot.

$$h(nT_s) = \begin{cases} 1, & \text{if } n = 0, \\ 0 & \text{if } n \neq 0 \end{cases}. \tag{5.7}$$

where n is an integer and T_s is the symbol period. In the frequency domain the Nyquist criterion is equivalent to the condition

$$\frac{1}{T_s} \sum_{k=-\infty}^{+\infty} H\left(f - \frac{k}{T_s}\right) = 1 \quad \forall f, \tag{5.8}$$

where $H(f)$ is the Fourier transform of $h(t_n)$.

When designing spectral filters for the signal, we should keep in mind the Nyquist ISI criterion.

Raised cosine filter. The raised cosine filter is described in the frequency domain by the transfer function

$$H(f) = \begin{cases} 1, & |f| \leq \frac{1-\beta}{2T_s} \\ \frac{1}{2}\left[1 + \cos\left(\frac{\pi T_s}{\beta}\left[|f| - \frac{1-\beta}{2T_s}\right]\right)\right], & \frac{1-\beta}{2T_s} < |f| \leq \frac{1+\beta}{2T_s} \\ 0, & \text{otherwise} \end{cases}, \tag{5.9}$$

where β is the *roll-off factor*, a parameter ranging from 0 to 1 controlling the shape of the filter. The time-domain response of the raised cosine filter is

$$h(t_n) = \begin{cases} \frac{\pi}{4T_s}\,\mathrm{sinc}\left(\frac{1}{2\beta}\right), & t_n = \pm\frac{T_s}{2\beta} \\ \frac{1}{T_s}\,\mathrm{sinc}\left(\frac{t_n}{T_s}\right)\frac{\cos\left(\frac{\pi\beta t_n}{T_s}\right)}{1-\left(\frac{2\beta t_n}{T_s}\right)^2}, & \text{otherwise} \end{cases}. \tag{5.10}$$

One can check that the raised cosine filter satisfies the Nyquist ISI criterion. We represent the time and frequency response of the filter in the figure 5.7

Root raised cosine filter. In practical communications the optimal filter which maximises the SNR in presence of stochastic noise is the matched filter, where the same filter is applied at the transmitter and the receiver. Therefore, while the raised cosine filter is a suitable spectral filter, we

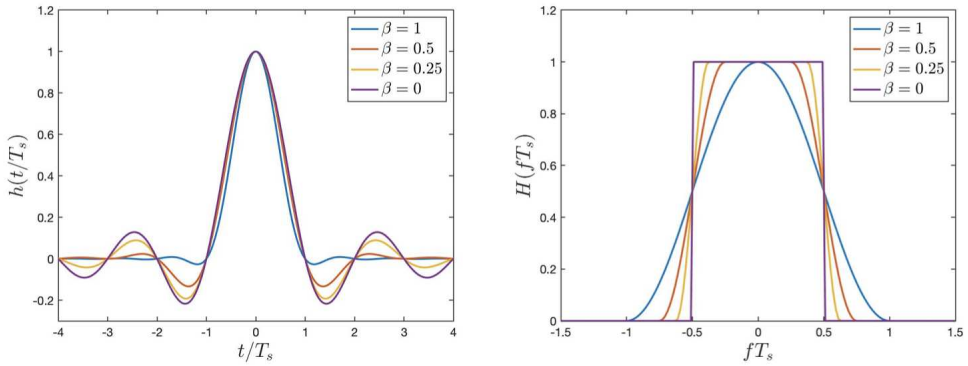


Figure 5.7: Time (left) and frequency (right) response of the raised cosine filter for different roll-off factors.

will prefer the root raised cosine filter (RRC) applied at Alice and at Bob's. The frequency response of the RRC filter is

$$H_{\text{RRC}}(f) = \sqrt{H(f)} \tag{5.11}$$

5.2 Signal distortions on the fiber

During propagation over the optical fiber, both classical and quantum signals undergo similar distortions which we review in this section. In the next section we will discuss how to compensate these using digital signal processing.

5.2.1 Structure of the fiber and losses

The fiber on which the light travels is depicted in figure 5.8. It is constituted of a core and a cladding, two waveguides built in silica, with the cladding having a refractive index slightly higher than the core. Around the cladding is a protective layer to protect the waveguides. Fibers can be categorized in two categories namely multi-mode fibers (MMF) and single-mode fibers (SMF). Based on the diameter of the core, the fiber can allow either several modes to propagate or only one, thus defining the fiber type as MMF or SMF. MMF fibers have a core that is typically $\sim 50 - 62.5\mu m$ while SMF have a core diameter of $9\mu m$. In this work we use SMF fibers.

Losses. The losses α in the fiber are often described in terms of dB/km and depends on the wavelength of the carrier wave. The output power is then written as

$$P_{out} = P_{in} \times 10^{-\frac{\alpha L}{10}}, \tag{5.12}$$

where P_{in} is the input power and L is the length of the fiber in km. In silica-based fibers, the minimal losses are reached when the laser wavelength is around 1550 nm and are of about 0.2 dB/km. In fact, wavelengths are categorised in different bands with the *Conventionnal Band*, or C-band, ranging from 1530-1565 nm. The C-band corresponds to the minimal absorption by the silica fiber but also the maximal gain from erbium doped fiber amplifiers, making the C-band the perfect wavelength for optical fiber communications.

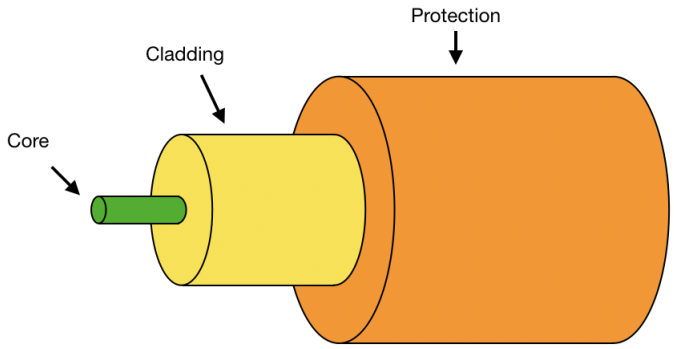


Figure 5.8: Representation of the optical fiber with the core, the cladding and the surrounding protection.

5.2.2 Polarisation rotation

Optical fibers are materials with an optical property called *birefringence*. This means that the refractive index of the material depends on the polarisation (and propagation direction) of light. The causes for this birefringence can be explained due to the slight asymmetry in the fiber core cross-section along the length. In addition, stress on the fiber -such as bending- will also create birefringence. In general the stress related birefringence dominates the geometrical one.

The effect of the birefringence is that the polarisation state at a given point in the fiber can be decomposed in a slow and a fast axis based on the local refractive index. As the light propagates over the fiber, the random rotation of the slow and fast axes will cause the polarisation of the light to rotate. For coherent communications, two independent signals are often multiplexed on orthogonal polarisation axes. Therefore polarisation rotation is a phenomenon that must be dealt with before retrieving the signals. Usually this can be done digitally using an adaptive equalizer, which we will discuss further in section 5.4. Note there also are physical components which allow us to control the polarisation state of the light.

- *Polarisation controller.* The polarisation controller permits manual tuning of the state of polarisation of light. It is constituted of a succession of three rotable waveplates in cascade: a quarterwave plate, a halfwave plate, a second quarterwave plate. We control the polarisation by rotating the waveplates.
- *Polarisation maintaining fiber.* The optical fiber can be built to intentionally generate stress along a specific axis of the fiber core, such that the fast and the slow axes are constant over the length of the fiber. Even under mild bends the axes should remain stable and therefore maintain the polarisation state. Several designs exist to build polarisation maintaining fiber which are represented in figure 5.9.

5.2.3 Perturbations from other channels

Several channels are often *multiplexed* in classical coherent communication links. This means that they co-propagate without interfering with each other "too much". This way several communication channels can coexist on a single fiber, increasing the total information throughput. Typically the multiplexing consists in attributing different central wavelengths to each channel and the communication link is called a wavelength division multiplexed (WDM) link. Unfortunately there is never a perfect isolation between multiplexed channels, therefore unavoidable perturbations from other channels occur in multiplexed communication channels. We review those which are relevant to this work here.

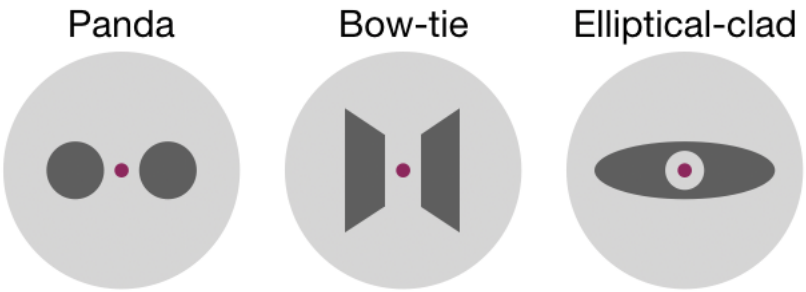


Figure 5.9: Cross-section of 3 different designs of polarisation maintaining fiber. Rods of a different material are built in the fiber cladding such that the stress applied on the core maintains the orientation of the slow and fast axis in the fiber. The rods are represented in darker tones of grey. The fiber core is in purple.

Cross-talk. The cross-talk is induced by channels in adjacent frequency slots which are never perfectly demultiplexed. Therefore there is always a fraction of the power in the adjacent channels which is transmitted.

Non linear effects. When the optical power in the fiber becomes to high, the response of the fiber becomes nonlinear. Such nonlinearities can be induced by the Kerr effect, causing the refractive index in the fiber to fluctuate as the square of the electric field. These result in several distortions such as self-phase modulation, cross-phase modulation and four-wave mixing. Other nonlinearities are induced by Raman scattering, where photons exchange energy with matter. The result is that the signal is scattered over several wavelengths. The nonlinear effects are the main limitation to the data rates achievable over long distance communications since they limit the optical input power.

5.2.4 Other effects

We discuss here other transformations light undergoes during propagation on the fiber. Specifically for our experiment over short distances, these do not play a role. However we mention them for the sake of completeness.

Chromatic dispersion. In the fiber, different wavelengths travel at different speeds. This phenomenon, referred to as chromatic dispersion, leads to pulse broadening and can create inter-symbol interference. Chromatic dispersion is quantified by the dispersion parameter expressed in ps/nm/km :

$$D = -\frac{2\pi c}{\lambda^2}\frac{d^2\beta}{d\omega^2} = \frac{2\pi c}{v_g^2\lambda^2}\frac{dv_g}{d\omega} \tag{5.13}$$

where c is the speed of light in vacuum, β is the propagation constant, λ the wavelength and v_g is the group velocity of the pulse. Compensation of chromatic dispersion in fiber communications can be achieved by propagating the signal in a dispersion compensating fiber or to pre-compensate the signal to account for chromatic dispersion.

Polarisation dependent loss and polarisation mode dispersion. The slow and fast axes of the fiber can undergo different losses resulting in polarisation dependent loss (PDL). PDL is defined by transmitting linearly polarised light and taking the ratio of the maximum transmitted power over the minimum transmitted power. Also, the birefringence in the fiber causes dispersion called polarisation mode dispersion (PMD).

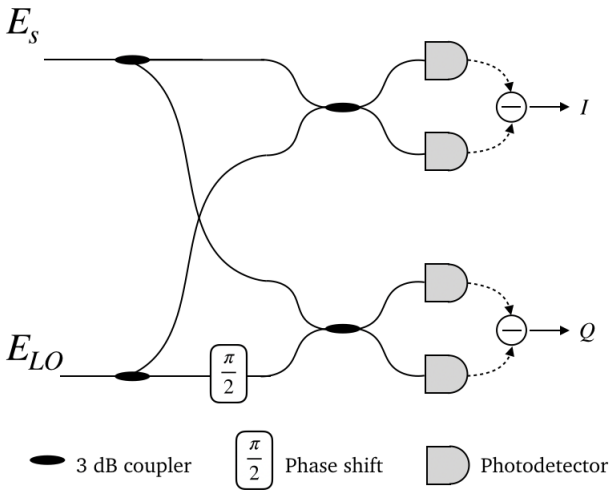


Figure 5.10: Schematic representation of the phase diversity hybrid. The detectors are not part of the hybrid but are represented here nonetheless.

5.3 Receiver architecture

After the generation and propagation of the symbols over the fiber, let us examine the receiver architecture allowing for coherent detection of the quadratures of the electromagnetic field.

5.3.1 Optical hybrids

The coherent detection process requires mixing the incoming signal with the local oscillator. This is done using a component called an *optical hybrid.*

Phase diversity hybrid. The phase diversity hybrid, or 90° hybrid, is the component which allows to measure both I and Q quadratures of the electromagnetic field. It takes the signal beam and the local oscillator as input and splits both beams in half. Then, one half of the signal is mixed with half of the local oscillator to detect the I quadrature and the other signal half is mixed with a $\pi/2$ dephased half of the local oscillator to detect the Q quadrature. The setup is represented in figure 5.10

Polarisation 90° diversity hybrid. The polarisation 90° hybrid allows the detection of the I and Q components of both polarisations. The signal is split on a polarising beamsplitter and each output is fed into a phase diversity hybrid. The LO is split in half and one half is transferred to each phase diversity hybrids. The Polarisation 90° optical hybrid is depicted in figure 5.11.

5.3.2 Detectors

Each quadrature is measured by a balanced receiver which is depicted in figure 5.12. It is constituted of two photodiodes generating a current based on the incoming optical power. The current generated by both photodiodes is substracted and then converted to a voltage on a transimpendence amplifier (TIA). Let us discuss the relevant characteristics which defined a balanced receiver.

Bandwidth. The bandwidth of the detector must be chosen according to the desired use. Typically detectors used for classical communications have a larger bandwidth than the detectors used

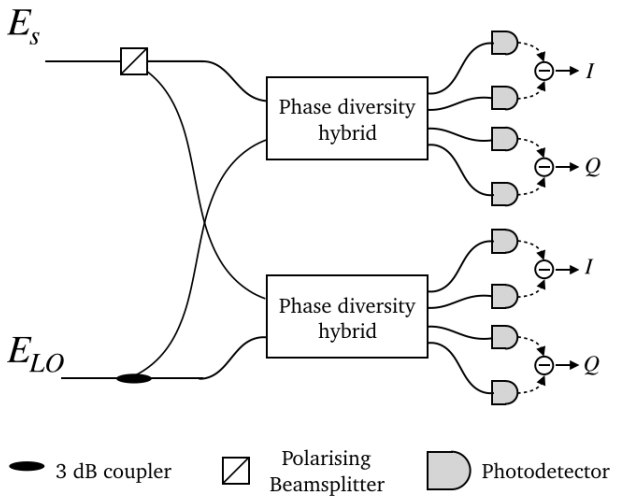


Figure 5.11: Schematic representation of the polarisation diversity hybrid.

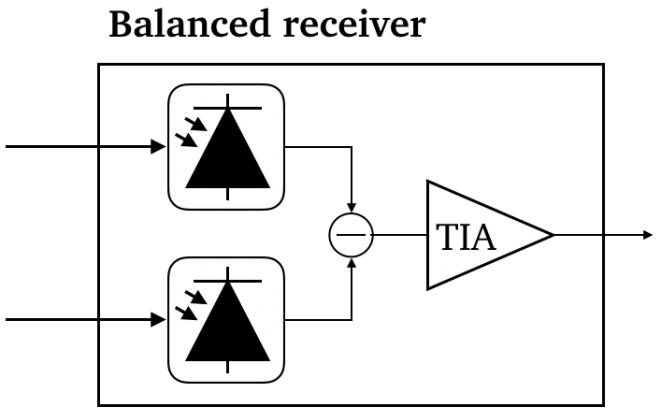


Figure 5.12: The balanced receiver subtracts the photocurrent generated by the photodectectors to retrieve the I or Q quadrature. TIA is the transimpedence amplifier which converts the current output by the photodiodes into a voltage.

for quantum communications. This is because high bandwidth detectors display a higher NEP (see below), a measure of the thermal noise of the receiver, which must be as low as possible for quantum communications.

Noise equivalent power (NEP). The NEP is a measure of the minimal input power to obtain an output SNR of 1. It is a measure of the noise floor of a detector as well as its sensibility. For QKD, it is crucial to choose detectors with low NEP to reduce the electronic noise.

Wavelength range. The photodiodes convert optical power into a current. Depending on the materials used in the construction of the photodiodes, they are sensitive to different optical wavelengths. For fiber based communications, one usually prefers photodiodes operating around the 1550 nm wavelengths.

Responsivity. The photodiode responsivity R_λ at wavelength λ measures the ratio of electrical current generated over the optical power on the photodiodes. It is expressed in A/W and quantifies the efficiency of the detection. The quantum efficiency Q_λ is a value used to quantify the number of electrons converted from photons in a photodiode. It is linked to the responsivity by

$$Q_\lambda = \frac{R_\lambda}{\lambda} \times \frac{hc}{e} \approx \frac{R_\lambda}{\lambda} \times (1240 \text{ W.nm/A}), \tag{5.14}$$

where h is Planck's constant, c is the speed of light in vacuum and e is the elementary charge. In particular for QKD detectors, it is desirable to have a quantum efficiency as close as possible to 1 in order to limit as much as possible the losses in the receiver.

Common mode rejection ratio (CMMR): In a perfect balanced receiver, we want the output voltage to be a function of the voltages output by each photodiode such that

$$V_{out} = G(V_+ - V_-). \tag{5.15}$$

In practice, imperfections lead to a small amplification of the sum of the output voltages as well such that

$$V_{out} = G(V_+ - V_-) + G_{cm}(V_+ + V_-). \tag{5.16}$$

The common mode rejection ration is defined as the ratio of both gains and is a measure of how well the detector performs a balanced detection. It is usually expressed in dB as

$$\text{CMRR} = 20 \log_{10}\left(\frac{G}{G_{cm}}\right). \tag{5.17}$$

5.4 Digital signal processing

In order to retrieve the information encoded on the electromagnetic field, the electrical signal generated by the detectors is sampled. Then, the samples are processed to recreate the symbols originally sent. This process is called *digital signal processing* and is a cornerstone of modern coherent communications. Let us describe some of the powerful tools at our disposal to translate our set of samples into the correct set of symbols.

5.4.1 Equalizer

In classical coherent communications, the adaptive equalizer is one of the most powerful tools of digital signal processing. It can compensate most channel impairments, filter noise, and can find the optimal sampling instant. It is based on finite-impulse-response (FIR) filters and algorithms for filter-tap adaptation. We discuss these below.

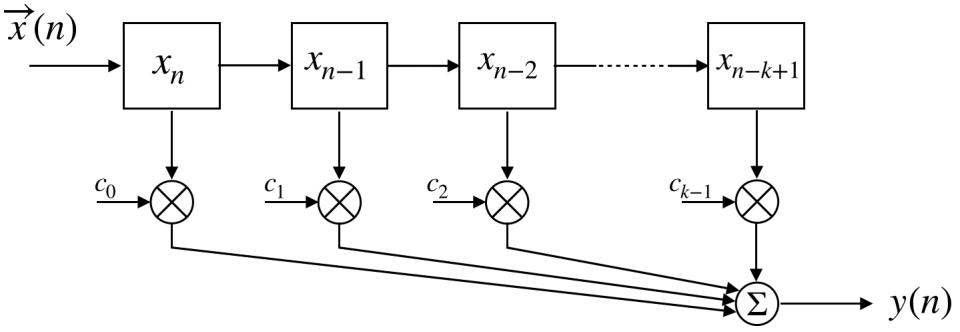


Figure 5.13: A FIR filter with k taps performs a linear combination of samples x_n to x_{n-k+1} using coefficients c_0 to c_{k-1} to output the symbol $y(n)$

FIR filter. The FIR filter is determined by a number of taps k and by tap coefficients $\vec{c} = [c_0, ..., c_{k-1}]$. The n^{th} run of the FIR filter has input a sequence of samples $\vec{x}(n) = [x_n, x_{n-1}, ..., x_{n-k+1}]$ and output the n^{th} symbol given by

$$y(n) = \vec{c} \cdot \vec{x}(n) \tag{5.18}$$

$$y(n) = \sum_{j=0}^{k-1} c_j x_{n-j} \tag{5.19}$$

The schematic representation of the FIR filter is depicted in figure 5.13. In fact, when the signal power is sufficiently low such that the channel response is linear, the frequency response of the received complex amplitude of a dual polarisation signal can be written in the form [73] :

$$\begin{pmatrix} E_x(\omega) \\ E_y(\omega) \end{pmatrix} = \mathbf{H}(\omega) \begin{pmatrix} E_x^{in}(\omega) \\ E_y^{in}(\omega) \end{pmatrix} \tag{5.20}$$

Therefore the transfer function of the equalizer should be as close as possible to

$$\mathbf{H}_{eq}(\omega) = \mathbf{H}^{-1} \tag{5.21}$$

$$= \begin{bmatrix} h_{xx}(\omega) & h_{xy}(\omega) \\ h_{yx}(\omega) & h_{yy}(\omega) \end{bmatrix} \tag{5.22}$$

With a sufficient number of taps and by choosing carefully the tap coefficients in the time domain, one can pilot the frequency response of the FIR filter to realize each element of the matrix $\mathbf{H}_{eq}$. Then the equalizer response can be realized using 2×2 butterfly-structured FIR filters as is depicted in figure 5.14. The consequence is that the FIR filter can separate the X and Y components of a signal with an arbitrarily varying polarisation, as well as compensate channel impairments such as GVD, PMD and PDL.

Filter-tap adaptation algorithm At the beginning of the equalisation the filter-tap coefficients are initialised to a given value, for instance all tap coefficients are set to 0 except the central one set to 1. Then the filter-tap coefficients are updated after each run based on some error function which depends on the modulation. For QPSK modulation we exploit the fact that the signal has constant amplitude. This is used as our criteria for the error function. When the signal amplitude is normalised to 1, the error function we use is :

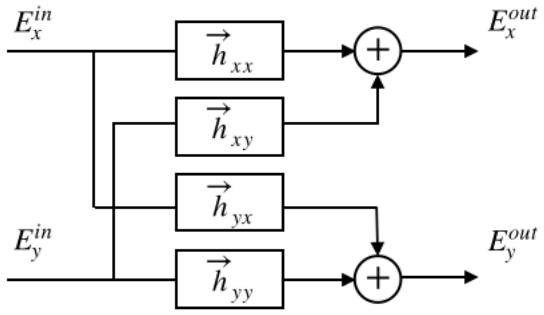


Figure 5.14: The 2×2 butterfly structured FIR filters. The $\vec{h}_{ij}$ are the FIR filters $\mathbf{H}_{eq}(\omega)$.

$$e_x(n) = (1 - |E_x^{out}(n)|^2)E_x^{out}(n), \tag{5.23}$$
$$e_y(n) = (1 - |E_y^{out}(n)|^2)E_y^{out}(n). \tag{5.24}$$

Then the filter-tap coefficients are updated from one run to the other as

$$\vec{h}_{ij}(n+1) := \vec{h}_{ij}(n) + \mu e_i(n)E_j^{out}, \tag{5.25}$$

where $(i,j) \in \{x,y\}^2$ and μ determines the speed of convergence of the filter. If μ is too large the filter might has too little resolution to perform correctly and if μ is too small it will take too long to converge. This filter-tap adaptation algorithm is named *Constant Modulus Algorithm* (CMA).

Clock timing recovery. Another unique function of adaptive FIR filters is to implement a variable time delay on the waveform with a much higher resolution than the sampling time interval. Therefore, as long as there is a sufficient number of taps, the adaptive FIR filter can retrieve the optimal sampling instant as is illustrated in the figure 5.15 taken from reference [73].

5.4.2 Carrier recovery

The phase of the signal laser is crucial to determine which symbol has been sent. For instance for the QPSK modulation format, the four symbols of the constellation have the same amplitude and are uniquely described by their phase. The homodyne and heterodyne detection discussed in chapter 1, together with the result of the measurement derived in equation (1.94), show that the measurement result provides a complex signal with a phase equal to $\theta_s - \theta_{LO}$ the difference between the phase of signal and LO. In order to determine θ_s, we must first estimate θ_{LO}.

In chapter 1, we omitted for simplicity the fact that the signal and LO are time varying light waves, and as such have angular frequencies ω_s and ω_{LO}. As a result the measured current is actually proportional to

$$\Delta I(t_n) \propto 2E_s E_{LO} \cos(\omega_{IF} t_n + \theta_s - \theta_{LO}), \tag{5.26}$$

where t_n is the sampling time and $\omega_{IF} = \omega_s - \omega_{LO}$ is the beating angular frequency between signal and LO. Therefore in our quest to retrieve θ_s we must also compensate the time dependant phase shift induced by $\omega_{IF} t_n$. The estimation and compensation of ω_{IF} and θ_s is called *carrier recovery*. We discuss how to do this here in the case where the signal is modulated according to a QPSK modulation since we will use these techniques in our experiment.

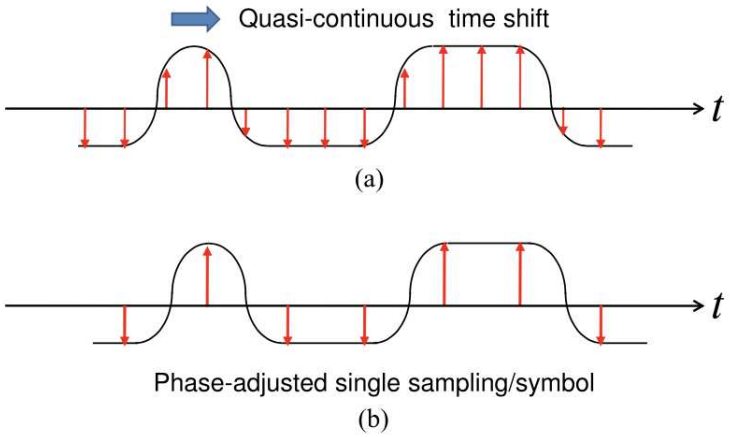


Figure 5.15: Figure taken from [73]. (a) The waveform is sampled at 2 samples per symbol. (b) After the adaptive FIR filter, the algorithm outputs the samples taken at the optimal instant for symbol decision.

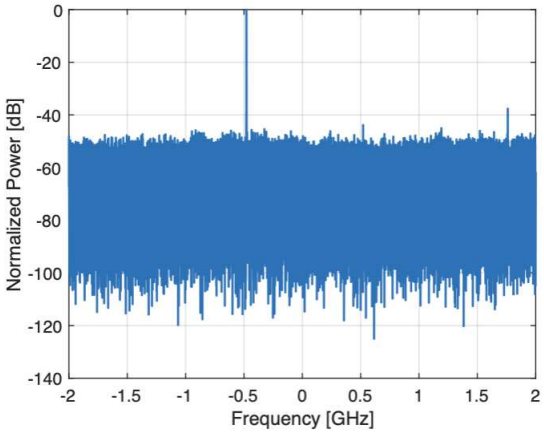


Figure 5.16: Raising the QPSK signal to the 4^{th} power cuts the fluctuations due to the modulation and concentrates the psd at a single frequency : the frequency offset.

Particularities of the QPSK modulation. A key component of carrier recovery in the case of QPSK modulation is the knowledge that $\theta_s \in \{\frac{\pi}{4}, \frac{3\pi}{4}, \frac{5\pi}{4}, \frac{7\pi}{4}\}$. The complex signal reconstituted from the measured sample $R_x = I + jQ$ can be written as :

$$R_x(t_n) = A \exp(i[\omega_{IF} t_n + \theta_s - \theta_{LO}]), \tag{5.27}$$

where A is the signal amplitude. Raising R_x to the power 4 cuts the phase changes due to the modulation since for all θ_s we have $4\theta_s = \pi[2\pi]$. Thus we have

$$R_x(t_n)^4 = -A^4 \exp(i[4\omega_{IF} t_n + 4\theta_{LO}]) \tag{5.28}$$

Frequency recovery.'The beating frequency is determined from the 4^{th} power signal very easily by shifting to the frequency domain and considering the maximum of the signal psd. Indeed most of the psd will be concentrated in a single peak located at frequency $f_{max} \approx 4\omega_{IF}/2\pi$ as is represented in the figure 5.16. We obtain the estimator for the beating frequency $\hat{\omega}_{IF} = \frac{2\pi f_{max}}{4}$. Then the signal is corrected by compensating the rotation due to the beating frequency :

$$R_x(t_n) := R_x(t_n) \times \exp(-i\hat{\omega}_{IF} t_n). \tag{5.29}$$

In most cases the estimator $\hat{\omega}_{IF}$ will not be exactly equal to ω_{IF} and therefore the time-dependant rotation of the constellation not entirely corrected at this stage. However this residual beating frequency after correction can be treated as additional LO phase and be compensated in the phase recovery stage. Therefore we suppose here that $\hat{\omega}_{IF} = \omega_{IF}$

Phase recovery. We proceed in a similar fashion to retrieve the LO phase. First we raise the frequency compensated signal to the 4^{th} power and obtain :

$$R_x(t_n)^4 = -A^4 \exp(i4\theta_{LO}). \tag{5.30}$$

Then the LO phase can be estimated as

$$\hat{\theta}_{LO} = \frac{\arg(R_x(t_n)^4)}{4} + \pi. \tag{5.31}$$

Note that the LO phase actually varies with time according to a Wiener process characterized by the laser linewidth $\Delta\nu$ [1]. However phase fluctuations are very small over a symbol period, such that a better way to estimate θ_{LO} is to average the phase over multiple symbols such that the phase estimator of the n^{th} symbol is given by

$$\hat{\theta}_{LO}(n) = \frac{1}{4} \arg\Big(\sum_{i=n-k}^{n+k} R_x^{\text{CFE}}(t_i)^4 \Big). \tag{5.32}$$

The length of the averaging window is here $2k + 1$ and must be carefully chosen based on the system considered.

5.5 Challenges for coherent quantum communications.

Compared to classical coherent communications, quantum coherent communications are operated with a signal comprising only a few photons per symbol. In this regime of low SNR the DSP algorithms discussed above perform poorly and cannot be executed as such. New solutions are therefore necessary to downsample the signal and perform carrier recovery. In addition to this, quantum signals

[1] The Wiener process characterizes the quantity $\Delta\theta_{LO}(t) = \theta_{LO}(t + \delta t) - \theta_{LO}(t)$ as a zero mean Gaussian random variable with variance $V = 2\pi\Delta\nu\delta t$

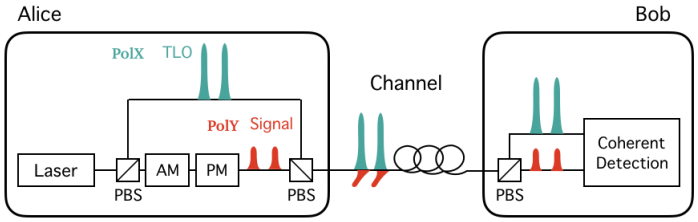


Figure 5.17: Example of a CV-QKD protocol with the TLO design. In this example the TLO is multiplexed with the signal using the polarisation degree of freedom. PBS : polarising beam splitter. AM : amplitude modulator. PM : phase modulator.

are naturally more sensitive to cross-talk from other channels since even one stray photon can generate considerable perturbations on the data, hence systems involving the coexistence of classical and quantum channels must be carefully designed. These issues must be correctly addressed if we hope to design efficient systems. The object of this section is to discuss these challenges in order to derive a relevant approach to our work.

5.5.1 Carrier recovery at low SNR

In the quantum regime the carrier recovery algorithms, such as the Viterbi & Viterbi algorithms for a QPSK modulation format, perform poorly. CV-QKD systems have evolved over the years to address this issue.

Transmitted local oscillator. First iterations of CV-QKD protocols solved this problem by deriving the local oscillator from the signal laser at Alice's side. The LO was then sent alongside the signal over the untrusted quantum channel to Bob and used to detect the quantum states. Examples of protocols using this design can be found in references [74, 65, 75, 76]. In this case the signal and LO have the same frequency and their phase fluctuations are minimal, which reduces the excess noise induced by imperfect carrier recovery compared to the case where the LO is a free-running laser with no fixed relation to the quantum states. This technique is sometimes referred to as the "Transmitted Local Oscillator" or TLO.

In reality, the TLO design presents security loopholes and performance flaws that are hard to overcome in practice. These lead to potential side-channel attacks which are detrimental to protocol security. The security flaws stem from the fact that the shot-noise calibration plays a crucial role in the estimation of the information leaked to Eve. The TLO design gives extra power to the eavesdropper since she can also manipulate the LO and therefore influence the shot-noise calibration procedure. Several attacks have been investigated in the case of a TLO protocol, such as a wavelength attack [32], a calibration attack [30] or a fluctuation attack [31]. While it is maybe possible to monitor the TLO design to insure that a given attack is not occurring, this would drastically increase the complexity of CV-QKD protocols and only provide security against known side-channel attacks.

In addition to the security loopholes, the TLO design also limits the system performance. First, the LO can generate crosstalk on the quantum channel during propagation. Second, CV-QKD protocols require the detection be made in the shot-noise limited regime, where the electronic noise is at least one order of magnitude below the shot-noise. To this end the LO at Bob's is required to have sufficient power, with typically $\sim 10^8$ photons per pulse. However as the distance between Alice and Bob increases, the LO power at Alice must also increase to satisfy the shot-noise limited detection criteria. This becomes harder to achieve in practical experiments since fiber nonlinearities arise when too much power is injected in the single mode fiber and cross-talk between the signal and LO will also deprecate the key rate.

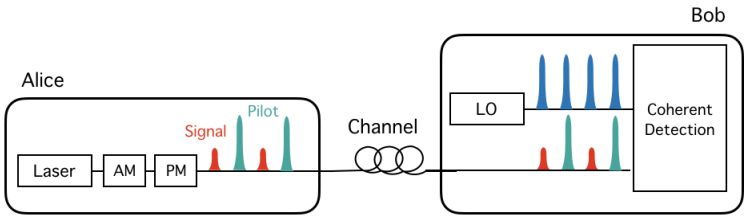


Figure 5.18: Example of the "LLO" design. The LO is generated at Bob's and does not propagate over the channel, thus Eve does not have access to it. The signal is multiplexed with pilot signals to provide phase and frequency information. In this example, the pilot and signal pulses are multiplexed in time. AM : amplitude modulator. PM : phase modulator. LO : local oscillator

"Local" local oscillator. Since the TLO design cannot be used, this means quantum coherent communication systems have to perform carrier recovery with a "local" LO (LLO) as in typical coherent communication. The common solution in this case is to rely on pilot signals multiplexed with the quantum states. The idea is to derive the pilot signals from the same laser used to generate the quantum states, such that pilot and quantum signals have a fixed phase and frequency relation. Then the carrier recovery algorithms can be applied to the pilot signal and the quantum states can be corrected during the DSP step based on the phase and frequency estimators computed on the pilot signals.

Examples of protocols using pilot signals can be found for example in references [17, 77, 78, 79]. The pilot signals are multiplexed with the quantum states using the time [78, 79], frequency [17] and/or polarisation [77, 17] degrees of freedom in order to reduce the pilot cross-talk on the quantum measurement.

5.5.2 Coexistence with classical channels

Our conclusion in subsection 4.4.3 was that the ability to coexist with classical channels was one advantage of CV-QKD compared to other solutions, but this does not mean it is trivial. The holy grail for quantum coherent communications would be for these protocols to be compatible with optical backbone links, covering a distance of about 80 km together with 100 classical channels at nominal input power. This would give them access to a large infrastructure and provide many opportunities for commercial applications.

This objective remains however out of our reach for the moment. The main challenge in this setting is the Raman noise generated by the classical channels at the quantum signal wavelength, which becomes the dominant noise source. Ideas for system designs involve choosing the quantum channel wavelength at a lower wavelength than the classical channels since Raman noise is less probable [70, 80] or to operate the system with reduced power of the classical channels [71]. Another hope for quantum coherent communications resides in the development of new DSP techniques which would enable equalizing the signal in the low SNR regime, therefore filtering the Raman noise affecting the channel. New DSP methods based on machine learning techniques have already been proven to perform better carrier recovery [81, 82], hence this is certainly an interesting direction to pursue.

5.5.3 Positioning of our work

A cost-based approach for CV-QKD involves deploying systems over the current fiber infrastructure, but based on the current state of the art this is difficult without modifying classical systems to reduce their impact on the quantum channel. In order to extract the best out of joint classical and quantum communications over the same fiber, we should look to design systems working on the current infrastructure but that are optimized for both the quantum and the classical channels.

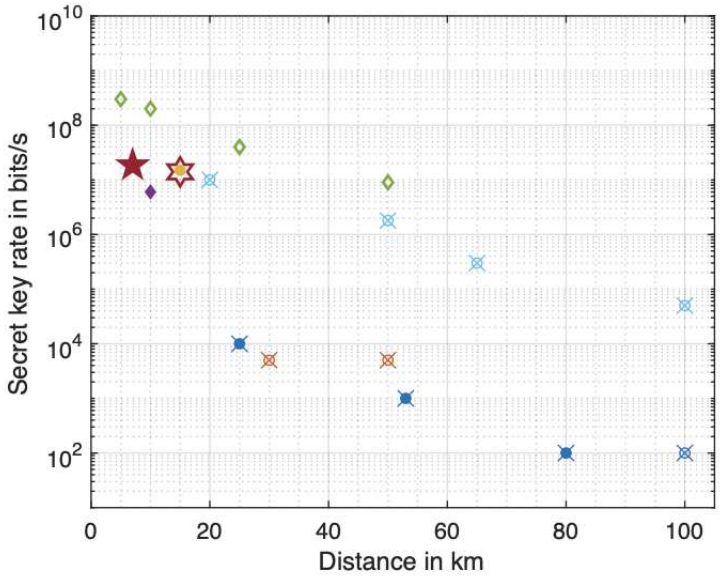
An interesting question when we think of joint systems is whether the classical channels will only be detrimental to the CV-QKD performance or if they can be used to gain some sort of advantage compared to QKD operated on a dark fiber. This question is at the core of the research conducted during this PhD thesis and we chose to address it in two ways described below.

- **Symbiotic operation of quantum and classical communications.** Our first proposal is an experimental demonstration of a CV-QKD experiment multiplexed with a classical channel in which we demonstrate that carrier recovery can be performed from a classical channel. Our objective is to show that when designing joint systems, we can relax the need for pilot tones which add to the overall complexity and do not carry classical information.

  In addition, when the quantum channel is used for CV-QKD, the key retrieved can also be used to encode part of the classical data transmitted. Hence the quantum and classical channels are mutually beneficial and are operated in a symbiotic fashion.

  Our work constitutes a proof-of-concept and paves the way towards efficient designs of joint systems which look to exploit the most out of their coexistence. We show a comparison of our results with the current state of the art in CV-QKD in the figure 5.19 and discuss our implementation further in chapter 6.

- **Covert QKD.** Our second proposal is a theoretical research project in which we investigate how to harness channel noise -for example due to classical channels- to provide a new security primitive, called covertness, to the QKD protocol. The idea behind covert communications is that the signal transmitted over the channel is indistinguishable from background noise for any quantum adversary. This can be a desirable security feature for QKD since even if the distilled key is provably secure, Eve still has knowledge that Alice and Bob performed the protocol and can use this to her advantage. We discuss this further in chapter 7 and provide our results.



Reference	Modulation	Phase reference	Local Oscillator	Security proof	Symbol
[74]	Gaussian	TLO	Transmitted LO	finite-size	
[65]	Gaussian	TLO	Transmitted LO	asymptotic regime	
[75]	Gaussian	TLO	Transmitted LO	asymptotic regime	
[77]	PCS-256QAM	pilot signals	Local LO	asymptotic regime	
[78]	PCS-64QAM	pilot signals	Local LO	finite-size	
[76]	Gaussian	TLO	Transmitted LO	finite-size	
[79]	Gaussian	pilot signals	Local LO	finite-size	
OFC2022	QPSK	classical channel	Local LO	asymptotic regime	
SPIE2022	PCS-64QAM	classical channel	Local LO	finite-size	

Figure 5.19: Plot of the key rate versus distance for different CV-QKD protocols in the literature. The different protocols are represented by different symbols according to their implementation choices. Modulation : Gaussian = circle, PCS = diamond, QPSK = pentagram. LO : TLO = crossed symbol, LLO = not crossed symbol. Security proof : finite-size = full symbol, asymptotic regime = hollow symbol. The table shows all references ploted in the graph as well as their characteristics and their symbol representation.

Chapter 6

Joint classical and quantum coherent communication

Contents

In this chapter we detail our experimental implementation of joint classical communications with CV-QKD without the use of pilot tones.

6.1 Experimental setup

The experimental setup is displayed in the figure 6.1 and the list of components used are summarized in the table 6.1

6.1.1 Transmitter : signal generation

The transmitter side corresponds to Alice's lab in the QKD protocol. The light is generated by a low-linewidth laser which is fed into the dual polarisation I/Q modulator. Two AWGs control the X-

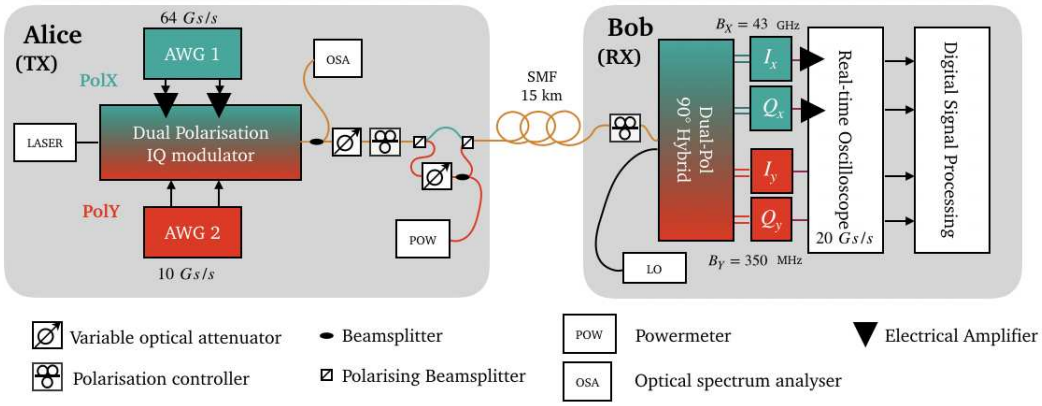


Figure 6.1: Experimental setup. AWG : arbitrary waveform generator. OSA : optical spectrum analyser. LO : local oscillator.

Device	Reference
Laser and LO	NKT Koheras Adjustik
Dual-Pol IQ modulator	Fujitsu FTM7977HQA
AWG1	Keysight M8195A
AWG2	Tektronix AWG7122B
PBS/PBC	General photonics PB-15-P1-FC/APC
Powermeter	Ando AQ2140
Attenuator 1	HP 8156A
Attenuator 2	Oz optics BB-100-11-1550-8/125-P60-3A3A-3-1
Dual-pol 90° hybrid	Kylia COH28-X
Balanced receivers I_x/Q_x	Finisar BPDV21x0R
Balanced receivers I_y/Q_y	Exalos EBR370005-02
Oscilloscope	DSOZ504A

Table 6.1: This table gives the references of the components used in the experiment for the interested reader.

and Y-polarisation of the field corresponding to the classical (AWG1) and quantum (AWG2) signal. At the exit of the modulator, a 10% fraction of the signal is directed towards an optical spectrum analyser to monitor the output of the modulator and to verify the voltage biases are set correctly.

Classical signal generation. The sequence of samples fed to the AWG1 is generated from a pseudo-random bit sequence which is then mapped to a corresponding sequence of QPSK symbols. The samples are then generated from the symbols thanks to a built-in interpolation function in MATLAB.

The spectral shaping of the classical signal is operated directly at the sample level. We limit its spectral width using a RRC filter, described in chapter 5, with a sharp roll-off factor of 0.1. Then the signal is frequency shifted by $f_{\text{shift},c} = 4$ GHz by multiplying the samples by a time dependant complex exponential. The representation of the classical signal spectrum before the RRC, after the RRC and after the frequency shift can be found in figure 6.2.

Quantum signal generation. The QPSK modulation for the quantum channel was generated similarly to the classical signal by adapting the symbol rate and the RRC roll-off factor to 0.4. Generating the PCS-64QAM constellation was less direct since we do not have a distribution matcher to map bits to symbols. Therefore we proceeded differently, first generating the symbols according to the desired probability distribution and then mapping them to the corresponding bits in a typical 64QAM constellation.

The quantum signal spectrum was shifted by $f_{\text{shift},q} = 1$ GHz in order to reduce noise generated by the residual carrier. The spectrum the joint classical and quantum signal before attenuation of the quantum channel is represented in figure 6.3.

Power leveling of quantum and classical signals. The desired number of photons per symbol on the quantum channel is obtained by attenuating the quantum signal relative to the classical signal. A first leveling can be achieved in the modulator by controlling the amplitude of the electrical signal generated by the AWGs. Electrical amplifiers placed at the output of the AWG1 increase the output power of the classical channel relative to the quantum channel.

However this leveling is not sufficient, hence we also use a series of components to attenuate the quantum channel specifically using the polarisation degree of freedom. To do this we begin by separating classical and quantum signals on a polarising beam splitter (PBS). A polarisation controller (PC) before the PBS is used to align the polarisations in the fiber with the axes of the PBS. The path corresponding to the classical signal is untouched and fed into the first input of a polarising beam combiner (PBC). The quantum signal is attenuated and fed into the second input of the PBC. Before it is recombined, part of the quantum signal is split on a 50/50 beamsplitter and directed towards an optical power meter to monitor the power on the quantum channel. The power meter is useful to manually set the PC. Since the quantum signal is less powerful than the classical signal at the exit of the I/Q modulator, we set the PC to minimize the power on the power meter. All the components and fiber used between the two PBS are polarisation maintaining.

Synchronisation of both channels. Since Alice and Bob need to compare their data during the QKD protocol, we need to share a reference frame for the beginning and the end of the data sequence. In a real system, Alice will send a finite sequence of symbols which Bob will measure, process and store. Then Alice decides to reveal a subset of the quantum states she sent which are easily identifiable at Bob's by their position in the detected sequence. In our experiment however, the sequence of quantum states is repeated continuously at Alice and the acquisition begins during a random symbol in the sequence. Therefore we need some method to generate the sequence at Alice based on Bob's measurement window.

This is achieved via synchronisation of classical and quantum data streams such that we can identify the beginning of the repeating quantum sequence from the classical data. To synchronise both channels we begin by providing AWG1 and AWG2 with a common clock reference. Then a arbitrary function generator (AFG) with the same clock reference generates a trigger signal so that

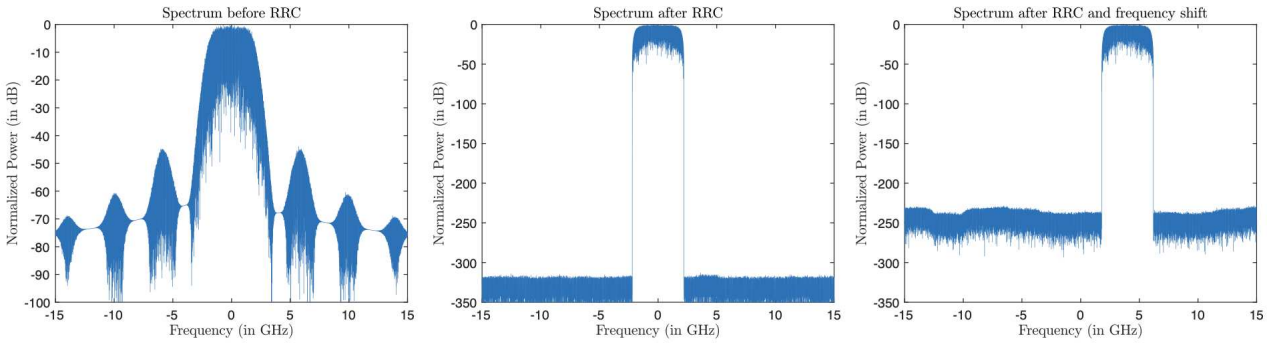


Figure 6.2: Classical signal spectrum (left) before the RRC, (middle) after the RRC, (right) after the RRC and frequency shift.

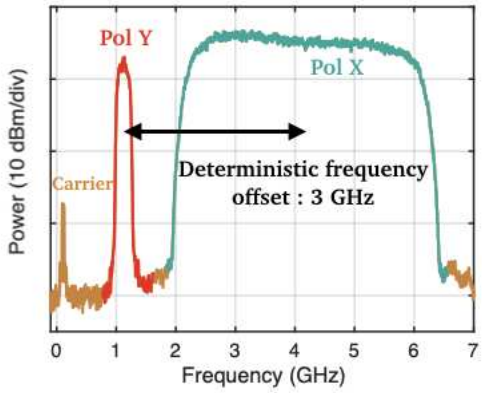


Figure 6.3: Spectrum of the signal at the exit of the I/Q modulator.

both AWG1 and AWG2 start emitting at the same time.

6.1.2 Receiver : signal detection

The receiver side plays the role of Bob in the QKD protocol. The coherent detection process is based on mixing the signal with the LO in the polarisation and phase diversity hybrid. Before the hybrid we use a PC to manually align the polarisation of the incoming signal with the axes of the PBS located in hybrid, such that the classical and quantum signals are optically routed towards the classical and quantum detectors respectively. The data is acquired by the oscilloscope piloted from the MATLAB session on the laboratory computer. Finally, the samples acquired are processed during the digital signal processing step.

Losses. It is crucial to quantify the losses at Bob's to apply the trusted receiver security proofs. Here we have 2 dB of losses due to the polarisation controller and the 90° hybrid.

Sensitivity to polarisation drifts. The PC is set manually during the CV-QKD experiment. However over time the state of polarisation (SOP) of the incoming field rotates and the setting of the PC must be adapted. Even a slight misalignment of the polarisation can lead to a significant increase in the excess noise measured during the experiment as is represented in the figure 6.6. Therefore the protocol performance is closely related to our ability to track the SOP over time and to correctly set

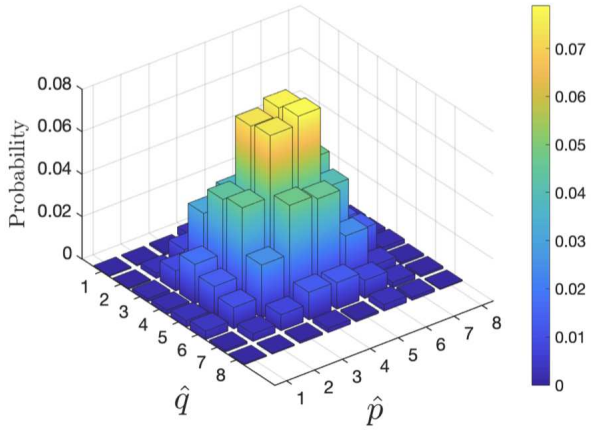


Figure 6.4: With only 2000 symbols, the PCS-64QAM constellation can only approach the theoretical occurrence probabilities for each symbol. We generate the constellation by generating the first 64 unique QAM symbols, and draw the rest randomly according to the desired probability distribution.

the PC.

Classical detectors. The balanced detectors used for the classical signal have a 43 GHz bandwidth in order to correctly detect the full classical signal. We placed electrical amplifiers after the detectors so that the noise floor of the oscilloscope was well below the noise floor of the detectors.

Quantum detectors. The quantum balanced detectors have a tunable bandwidth between 80 and 350 MHz. We chose to set the bandwidth at its maximum in order to have some margin in the signal-LO frequency offset for the detection of the 250 MBd quantum signal. These receivers have built-in low-noise electrical amplifiers, thus we do not need to add any amplifying device and we connect them directly to the oscilloscope.

Local oscillator. The LO is tuned such that the LO central frequency is close to the quantum signal central frequency. Actually, the combination of the LO central frequency f_{LO} and the bandwidth of the detectors B_{elec} determine a "spectral window", represented in figure 6.5, of the optical signals that can be measured. Typically we want to set the LO central frequency such that the quantum and classical signals are in the spectral windows defined by the quantum and classical detector's bandwidths respectively. Looking to the spectrum in figure 6.3, we also want the strong classical signal as far as possible from the quantum detectors spectral window in order to mitigate the excess noise induced by the classical channel. Therefore it is best to choose a LO central frequency below the quantum signal central frequency.

Oscilloscope. The oscilloscope sampling rate must be carefully chosen based on the symbol rate of the detected signals. We discussed above the LO central frequency would be chosen below the quantum signal central frequency. Therefore the frequency offset between the higher frequencies of the classical spectrum and the LO will be around 6 GHz. In order to satisfy the 2 times oversampling criterion [83], we need to sample the classical signal at least at a sample rate of 12 Gsa/s. Since the oscilloscope only offers the possibility to sample the signal at 10 Gsa/s or 20 Gsa/s (or more), we chose to operate the oscilloscope at sampling rate 20 Gsa/s.

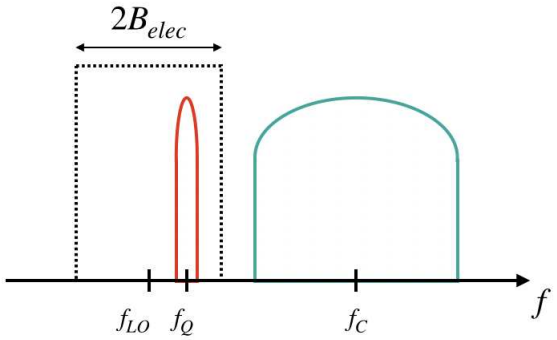


Figure 6.5: The LO central frequency as well as the detector bandwidth define a spectral window of the signals that can be detected. In this schematic representation, f_{LO} is chosen such that the quantum signal spectrum is in the spectral window and the classical signal is not.

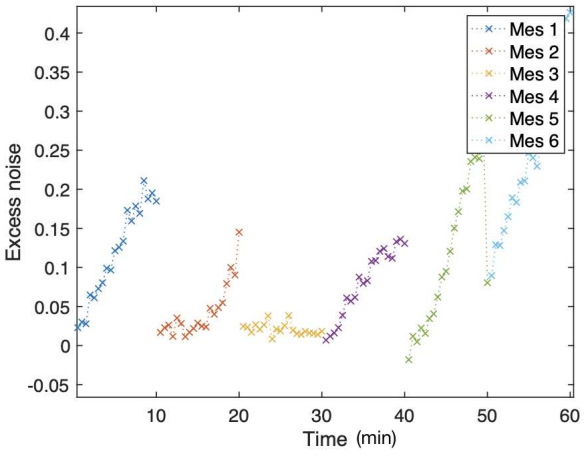


Figure 6.6: In this graph we show the sensitivity to polarisation of the excess noise measurement during the protocol. We acquire data from the oscilloscope over 1 hour with an interruption every 10 minutes. During the pause we set the PC in the best way possible by hand. The results of the hour of measurement are then plotted and divided into 6 measurements denoted by "Mes 1-6". We clearly see the excess noise over time increases until the polarisation is realigned. We can also observe the mean noise level increases in measurements 5 and 6 which is due to the drifts in the settings of the IQ modulator. We discuss these drifts in more detail in the subsection 6.4.4.

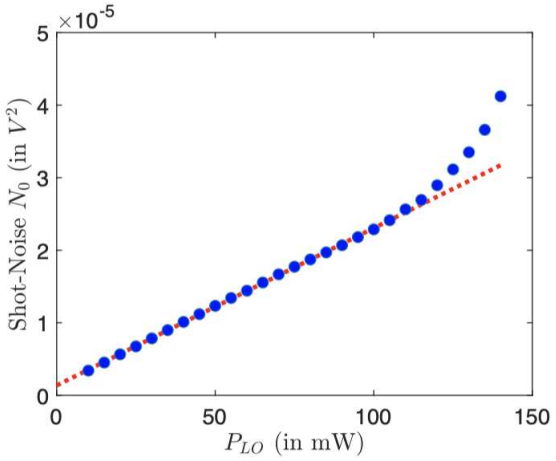


Figure 6.7: Shot-noise plus electronic noise variance as a function of the LO power. The blue circles are measurements and the dashed red line is a linear interpolation of the linear regime. We observe a linear dependence until the LO power is above 110 mW, at which point the detectors respond in a non-linear fashion.

6.2 Calibration

The precise calibration of the shot-noise is central to the CV-QKD experiment. Since the action of the eavesdropper is quantified by the excess noise -the noise above the shot-noise threshold- it is crucial that the shot-noise is well known. Underestimating the shot-noise would lead to an overestimation the excess noise and would therefore cause the protocol to extract less secret key than what it could. Even worse, overestimating the shot-noise would lead to an underestimation of the excess noise and potential security flaws in the protocol. The object of this section is to discuss and describe our shot-noise calibration.

6.2.1 Receiver linearity

The electronic noise ν_{el} is expressed in SNU as

$$\nu_{el}^{\mathrm{SNU}} = \frac{\nu_{el}^{V^2}}{N_0}, \tag{6.1}$$

where the superscripts SNU and V^2 refer to the unit and N_0 is the shot-noise variance. The value $\nu_{el}^{V^2}$ is stable and only depends on the noise floor of the low-noise receivers and of the oscilloscope. Hence ν_{el}^{SNU} is inversely proportional to the shot-noise value N_0 which is itself proportional to the LO power. Therefore it is interesting to operate the experiment with high LO power in order to minimise ν_{el}^{SNU}. The ratio $\nu_{el}^{V^2}/N_0$ is called the clearance and is usually expressed in dB. It gives the value of the electronic noise in SNU.

However we cannot simply set the LO to the strongest output power (200 mW or 23 dBm) because above a certain threshold the receivers do not respond linearly to their input, which induces noise. Therefore we must make sure we set the LO power such that the balanced receivers are operated in the linear regime. We show in figure 6.7 a plot of the shot-noise value in V^2 versus the LO launch power. We clearly observe a linear dependency of the shot-noise to the LO power until the LO reaches approximately 110 mW, after which the receiver response is outside of the linear regime. We chose the LO launch power to be 100 mW and display the clearance in the figure 6.8

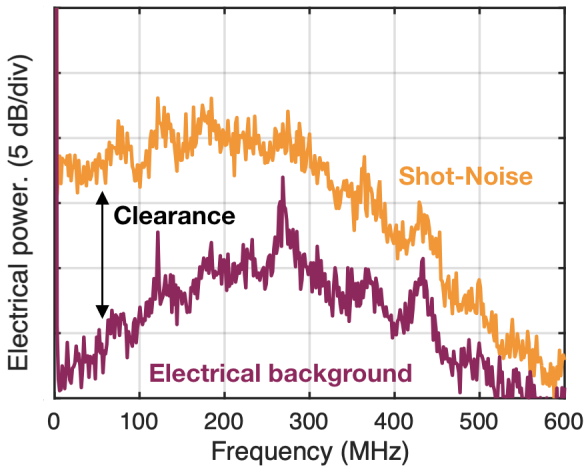


Figure 6.8: Power spectral density output of the balanced receivers with and without the LO turned on.

6.2.2 Shot-noise estimation

We describe our shot-noise estimation procedure here.

Building the shot-noise estimator. We estimate the shot-noise experimentally by the following procedure. First, when the signal and LO are turned off, the data observed on the oscilloscope corresponds to the fluctuations induced by the electronic noise of the detectors. We record from the oscilloscope a set of samples $\{X_{el}^i\}_{i=1}^n$ which are centered before we compute the electronic noise estimator expressed in V^2 as :

$$\hat{\nu}_{el}^{V^2} = \frac{1}{n}\sum_{i=1}^{n}\left(X_{el}^i\right)^2 \tag{6.2}$$

Then the LO is turned on, generating shot-noise on the samples read by the oscilloscope. We perform a second measurement to obtain a set of samples $\{X_{N_0}^i\}_{i=1}^n$. These samples are centered and we compute the shot-noise estimator as :

$$\hat{N}_0 = \frac{1}{n}\sum_{i=1}^{n}\left(X_{N_0}^i\right)^2 - \hat{\nu}_{el}^{V^2} \tag{6.3}$$

Electronic noise variations. In theory for every shot-noise estimation we should also estimate $\nu_{el}^{V^2}$. In practice however this value of the electronic noise can be considered constant at the scale of a day of experimental work. We show this in figure 6.9 by computing successive estimators for $\nu_{el}^{V^2}$ over more than 7 hours. In the plot we normalised our values by a typical value of $\hat{N}_0$ to put the electronic noise variations in perspective compared to the shot-noise. We find that the standard deviation of the electronic noise measurement is of the order of 5×10^{-4} SNU. Since this value is much smaller than other fluctuating terms we can consider it is constant during the experiment.

Shot-noise variations. The shot-noise value fluctuates over time, for example because of fluctuations in the LO power or vibrations in the lab. We found that a particular cause of instability was temperature variations in the lab. We illustrate this in the figure 6.10 where we can observe the correlations between temperature and shot-noise variations.

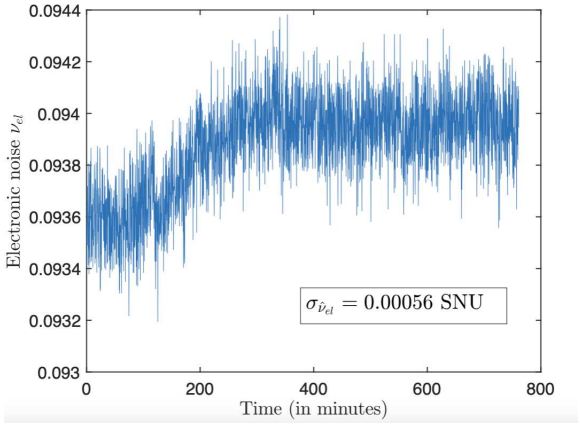


Figure 6.9: Electronic noise, in SNU, evolution over time. We observe the electronic noise variations are of the order of 10^{-4} SNU, which is negligible compared to other system fluctuations.

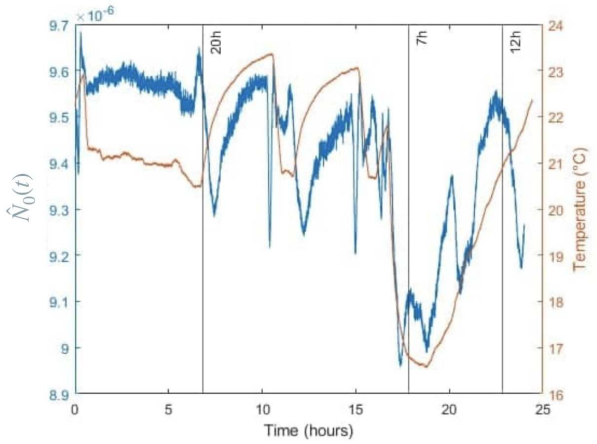


Figure 6.10: Evolution of $\hat{N}_0(t)$ over time, plotted in blue. We also plot the temperature fluctuations in the lab in orange.

Because of this the shot-noise fluctuations must be tracked during the experiment, which we achieve by performing a shot-noise estimation before each data acquisition. Since there is a delay δt between the shot-noise acquisition and the data acquisition, it is interesting to investigate how the shot-noise behaves during this time interval in particular because these fluctuations will also affect our excess noise estimation. For this we take a high estimation of $\delta t = 7.5s$ and study the quantity

$$\Delta\hat{N}_0(t) = \frac{\hat{N}_0(t+\delta t) - \hat{N}_0(t)}{\hat{N}_0(t+\delta t)}. \tag{6.4}$$

The standard deviation of this estimator quantifies the average fluctuation of the shot-noise between a shot-noise estimation block (at time t) and a data acquisition block (at time $t + \delta t$). The results are displayed in the figure 6.11 and show that the standard deviation of $\Delta\hat{N}_0(t)$ is approximately 2×10^{-3} SNU, which is also the minimal precision on the excess noise we can hope to achieve.

Data acquisition procedure. According to our results we define the following acquisition procedure to estimate successive blocks of quantum and classical data. We begin by estimating once and

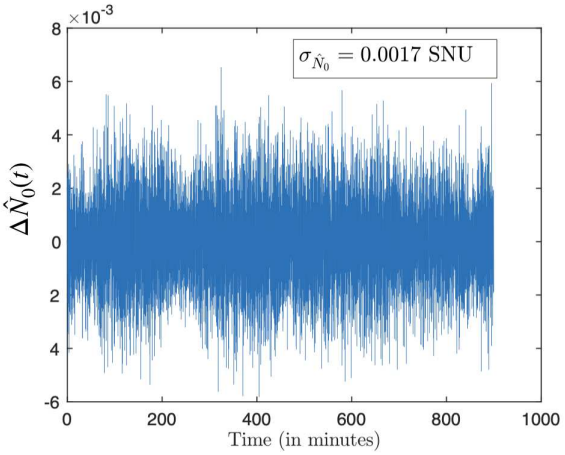


Figure 6.11: We plot $\Delta\hat{N}_0(t)$ over time and estimate, in SNU, how much the shot-noise fluctuates between the shot-noise estimation and the data measurement.

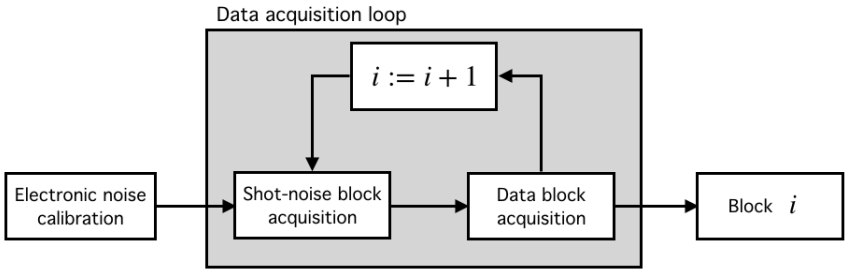


Figure 6.12: The acquisition loop for our CV-QKD protocol. We estimate the electronic noise once and for all. Then we alternate shot-noise estimation blocks with data blocks in order to track the shot-noise fluctuations.

for all the electronic noise and do not track its fluctuations for the rest of the experiment. Then, we alternate between one measurement dedicated to the shot-noise estimation with the signal off and one measurement dedicated to the key distillation with the signal on. This is represented in the figure 6.12.

6.2.3 Improving the statistical precision of the shot-noise

The standard deviation of $\Delta\hat{N}_0(t)$ derived in the previous subsection should be minimized to improve the precision of the excess noise estimation. This can be achieved by different ways, for example by reducing the delay δt or by stabilizing the temperature in the laboratory. Unfortunately at our level we do not have much control over these : δt is fixed by the wait time due to the synchronisation of the AWGs and the temperature regulation system is not under our control. Hence we attempt to leverage a third solution which we can control : the statistical precision of our estimators. This will be the focus of this subsection, but note the concepts developed here will also be useful to predict the precision on the excess noise estimator.

Statistical precision and number of points. Statistical effects are directly related to the number of points used to compute the estimators as a consequence of the central limit theorem. To see this let us consider the shot-noise estimator $\hat{N}_0$ is computed from the set of *i.i.d.* random variables $\{X^i_{N_0}\}_{i=1}^n$ where for all i, $X^i_{N_0} \sim \mathcal{N}(0, N_0 + \nu_{el})$. We can compute the mean and variance of the random variable $(X^i_{N_0})^2$ as

$$\mathbb{E}[(X^i_{N_0})^2] = N_0 + \nu_{el}, \tag{6.5}$$

$$\mathrm{Var}[(X^i_{N_0})^2] = 2(N_0 + \nu_{el})^2. \tag{6.6}$$

Note the second equality is obtained by looking at the moment of X_{N_0}. The central limit theorem states that in the limit of large numbers, the sum of *i.i.d.* random variables converges towards a Gaussian random variable with mean and variance the sum of the means and the sum of the variances of the *i.i.d.* random variables. Therefore we have that

$$\frac{1}{n}\sum_{i=1}^{n}\left(X^i_{N_0}\right)^2 \underset{n\to\infty}{\sim} \mathcal{N}(N_0 + \nu_{el}, \frac{2}{n}(N_0 + \nu_{el})^2) \tag{6.7}$$

Let us put aside the estimation of ν_{el} for the moment and let us consider that $\hat{\nu}_{el} = \nu_{el}$. In the limit of a large number of samples, we can write that

$$\hat{N}_0 \sim \mathcal{N}(N_0, \frac{2}{n}(N_0 + \nu_{el})^2). \tag{6.8}$$

Hence the estimator $\hat{N}_0$ follows a Gaussian probability distribution and has standard deviation

$$\sigma_{\hat{N}_0} = \sqrt{\frac{2}{n}}(N_0 + \nu_{el}) \underset{\text{SNU}}{\approx} \frac{1.56}{\sqrt{n}}, \tag{6.9}$$

where we obtained the value in SNU by replacing ν_{el} by our experimental value of 0.1 SNU. Looking at equation 6.9 we obtain a rule of thumb for the statistical precision of $\hat{N}_0$ which scales as $\frac{1}{\sqrt{n}}$.

Importance of the *i.i.d.* hypothesis. A key hypothesis in the central limit theorem is that the shot-noise sample points $\{X^i_{N_0}\}_{i=1}^n$ are all *i.i.d.* Therefore it is not sufficient to consider only the number of sample points used to compute $\hat{N}_0$ but one must consider the number of *i.i.d.* sample points retrieved from the oscilloscope. This can be seen in the figure 6.13 where we plot $\Delta\hat{N}_0(t)$ in the two cases where the oscilloscope samples the points at 1 GHz and at 20 GHz. In both cases the same number of points are used to compute $\hat{N}_0$, however they are spread over a longer time window

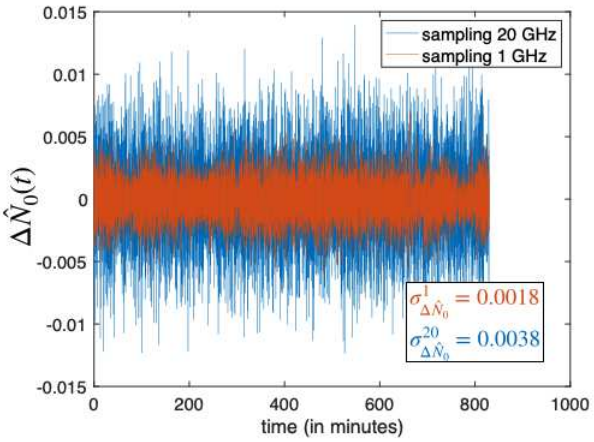


Figure 6.13: We plot $\Delta\hat{N}_0(t)$ for two different oscilloscope sampling rates and show the importance of the *i.i.d.* hypothesis in the central limit theorem.

when the oscilloscope runs at 1 GHz compared to the case where it runs at 20 GHz. From the figure, we observe the measurement at 1 GHz is much more stable than the measurement at 20 GHz. This is explained by the fact that there are more *i.i.d.* samples in this case, therefore it is interesting to understand how many *i.i.d.* samples we have in our acquisition.

Considering that the detectors have a bandwidth B_{elec}, the minimal time between two samples $X^i_{N_0}$ and $X^{i+1}_{N_0}$ for them to be independant is given by

$$T^{iid}_{samp} = \frac{1}{B_{elec}}. \tag{6.10}$$

Hence for the target value n of *i.i.d.* sample points, the acquisition $\{X^i_{N_0}\}_{i=1}^n$ must span at least a time $T_{acq} = n \times T^{iid}_{samp}$. In practice the oscilloscope samples at rate f_{acq} faster than 350 MHz, therefore we will obtain a total number of samples $n_{tot} > n$ which are not *i.i.d.*, as we illustrated in figure 6.13. The number of sample points n_{tot} required to have n *i.i.d.* points is given by

$$n_{tot} = T_{acq} \times f_{acq}, \tag{6.11}$$

$$= n \times \frac{f_{acq}}{B_{elec}}. \tag{6.12}$$

Equivalently, we can find the number of *i.i.d.* samples from the the total number of samples and the sampling rate :

$$n = n_{tot} \times \frac{B_{elec}}{f_{acq}} \tag{6.13}$$

Statistical precision in our experiment. Based on what was said above, the best option to precisely estimate the shot-noise is to use a slower sampling rate to cover a larger time window. Given that the maximum number of points that can be retrieved from the oscilloscope is around 50 Mpts, we can compare the theoretical statistical precision of the estimation at $f_{acq} = 1$ GHz and $f_{acq} = 20$ GHz. We begin by computing the number of *i.i.d* samples in both cases :

$$\begin{aligned} n^{1\text{GHz}} &= 17.5 \times 10^6, \\ n^{20\text{GHz}} &= 0.875 \times 10^6, \end{aligned} \tag{6.14}$$

which then provides the standard deviations due to statistical effects

$$\begin{aligned}\sigma_{\hat{N}_0}^{1\text{GHz}} &= 3.7 \times 10^{-4},\\ \sigma_{\hat{N}_0}^{20\text{GHz}} &= 1.7 \times 10^{-3},\end{aligned} \tag{6.15}$$

For a Gaussian random variable, we can bound the probability that the shot-noise value N_0 is contained in an interval $I_{k\sigma}$ of length $2k\sigma_{\hat{N}_0}$ centered on $\hat{N}_0$ by $68.27\%, 95.45\%$ and 99.73% for $k = 1$, 2 and 3 respectively. Hence we will define the confidence in our estimator $\hat{N}_0$ by considering the length of the confidence interval $p_{k\sigma} = |I_{k\sigma}|$. Lets examine the statistical precision of our estimation for $k = 2$ and $k = 3$. We have

$$\begin{aligned}p_{2\sigma}^{1\text{GHz}} &= 1.5 \times 10^{-3}, \qquad p_{3\sigma}^{1\text{GHz}} = 2.2 \times 10^{-3},\\ p_{2\sigma}^{20\text{GHz}} &= 6.8 \times 10^{-3}, \qquad p_{3\sigma}^{20\text{GHz}} = 1 \times 10^{-2}.\end{aligned} \tag{6.16}$$

The results displayed above confirm that we must estimate the shot-noise at sampling frequency 1 GHz if we hope to precisely estimate excess noise values of the order of 0.01 SNU and additionally provide the statistical precision of about 0.002 SNU in our estimation while doing so.

Naturally these results only concern the statistical precision and do not account for the temporal variations of the shot-noise. The standard deviations displayed in the figure 6.13 account for both effects and can be used to estimate the global precision of the shot-noise estimator. We find that at sampling rate 1 GHz we obtain a precision of

$$\begin{aligned}p_{2\sigma}^{1\text{GHz}} &= 7 \times 10^{-3}\\ p_{3\sigma}^{1\text{GHz}} &= 1 \times 10^{-2}.\end{aligned} \tag{6.17}$$

Difference in electrical gain based on the oscilloscope sampling frequency. We highlighted the necessity to estimate the shot-noise with the oscilloscope running at 1 GHz. However we noticed that the sampling rate also affects the electrical gain of the oscilloscope, therefore the shot-noise estimation performed at 1 GHz is not centered on the same value than the shot-noise estimation performed at 20 GHz. We illustrate this in the left plot in figure 6.14 where we can clearly see the difference in not only the fluctuations, but also for the mean value of the estimation between 1 GHz and 20 GHz sampling rate.

To solve this issue we performed several shot-noise measurements by alternating the sampling frequency of the oscilloscope. Then we computed the ratio between the estimation at 20 GHz and the estimation at 1 GHz and obtained the value

$$R_{20/1} = \frac{\hat{N}_0^{20\text{GHz}}(t)}{\hat{N}_0^{1\text{GHz}}(t)}. \tag{6.18}$$

Then the shot-noise estimator at 20 GHz is computed from the estimator at 1 GHz as

$$\hat{N}_0^{20\text{GHz}} = R_{20/1} \times \hat{N}_0^{1\text{GHz}}(t). \tag{6.19}$$

The value of $R_{20/1}$ is different for both quadratures and is stable as long as the electric cables linking the detectors to the oscilloscope do not move. Every one or two weeks we re-estimate this parameter to verify the value has not shifted.

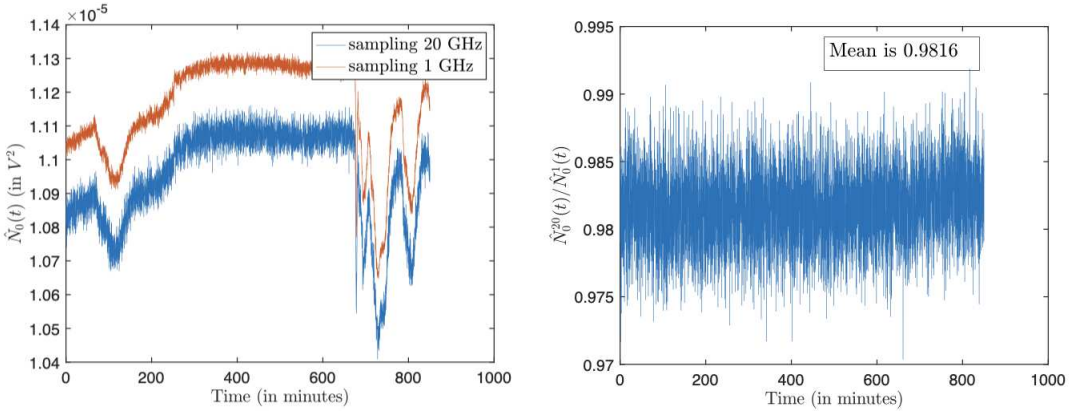


Figure 6.14: (left) We perform shot-noise estimations over night by alternating the oscilloscope sampling frequency between 1 GHz and 20 GHz. We observe that the mean values of the shot-noise estimation in both cases is not the same because the electrical gain of the oscilloscope depends on the sampling frequency. (right) In this plot we show the ratio of the shot-noise estimator at 20 GHz and at 1 GHz. This ratio is relatively stable, but can change if we touch the electrical cables linked to the oscilloscope.

6.3 Digital signal processing

During the DSP stage our aim is to reconstruct the sequence of classical and quantum symbols. The classical symbols will then be demodulated into a bit sequence while we will use the quantum symbols to estimate the excess noise of our transmission. In a real-life implementation the quantum data should also be mapped to a bit sequence to form the raw key, but this is outside the scope of this work where we focus on a proof of concept of joint classical and quantum communications.

We begin the DSP stage after the acquisition of the data retrieved from the oscilloscope, which provides a list of complex samples $\{c(n)\}_{n=1}^{n_{acq}}$ for the classical data and $\{q(n)\}_{n=1}^{n_{acq}}$ for the quantum data. We process the classical data first in order to extract the synchronisation information as well as the phase and frequency estimators used to correct the quantum data.

6.3.1 Classical channel

The DSP applied to the classical channel is for the most part composed of the DSP algorithms discussed in chapter 5. We give the recap of the different transformations here.

Backshifting the classical signal. The first step is to spectrally shift the classical data in order to correct the frequency shift between classical and quantum channels we induced at emission. The frequency shift is given by $\Delta f_{\text{shift}} = f_{\text{shift},c} - f_{\text{shift},q} = 3$ GHz, hence multiply the classical samples as

$$c(n) := c(n) \times \exp\left(-j2\pi n \frac{\Delta f_{\text{shift}}}{f_{acq}}\right) \tag{6.20}$$

RRC filter. We then apply the matched RRC filter directly on the samples such that

$$c(n) := \mathcal{F}^{-1}\left(\mathcal{F}\left(\{c(n)\}_{n=1}^{n_{acq}}\right) \times \mathrm{H}_{RRC}(f)\right) \tag{6.21}$$

where $\mathcal{F}$ stands for the Fourier transform and H_{RRC} is the RRC filter described in chapter 5.

CMA. The CMA corrects many channel impairments and also finds the optimal sampling time for the symbol. As opposed to the 2x2 butterfly FIR filter described in 5.4.1, we do not use the CMA to compensate the polarisation rotations in the fiber since we perform the polarisation separation manually. Here the CMA is operated in "single-input single-output" (SISO) mode and only considers one polarisation.

The number of samples per symbol n_{sa} for the classical data is given by the ratio $n_{sa} = f_{acq}/f_c$ and is equal to 5 in our case. The CMA makes the transition from the set of samples $\{c(n)\}_{n=1}^{n_{acq}}$ to the set of symbols $\{\tilde{c}(k)\}_{k=1}^{n_{symb}}$ using the filter-tap coefficients $\{h(i)\}_{i=0}^{W-1}$ as

$$\tilde{c}(k) = \sum_{i=0}^{W-1} h(i) \times c\Big(n_{sa}k - \lfloor \frac{W}{2} \rfloor + i\Big). \tag{6.22}$$

Recall the CMA is an adaptive equalizer, meaning that the filter-tap coefficients are updated with an error function feedback. As the algorithm runs over the set of samples, the filter-tap coefficients converge towards a constant value and the algorithm is stationary. We use 10 000 symbols to train the algorithm until the filter converges, therefore we simply drop the 10 000 first symbols and only work with remaining ones. For simplicity we conserve the same notation for the number of classical symbols n_{symb}.

Carrier recovery. The next step is the carrier recovery. We first perform the frequency offset estimation and correction using the 4^{th}-power Viterbi and Viterbi algorithm described in 5.4.2. This produces the frequency offset estimator $\hat{f}_\Delta$ which is then used to correct the data :

$$\tilde{c}(k) := \tilde{c}(k) \times \exp\Big(-j2k\pi \frac{\hat{f}_\Delta}{f_c}\Big) \tag{6.23}$$

Following this, we perform the phase estimation using the 4^{th}-power Viterbi and Viterbi algorithm averaged over a large window of 91 symbols. We made the choice of the large window to improve the phase estimation precision because we have ultra-low linewidth lasers, therefore the phase is relatively constant over the averaging window. The algorithm produces a sequence of phases $\{\phi_k\}_{k=1}^{n_{symb}}$ which are then used to correct the data :

$$\tilde{c}(k) := \tilde{c}(k) \times \exp(-j\phi_k) \tag{6.24}$$

BER estimation and sequence beginning. Finally the sequence of symbols is mapped to a sequence of measured bits following the QPSK symbol-to-bits map. With our knowledge of the sequence of bits sent by Alice, we search for correlations between that sequence and the sequence at Bob's. The correlation is maximal when Alice's sequence matches Bob's sequence, thus we find the index k_{start} and the symbol $\tilde{c}(k_{start})$ in Bob's data corresponding to the beginning of the sequence sent by Alice. From the index k_{start} and the number of symbols at Bob's, we can generate the full bit string that was sent by Alice. We compare this bit string with the one at Bob's and measure the BER as the ratio of errors over the total number of bits. After this step, we begin the quantum data DSP.

6.3.2 Down sampling

The first step in the quantum data processing is transposing our set of samples $\{q(n)\}_{n=1}^{n_{acq}}$ in a set of symbols. Since we want to use the phase and frequency estimators derived on the classical channel to correct the quantum data, we must make sure to preserve an equivalence between the two channels. Recall we discarded 10 000 symbols -initially 50 000 samples since we have 5 samples per symbol- on the classical channel corresponding to the CMA training sequence. In order to preserve the equivalence between the data streams, we must also discard 50 000 samples on the quantum channel. However we conserve the notation n_{acq} for simplicity here.

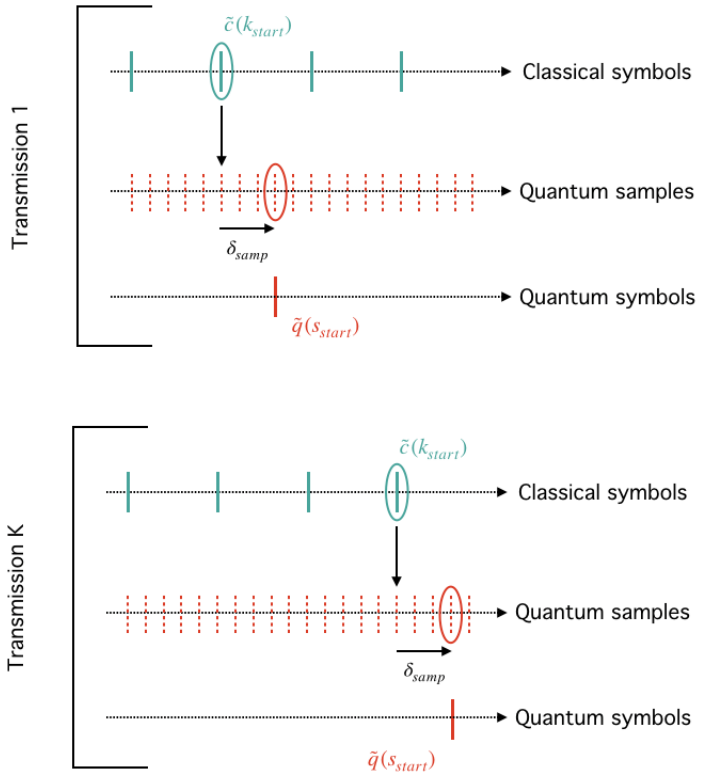


Figure 6.15: Schematic representation of the guided down sampling method. From the beginning of the classical sequence, we find the sample corresponding to the beginning of the quantum sequence. The optimal sample choice for the first quantum symbol is located at constant distance δ_{samp} of this sample. We can then sample the full quantum sequence starting from the first symbol.

We down sample the signal from $f_{acq}/f_q = n_{sa,q} = 80$ samples per symbol to 1 sample per symbol. Since we clearly oversample the quantum channel, our approach is to select the one sample closest to the optimal sampling instant. For this we have different methods discussed below.

Guided down sampling. Assuming the synchronisation between both channel holds, the beginning of the quantum sequence matches the beginning of the classical sequence. Hence the position of the optimal sample for the first quantum symbol should be the same relative to the first classical symbol over multiple acquisitions. We illustrate this idea in figure 6.15 and describe the process here. First we know the index k_{start} corresponding to the beginning of the classical data sequence. Therefore we know that the first sample of the quantum sequence is $q(n_{sa} \times k_{start})$. Since the channels are synchronised, the optimal sample for the beginning of the quantum sequence is $\tilde{q}(s_{start}) = q(n_{sa} \times k_{start} + \delta_{samp})$ where the optimal shift δ_{samp} is constant over multiple acquisitions. We can then create the set of quantum symbols by taking every $n_{sa,q}$ sample forward and backwards to generate the set of quantum symbols $\{\tilde{q}(s)\}_{s=1}^{n_{symb,q}}$.

The question remains on how to gain knowledge of δ_{samp}. To do this we run the protocol once operating the quantum signal in the classical regime. When the classical DSP is finished, we try all possible values for $\delta_{samp} \in \{0, n_{sa,q} - 1\}$ and select the value which minimizes our error function. Said error function is inspired from the CMA in classical coherent communications as we look to minimize the intra-symbol variance of the signal modulus. When Alice employs a QPSK modulation this is easy : since all the symbols of the constellation have the same modulus, we simply select the sample which minimizes the variance of the signal modulus. When the PCS-64QAM constellation is employed, we must first group the sequence of symbols at Bob's depending on which symbol was sent by Alice. Then we take the value of δ_{samp} which minimizes the average variance of the modulus of all symbols in the sequence corresponding to the same 64-QAM symbol sent by Alice.

Pulses. The second way to down sample the signal is to carve pulses on the quantum signal instead of operating the channel with continuous-wave light. This way, we can simply select the one out of $n_{sa,q}$ possible samplings which maximize the detected power.

Exhaustive search. The final downsampling approach is simply to test all downsampling possibilities (among $n_{sa,q} = 80$) and select the one which provides the best excess noise measurements. While computationally intensive, this method is useful to verify whether the system behaves as we expect.

During the course of this work we first modulated the quantum states according to a QPSK modulation, and then scaled up the constellation to a PCS-64QAM. In the case of the QPSK modulation we used exclusively the guided down sampling method. This method functions regardless of the quantum signal power thus it can effectively down sample a very low-intensity signal, as is required for the security of QKD using a QPSK modulation. When we shifted to the PCS-64QAM, we continued using the guided down sampling but also verified our results with the exhaustive search. The implementation of pulses is ongoing at the time this is written.

6.3.3 Frequency and phase correction

Following downsampling, we use the frequency and phase estimators computed on the classical channel to correct the quantum data. First the frequency offset is corrected as

$$\tilde{q}(s) := \tilde{q}(s) \times \exp\left(- j2s\pi \frac{\hat{f}_\Delta}{f_q} \right). \tag{6.25}$$

Then we proceed to the phase correction. Given the set of classical symbol phases $\{\phi_k\}_{k=1}^{n_{symb}}$, we average the ϕ_k over groups of length $f_c/f_q = 16$ in order to produce the set of quantum symbol phases $\{\theta_s\}_{s=1}^{n_{symb,q}}$. We then correct the quantum data phases :

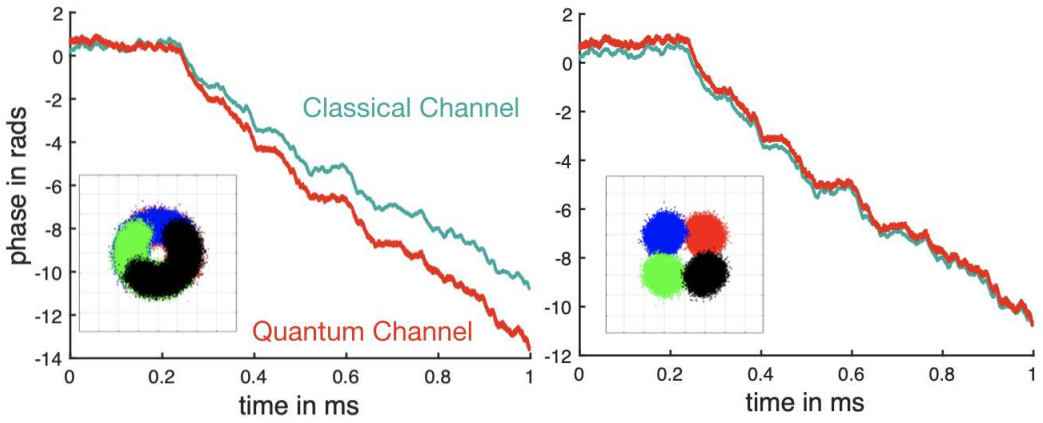


Figure 6.16: (left) Phase evolution of the classical and quantum signals over time after compensation of the frequency offset $\hat{f}_\Delta$. We observe there remains a frequency offset between both channels which induces a rotation of the constellation points showed in inset. (right) We show the same graph after using our residual frequency offset compensation algorithm. It efficiently compensates the residual offset therefore correcting the constellation rotation such that we can clearly observe the 4 QPSK symbols.

$$\tilde{q}(s) := \tilde{q}(s) \times \exp(-j\theta_s). \tag{6.26}$$

Ideally the carrier recovery for the quantum signal would end here. However we observe that there remains a residual frequency offset in the quantum data which causes a rotation of the constellation and considerably increases the excess noise estimation. To see this consider the left graph of figure 6.16. Here we operate both channels in the classical regime and we perform the full DSP of the classical channel. Then we down sample the quantum signal and correct the frequency offset with the estimator computed on the classical channel. Since both channels are operated in the classical regime, we can use the Viterbi & Viterbi phase estimation algorithm on both channels to compare their phase evolution over time. We see that there is a time-dependant linear offset between the phases on the quantum channel and on the classical channel, which corresponds to the residual frequency offset we mentioned. The inset shows the QPSK constellation we obtain after the DSP step of equation 6.26, illustrating the rotation of the constellation points.

Cause behind the residual frequency offset. We can understand this phenomenon by returning to the beginning of the classical DSP. We start by backshifting the classical channel by 3 GHz such that the central frequency of classical and quantum data matches, this way the frequency offset estimator computed on the classical channel will also be the frequency offset for the quantum signal. However this assumes that the difference in the central frequency of the quantum and classical spectra is *exactly* 3 GHz. In reality the AWGs do not have a common clock reference with the oscilloscope used for the measurement, therefore what is 3 GHz for the clock reference at Alice can appear to be different with the clock reference at Bob's.

Besides the reference clock difference, another cause to the residual frequency offset is caused by the clock jitter in Alice's system. The stability of clocks in electronic devices, which is never perfect, is usually expressed in *parts per million* or ppm. This quantifies the average difference of the number of samples the device outputs compared to the ideal case over a million samples. Our reference clock at Alice has a precision of 1 ppm, which means that our output signal has a frequency precision of 10^{-6}. Therefore we achieve our target frequency shift of 3 GHz with a precision of 3 kHz.

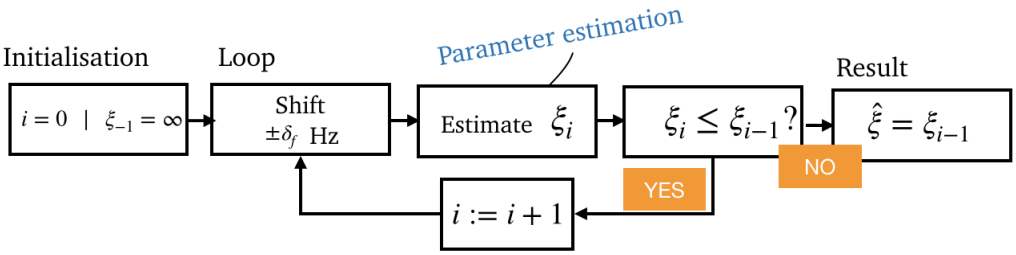


Figure 6.17: The residual frequency offset compensation algorithm exploits the parameter estimation phase of the QKD protocol. Bob performs a +5 Hz and a -5 Hz incremental rotation of his data until he reaches a local minimum for the excess noise estimator. When he does, the total frequency correction performed on his data is the residual frequency offset.

Correcting the residual frequency offset. This problem is unavoidable in all architectures for which the quantum carrier frequency is estimated from a frequency multiplexed signal. To solve this, we found in the literature [84] a method consisting in sending two pilot tones instead of one. By estimating the frequency offset between both pilots the authors track the clock fluctuations and correct the frequency offset term. However we propose a new approach to this problem without the need to engineer additional reference signals. We exploit the parameter estimation phase of the QKD protocol. Instead of revealing his symbols at the same time than Alice, Bob uses the information disclosed by Alice to correct the frequency offset in his data. He does this by implementing a $\pm\delta_f$ incremental frequency shifts to his constellation, looking to minimize the excess noise estimator. While the excess noise estimator decreases he continues rotating his data until he reaches a local minimum. For our work we chose $\delta_f = 5$ Hz since we did not notice any particular advantage when increasing the granularity of the search. This algorithm is represented in figure 6.17. The right graph in figure 6.16 shows the phase evolution of classical and quantum signals after correction by our algorithm. We observe it matches for both channels, and efficiently corrects the distortion of the constellation, which is showed in inset.

Residual phase offset. After all impairments have been corrected, there remains a phase offset on the quantum constellation. This is easily corrected using a method similar to the residual frequency offset compensation algorithm. We rotate all quantum symbols by an incremental phase shift until the excess noise estimator is minimal.

6.3.4 Parameter estimation

The goal of the parameter estimation is to compute an estimator for the excess noise over the transmission.

Excess noise estimator. Let us denote the sequence of symbols sent by Alice by $\{\tilde{a}(s)\}_{s=1}^{n_{acq}/n_{sa,q}}$ where each symbol is the realization of a random variable A with variance V_A in SNU. The theoretical variance of Bob's data is given from the different experimental parameters as

$$V_B = \frac{T}{2}V_A + 1 + \nu_{el} + \frac{\xi}{2}. \tag{6.27}$$

By taking the conditional variance of Bob's data, we find the following relation to express the excess noise

$$\xi = 2 \times (V_{B|A} - 1 - \nu_{el}). \tag{6.28}$$

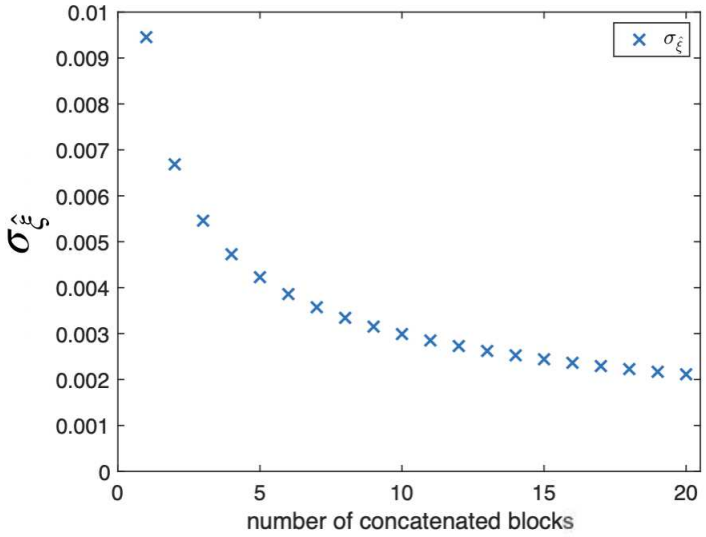


Figure 6.18: Evolution of $\sigma_{\hat{\xi}}$ as a function of the number of blocks averaged to build $\hat{\xi}$. We can increase precision of the excess noise estimation by concatenating several blocks.

We build the excess noise estimator by replacing the theoretical values above by the corresponding estimators. We compute $\hat{V}_{B|A}$ by taking the intra-symbol variance of Bob's data. This amounts to grouping the quantum symbols based on the symbol sent by Alice to generate the group of symbols $Q_a = \{\tilde{q}(s)/\tilde{a}(s) = a\}$. There are therefore 4 groups when we use the QPSK modulation and 64 groups for the PCS-64QAM modulation. Then we can compute the conditional variance of the quadratures given symbol a was sent $\hat{V}_{B|A=a} = \mathrm{Var}(\mathbb{Re}[Q_a]) = \mathrm{Var}(\mathbb{Im}[Q_a])$. Finally we obtain the conditional variance estimator given by

$$\hat{V}_{B|A} = \sum_a p(a) V_{B|A=a}, \tag{6.29}$$

where the $p(a)$ are the experimental probabilities for each symbol equal to 1/4 for the QPSK modulation format and displayed in figure 6.4 for the PCS-64QAM modulation format.

Precision of the excess noise estimator. The overall precision of our excess noise estimation depends on the one hand of the statistical effects in the estimation of $\hat{V}_{B|A}$ and on the other hand on the precision on the shot-noise calibration. We discuss these here.

- *Statistical precision of* $\hat{V}_{B|A}$. Similarly to the methodology we detailed for the shot-noise estimation, the estimator of $\hat{V}_{B|A}$ can be approached by a Gaussian random variable with mean value $V_{B|A}$ and variance $\frac{2}{n_q} V_{B|A}^2$ where n_q is the number of quantum symbols used for the estimation. Considering the excess noise is orders of magnitude below the shot-noise, and using our previous approximation of $\nu_{el} = 0.1$ SNU, let us approximate the variance due to statistical effects of $\hat{V}_{B|A}$, expressed in SNU^2, as :

$$\mathrm{Var}(\hat{V}_{B|A})_{stat} = \frac{2}{n_q} \times 1.21. \tag{6.30}$$

- *Precision on the shot-noise calibration.* Since we are in shot-noise units, subtracting the contribution of the shot-noise to the total noise is achieved by subtracting 1 SNU. This can be misleading because it looks as if we can always subtract the contribution of the shot-noise when

in reality the variance in the shot-noise calibration is transferred to the excess noise measurement. This term dominates the precision on the electronic noise measurement such that the variance of the excess noise estimator due to imperfect calibration is expressed as :

$$\mathrm{Var}(\hat{\xi})_{calib} = 4 \times \mathrm{Var}(\Delta\hat{N}_0), \tag{6.31}$$

In total, the variance of the excess noise estimation is the sum of the variances induced by the statistical effect and by the calibration, such that

$$\mathrm{Var}(\hat{\xi}) = 4 \times \left(\mathrm{Var}(\hat{V}_{B|A})_{stat} + \mathrm{Var}(\Delta\hat{N}_0)\right) \tag{6.32}$$

Let us now investigate the precision we can achieve over one acquisition and by averaging multiple acquisitions. In one acquisition with 10 Mpts we have $n_q = 124\ 375$ symbols, which yields, according to 6.30 and to the variance of $\Delta\hat{N}_0$ determined experimentally in figure 6.11, the standard deviation for the excess noise estimator :

$$\sigma_{\hat{\xi}_{ch}} = 0.0095 \tag{6.33}$$

This value can be improved upon by averaging excess noise estimators over multiple blocks, which will result in dividing the standard deviation of $\hat{\xi}$ by the square root of the number of blocks. We give the evolution of $\sigma_{\hat{\xi}}$ as a function of the number of blocks in the figure 6.18.

6.4 Parameter optimisation and results

Now that we have described how to operate the joint quantum and classical coherent communication experiment, let us discuss how we chose our experimental parameters for both experiments and the results obtained

6.4.1 Quantum channel power

The modulation variance V_A used on the quantum channel should be chosen as to maximise the key rate. This value greatly depends on the modulation format employed, but also on the targeted distance and on the expected excess noise. In figure 6.19 we plot the theoretical key rates for both the QPSK and PCS-64QAM formats for different distances. The plot for the QPSK modulation, which is obtained via solving the SDP defined in reference [52], was also taken from this reference. We plotted the data corresponding to the PCS-64QAM format using code provided by the authors of [48].

QPSK. Using the QPSK modulation the optimal coherent state amplitude is of about $\alpha = 0.5$ at 20 km corresponding to $V_A = 2\alpha^2 = 0.5$. We will operate our experiment over 15 km, hence the optimal value of V_A is possibly higher. However we observe it does not vary very much which the distance when looking at the plots for the larger distances of 50, 80 and 100 km. We will assume 0.5 is the optimal modulation variance in our case.

PCS-64QAM. Compared to QPSK, the PCS-64QAM format tolerates larger modulation variances. It seems the optimal V_A in this case is around $V_A = 5$ and does not depends very much on the distance and on the excess noise in the range of parameters investigated.

6.4.2 Classical channel power

After optimising the quantum channel modulation variance, we investigate the effect of the classical channel on the performance of the protocol. The power of the classical channel, P_c, has a threefold impact we discuss below.

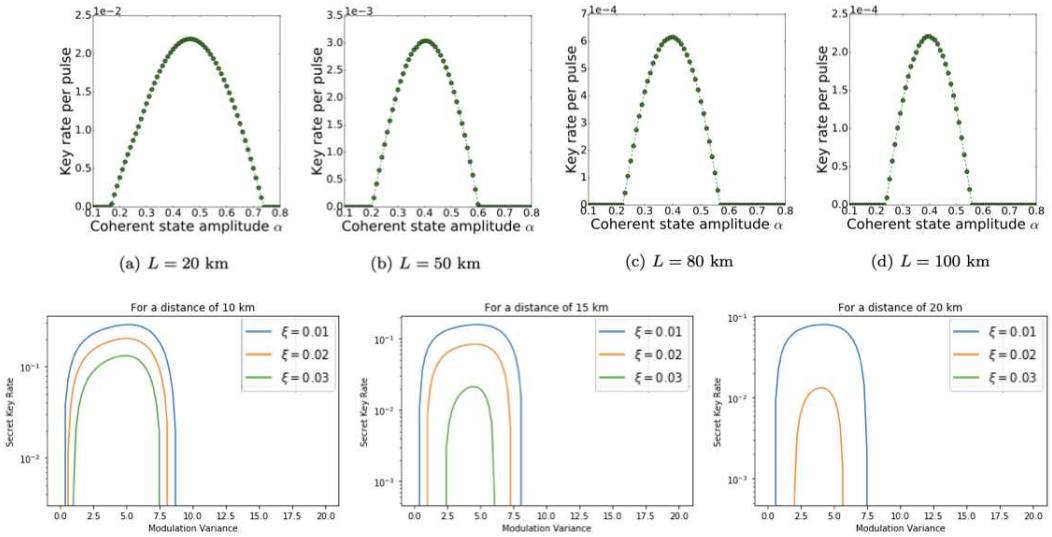


Figure 6.19: (top) Key rate per symbol using the QPSK modulation versus the coherent state amplitude. Plot taken from reference [52]. The excess noise at Alice was set at $\xi_A = 0.01$ SNU, hence the excess noise at Bob's is defined by $\xi_B = 10^{-0.02\times d}\xi_A$ where d is the distance. (bottom) Key rate per symbol using the PCS-64QAM modulation versus the modulation variance for 3 values of excess noise, defined at Alice.

Leakage on the quantum channel. The classical channel is multiplexed in frequency and polarisation with the quantum channel. However the components used to polarisation multiplex both signals, for example the PBS and the dual-polarisation I/Q modulator, have a finite *polarisation extinction ratio* (PER). This means there is necessarily some power from the classical channel which will leak on the quantum channel and generate excess noise. In addition to the finite PER, the components set manually always suffer from slight misalignment from their optimal position which generates more leakage from one channel to the other. The frequency offset between both channels generates additional extinction by shifting the classical data outside of the bandwidth of the quantum receivers, but unfortunately the classical channel will still generate excess noise on the quantum signal. We can write the excess noise due to the leakage of the classical channel, noted ξ_{leak}, in a general way as

$$\xi_{\text{leak}} = e_{\text{cq}} P_c \tag{6.34}$$

where e_{cq} is a parameter representing the total extinction between the channels, which is in general not constant during the course of the experiment due to shifts in polarisation and the free-running signal and LO which modifies the frequency offset and hence the extinction obtained via the frequency degree of freedom.

In the figure 6.20, we plot the value of ξ_{leak} for different values of P_c by regularly calibrating the LO frequency offset and the polarisation controllers. This plot highlights the linear relation between P_c and ξ_{leak} and gives some insight as to what value of ξ_{leak} we should expect.

Precision of phase recovery. The phase recovery procedure is performed on the classical data for both the classical and quantum channels. Its goal is to provide an estimator $\hat{\phi}$ for the relative phase between signal and LO ϕ. The precision of $\hat{phi}$ depends on the noise on the classical channel during the Viterbi & Viterbi phase recovery algorithm, σ_c^2, and on P_c. It can be written as [20]

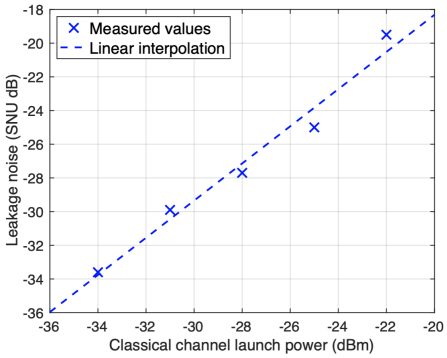


Figure 6.20: Excess noise due to the leakage of the classical signal on the quantum data. To plot this graph we cut the modulation on the quantum channel and compared the noise levels -in SNU- with and without the classical signal.

$$\Delta\phi = \frac{\sigma_c^2}{P_c}, \tag{6.35}$$

where $\Delta\phi = \mathrm{Var}(\phi - \hat{\phi})$ is the variance of the residual phase after correction and is inversely proportional to P_c. In the case of small $\Delta\phi$ this can be translated into a quadrature variance on the quantum channel as

$$\xi_{\mathrm{phase}} = TV_A\Delta\phi. \tag{6.36}$$

Therefore the excess noise due to imperfect phase recovery is inversely proportional to P_c. From the results obtained in figure 6.20, we can determine an approximately optimal value of P_c based on the measured excess noise. If the leakage noise is dominant, *i.e.* the measured ξ is approximately equal to the expected leakage noise, then it means we should reduce the P_c. On the other hand if we find excess noise values much larger than the expected leakage noise, then we should increase P_c to reduce the imperfect phase recovery noise.

Classical BER. The BER on the classical channel is directly correlated to P_c. Since we are designing a joint classical and quantum communication system we must insure that we provide reliable classical communications. A particularly useful tool for this is forward error correction (FEC) which consists in introducing some redundancy bits in the communication to correct any errors below a certain threshold. To be conservative, we assume a raw BER of 10^{-2} can be corrected with a 20% overhead on the data. Hence we will assume that if we achieve an experimental BER below this threshold we have achieved reliable classical communications.

6.4.3 Results

We operated our hybrid classical and quantum communication system during one hour and measured the classical BER and the excess noise on the quantum channel. The set of parameters, measurement results and expected key rates are displayed in the table 6.2. The excess noise for each modulation is taken as the average over all measurements, which are plotted in the figure 6.21.

Discussion. We performed two experimental demonstrations of a joint quantum and classical transmission over one fiber, using either a PCS-64QAM or a QPSK modulation format on the quantum channel. We exploited the fixed phase and frequency relation between classical and quantum channels, due to them originating from the same laser, to perform the DSP on both channels using the estimators

	QPSK	PCS-64QAM
V_A (SNU)	0.5	5
P_c (dBm)	-30	-22
distance (km)	15	10
ξ (SNU)	0.009	0.0212
ν_{el} (SNU)	0.09	0.09
BER	1.10^{-4}	$\leq 1.10^{-7}$
Key rate (Mbps)	14	18.5
Security proof	[52]	[48]
Finite-size effects	No	Yes

Table 6.2: Comparison of the parameters used and experimental results for both experiments with different modulation formats on the quantum channel.

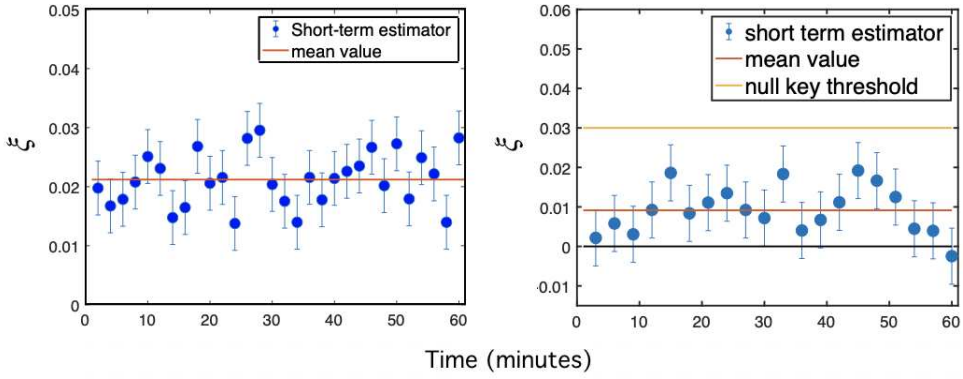


Figure 6.21: Excess noise measurement performed during one hour with the PCS-64QAM format (left) and the QPSK modulation format (right) on the quantum data. Each point is the average excess noise taken over 3 blocks of 124375 symbols. The statistical error bars at 3 σ are displayed.

computed on the classical channel. Hence, we did not need to generate dedicated pilot tones to solve the carrier recovery problem on the quantum channel.

With the QPSK modulation, we had to set the quantum channel power to an extremely weak value of $V_A = 0.5$ in order to stick to the optimal values of the security proof used. In this regime the phase noise is not as dominant as for higher values of V_A therefore it was advantageous to operate the experiment with a low value of P_c to minimise ξ_{leak} which we expected would play a significant role in our total excess noise measurement. With the chosen classical channel launch power of $P_c = -30$ dBm, the BER is below the FEC threshold therefore reliable classical communication is achievable at rate 3.2 Gbps assuming a 20% FEC overhead. Our low average excess noise of 0.009 SNU allowed us to infer our secret key rate of 14 Mbps from the data provided in reference [52], which we transposed in this manuscript in the figure 4.2 (left). This first experiment yielded encouraging results of a joint classical and quantum communication system over the same fiber and importantly of the benefits the classical channel could provide upon the quantum data. Beyond the carrier recovery, important synchronisation information was also retrieved from the classical data which enabled the sampling of the very weak quantum signal.

However a few frustrations remained as to the regime of parameters used for the experiment. First, the very weak value of V_A insures that at larger distances the SNR will essentially go to 0 and no secret key will be obtainable. Also the very high sensitivity of the key rate to the excess noise value causes the secret key rate to vanish when we take into consideration the worst-case estimator in the finite-size regime. Finally, the classical channel was operated at a very low power, far from typical values observed in coherent communication systems. During the course of this thesis, new security proofs [48] provided tools to easily compute key rates for arbitrary modulations and showed that key rates approaching the Gaussian modulation could be achieved using the PCS-QAM format with a limited number of states, starting from 64. Hence we set out improve the range of parameters used in the experiment with this modulation format.

With the PCS-64QAM format, the optimal value of $V_A = 5$ is 10 times what is was previously. This means, according to our model 6.36, that the phase noise will play a significant larger role compared to before. We increase P_c by a factor ~ 6 to mitigate the increase in ξ_{phase} but induce additional ξ_{leak} by doing so. Therefore we naturally obtain a larger value of $\xi = 0.0212$ SNU in this regime, but this is tolerated by the security proof. Our experimental data is compatible with a secret key rate of 18.5 Mbps with the worst-case estimator and the privacy amplification penalty due to the finite-size effects. Although we had to reduce our communication link to 10 km to maintain a positive key rate in the finite-size regime, our results are compatible with a key rate of 44 Mbps at 15 km and enable key distillation up to approximately 40 km in the asymptotic regime. These results prove that hybrid quantum and classical systems can coexist and be designed such that they are beneficial to the QKD channel. Future designs of joint systems could even use the secret key obtained during the QKD protocol to encode some of the classical symbols leading to symbiotic operation of joint quantum and classical communications.

6.4.4 Improvement perspectives

The results presented here constitute an encouraging proof-of-concept of the designs of hybrid communication systems. For future work, we strongly believe these results can be improved on, perhaps drastically, by exploring a few direction we would like to discuss here.

Polarisation control. A first step towards improving the experiment would involve deploying automatic polarisation controllers at Alice and Bob's in order to maintain the SOP at the optimal setting over the course of the transmission. This is crucial not only for performance, but also for consistent repeatability of the experiment and efficient optimization of the other experimental parameters.

Synchronisation. We believe the synchronisation of the two AWGs generates instability and perhaps additional noise. First, the fact that AWG2 emits periodically makes it rather difficult to

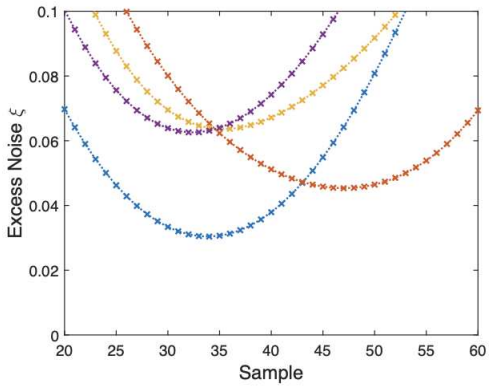


Figure 6.22: To plot this graph we ran several iterations of the acquisition loop. When it came to down sampling the quantum data, we computed the excess noise for every sample before and after the optimal sampling instant determined during the guided down sampling. Then we plotted the results as a function of the sample used for the rest of the DSP. Here each color corresponds to one acquisition. We centered the optimal sampling instant at 40 samples. We observe that the true optimal sampling instant -for which the excess noise is minimal- is not consistently at 40 samples, but rather fluctuates around this value.

adapt the voltage biases to the drifts in the IQ modulator. This is because we tune the biases based on what is observed on the optical spectrum analyser, therefore if the signal alternates between on and off it is impossible to achieve a fine tuning. Hence we often perform the experiment with a stronger residual carrier than what is possible with our modulator, which undoubtedly generates noise on the quantum channel, especially when it is the Y-polarisation setting that drifts since that is the polarisation allocated to the quantum data. The effect of the drifts in the optimal voltage biases for the IQ modulator can be seen in the figure 6.6.

Another effect of the periodic emission of the AWG2 is that this adds a delay between a shot-noise estimation and a data block estimation, since we must wait for the AWG2 to emit after the shot-noise block was acquired. This time-delay increases the variance of the shot-noise estimator $\Delta\hat{N}_0$ and therefore increases the fluctuations in the total experiment. Continuous emission and synchronisation would solve both these problems as we could set the voltage biases during the experiment because the spectrum would be constant and we could perform the data acquisition, following the shot-noise estimation, as soon as the oscilloscope is ready to acquire another block.

The second detrimental effect stemming from the synchronisation is that it seems like the optimal sampling instant for the quantum data relative to the classical channel is not constant over time like we thought. This is illustrated in the figure 6.22. If perfect synchronisation was achieved at Alice, it is possible some fluctuation of the optimal sampling instant would remain of the order of a couple samples, perhaps up to 5 samples corresponding to a classical symbol duration. However we observe that the optimal sampling instant can vary over more than 3 or 4 classical symbols over successive acquisitions. We believe this is due to a synchronisation problem and that the it would disappear if we could operate one AWG with 4 outputs for the I and Q components of both polarisations.

Filtering Also from figure 6.22 we can observe the strong coherence between two successive samples, since the sampling time (20 GHz) is much higher that the system variations (350 MHz). Therefore it should be possible to build a filter, in the spirit of a FIR filter discussed in 5.4.1, to build our quantum symbol from several samples. We believe this could mitigate some noise but the question of how to design the filter remains open.

DSP. A final point of improvement for this work would be the deployment of DSP routines which

perform better than the ones employed here. In particular for carrier recovery, machine learning has been shown to perform better than other methods [85] and has already been applied to improve the performance of CV-QKD protocols [82].

6.4.5 Conclusion

The experimental work proposed here demonstrates that the design of hybrid communications systems can be beneficial to the quantum communication since efficient carrier recovery can be performed on the classical channel. As a bonus, the classical channel also provides all the information needed to downsample and synchronise the transmitted and received sequence. We strongly believe the results displayed here can be improved upon significantly by implementing the leads discussed above, which promises even better results in the future. In general, performing QKD on classical communication links is challenging, hence building classical and quantum communication systems together can give more tools to optimize the secret key rate and the classical communication rate.

Chapter 7

Covert quantum key distribution

Contents

In the previous section we demonstrated a proof-of-principle experiment for joint quantum and classical communications based on exploiting the coexistence to benefit both channels. In particular we showed that the classical channel can provide good estimators for the quantum phase and frequency recovery and we also suggested that the secret key obtained via the QKD protocol could be used to encrypt a fraction, if not all, of the classical symbols.

In this chapter we discuss another way to beneficially harness the coexistence between channels. In layman terms, we investigate how to "hide" the quantum signals in the noise generated by classical channels such that it is indistinguishable from background noise for an eavesdropper. This provide an interesting new security primitive to the quantum communication system : covertness.

7.1 Introduction to covert communications

Covert communications consist in making the communication indistinguishable from background noise for anyone except the legitimate receiver. The motivation behind this security primitive can stem from the metadata leaked during a communication protocol that can be security sensitive. Actually there exists communication scenarios (e.g. in a dictatorship) where the mere fact of communicating between two parties must be concealed, for security reasons. In particular the realisation of a QKD protocol, aimed at providing ultra-secure keys for extremely sensitive communications, may attract even more the attention of the "dictator" than classical communications. In this case the dictator, Eve, could potentially correlate the realisation of the QKD protocol to the intentions of Alice and Bob. It is

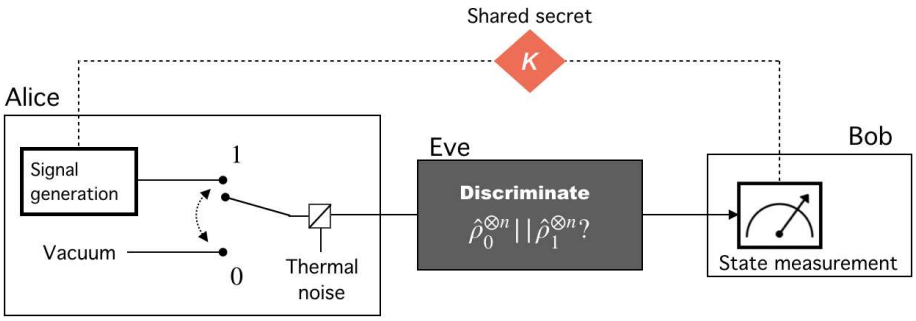


Figure 7.1: Covert communication setup : Alice either communicates or not with equal probability. The communication is comprised of n states. In both scenarios, thermal channel noise is present and is outside of Eve's control. For this reason we represent the thermal noise inside Alice's lab. Also, Alice and Bob share a secret K before starting the protocol.

therefore interesting to investigate how we can prevent Eve from knowing that Alice and Bob are running a QKD protocol, i.e. whether QKD can be run in a covert manner.

Setting for covert communications. A covert communication protocol can be described as follows. Alice and Bob are linked by a quantum channel over which the average state transiting from Alice to Bob's is denoted $\hat{\rho}_0$. This state is called the idle state and corresponds to the background noise on the channel. During the communication phase Alice will send a total of n symbols to Bob. The average state on the channel during the communication is written $\hat{\rho}_1^{\otimes n}$. We assume that from Eve perspective it is equally likely for Alice to communicate or not during a given time interval, hence for her the states $\hat{\rho}_0^{\otimes n}$ and $\hat{\rho}_1^{\otimes n}$ are equally likely. The communication is said to be δ-*covert*, where $\delta > 0$, if we can bound the probability that Eve can distinguish between these two states by

$$\mathbb{P}_e \geq 1/2 - \delta. \tag{7.1}$$

The factor δ is called the detection bias. We give a depiction of the setting of a covert communication protocol in the figure 7.1.

Important results of covert communications. The main result in the field is the so-called "square-root law" which states that the number of covert bits that can be transmitted scales as $\mathcal{O}(\sqrt{n})$ [86]. The intuition behind the square-root law is the mathematics of statistical testing and the central limit theorem insuring that Eve's observations will have uncertainty of magnitude $1/\sqrt{n}$. Covert communications have been investigated against a classical [87, 88, 89] and even a quantum adversary [90, 91]. In both cases the square-root law holds. In addition these works have put into light two prerequisites to any covert communication scheme :

1. There must be some noise outside of adversarial control.
2. Alice and Bob must share some secret K of sufficient length before the protocol.

These two conditions can be well understood intuitively. The first stems from the fact that if all the noise is due to Eve, then she could suppress the noise and therefore detect the communication with a basic power test using perfect detectors. This contrasts with the golden standard of QKD where all noise is attributed to the eavesdropper and we will discuss further how we envision covert QKD in this context. The second point is necessary for Alice and Bob to retrieve information from the noise-like signal and we will give an example below of how the shared secret is used.

Covert QKD. A crucial question for covert QKD protocols is whether a covert QKD protocol can generate more secret key than the one used by Alice and Bob during the protocol. Previous works [92, 93] have worked towards designing covert key expansion protocols with δ-covertness and ϵ-security such that this is the case, but only achieve a limited range of channel parameters which are not useful in practice.

Another approach was investigated in [94], where the authors modify a discrete-variable BB84 protocol so that the communication is also covert. They achieve this by spreading the communication states over a large transmission interval and attribute to each time-bin a qubit transmission probability $q << 1$. In this case the communication state from Eve's perspective is the mixed state $(q\hat{\rho}_1 + (1-q)\hat{\rho}_0)^{\otimes n}$ which can be be made arbitrarily close to the idle state by decreasing q. The secret shared by Alice and Bob designates the time bins containing the signal so Bob can perform his regular QKD measurement. However the shared secret length necessary to identify the signal time-bins dominates the amount of covert secret bits that can be produced. The authors therefore rely on a computational solution to distribute the shared secret, in the form of Pseudo-Random Number Generators (PRNGs). This leads to a hybrid protocol where the distilled key has the same information-theoretical security (ITS) than a regular QKD protocol -because the keyrate analysis supposes Eve knows the time-bins containing QKD states- while its covertness is insured under the two conditions that the shared key generated via the PRNG is unknown to Eve and that the noise used for covertness is in fact outside of her control.

We believe this hybrid computational/ITS approach to covert QKD is the most practical approach towards designing such systems, but has not been investigated in the case of CV-QKD. As we discussed in section 4.4.3, these protocols are promising candidates for QKD in a WDM environment where unavoidable Raman noise will hinder the keyrate but could be used to achieve covertness [95]. If successful our results would provide another way to harness the coexistence between quantum and classical data and pave the way towards new designs of joint communication systems.

In the next section we begin by deriving a condition on the modulation variance of the quantum data so that the communication is δ-covert. We show that covert CV-QKD without using some shared secret to give an advantage to Alice and Bob does not allow to share a covert secret key. Hence we move on in the next sections to derive a way to harness the shared secret resource for CV-QKD systems, but show that the square-root law still limits the amount of covert and secret bits that can be transmitted. Then, we propose practical models where the square-root law can be relaxed and therefore in which covert QKD is easily achievable.

7.2 Covert analysis of CV-QKD

Let us investigate the conditions under which the PM states sent by Alice obey the δ-covertness condition of equation 7.1.

7.2.1 From QKD parameters to idle and communication states

In this work we will focus on the case Alice and Bob use the GG02 protocol, described in 4.1.1, where Alice uses modulation variance V_A and Bob measures excess noise $T\xi_A$. Compared to our previous convention to define the excess noise at the channel output, here we will see it is more practical to define it at the channel input to perform the covert analysis.

We make the additional assumption that the channel noise is due to a thermal state with mean photon number $\bar{n}_{\text{th}}$. This is convenient for the rest of the analysis since the average state in the GG02 protocol can also be written as a thermal state with mean photon number $\bar{n}_A$. The relation between QKD parameters and mean photon number is given by [20]

$$V_A = 2\bar{n}_A, \tag{7.2}$$
$$\xi = 2\bar{n}_{\text{th}}.$$

The innocent and communication states are therefore written as :

$$\hat{\rho}_0^{\otimes n} = \left(\sum_{i=0}^{\infty} \frac{\bar{n}_{\text{th}}^i}{(1+\bar{n}_{\text{th}})^{1+i}} |i\rangle \langle i| \right)^{\otimes n}. \tag{7.3}$$

$$\hat{\rho}_1^{\otimes n} = \left(\sum_{i=0}^{\infty} \frac{(\bar{n}_{\text{th}}+\bar{n}_A)^i}{(1+(\bar{n}_{\text{th}}+\bar{n}_A))^{1+i}} |i\rangle \langle i| \right)^{\otimes n}. \tag{7.4}$$

7.2.2 Condition on V_A for δ-covertness

To find the desired condition on V_A we look to bound the probability of Eve discriminating between the innocent and communication states. Her best strategy is to build a binary POVM $(\hat{\Lambda}_0, \hat{\Lambda}_1)$ to perform her discrimination. She can make two types of errors while doing this. The first is when she raises a false alarm, also called a type I error in statistical testing. The second is when she misses detection of the communication state, or type II error. Let $\mathbb{P}_{\text{FA}}$ and $\mathbb{P}_{\text{MD}}$ be the respective probabilities of these events. We can express these quantities as

$$P_{\text{FA}} = \text{Tr}\big[\hat{\Lambda}_1 \hat{\rho}_0^{\otimes n}\big], \tag{7.5}$$
$$P_{\text{MD}} = \text{Tr}\big[\hat{\Lambda}_0 \hat{\rho}_1^{\otimes n}\big]. \tag{7.6}$$

Since we assumed communication and idle states were equally likely from Eve's perspective, we can write the total error probability we are looking to bound as

$$\mathbb{P}_e = \frac{1}{2}(P_{\text{FA}} + P_{\text{MD}}). \tag{7.7}$$

Combining (7.5) and (7.6) into (7.7) and substituting $\hat{\Lambda}_1 = \hat{I} - \hat{\Lambda}_0$ gives

$$\mathbb{P}_e = \frac{1}{2} - \frac{1}{2}\,\text{Tr}\big[\hat{\Lambda}_0(\hat{\rho}_0^{\otimes n} - \hat{\rho}_1^{\otimes n})\big]. \tag{7.8}$$

The term on the far right can be successively bounded by the trace distance and the quantum relative entropy [1] [96] which finally gives :

$$\mathbb{P}_e \geq \frac{1}{2} - \sqrt{\frac{1}{8} D(\hat{\rho}_0^{\otimes n} || \hat{\rho}_1^{\otimes n})} \tag{7.9}$$

A nice property of the quantum relative entropy is that it is additive for tensor product states [96]. Hence given the equation above we find that the condition

$$D(\hat{\rho}_0 || \hat{\rho}_1) < \frac{8\delta^2}{n} \tag{7.10}$$

Is sufficient to insure the δ-covertness condition of equation 7.1. The quantum relative entropy between these states can be shown to be upper bounded by (for derivation see annex A) :

$$D(\hat{\rho}_0 || \hat{\rho}_1) \leq \frac{\bar{n}_A^2}{2\bar{n}_{\text{th}}(1+\bar{n}_{\text{th}})} \tag{7.11}$$

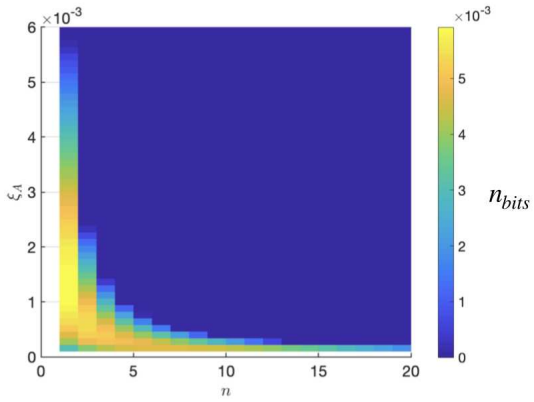


Figure 7.2: Total number of covert and secret bits ($n \times r$) obtained via the covert GG02 protocol with the constraint in equation 7.12. We run the simulation over both parameters ξ and n to show that there is no good regime allowing a significant amount of bits to be obtained. This plot constitutes an upper-bound to what can be achieved in practical scenarios since the transmittance was taken as $T = 0.99$ and performance decreases with T. Also, the detection bias was set to a high value of $\delta = 0.1$.

Finally, combining (7.10) with (7.11) and replacing the mean photon numbers by the QKD parameters given by 7.2 gives the threshold value V_A^{covert} under which the communication is δ-covert :

$$V_A \leq \frac{8\delta\sqrt{\frac{\xi}{2}(1+\frac{\xi}{2})}}{\sqrt{n}} = V_A^{\text{covert}}. \tag{7.12}$$

It is interesting to understand how the constraint above impacts the performance of the QKD protocol. Since the number of QKD states plays a role in equation 7.12, instead of the secret key rate r given in 4.7, we use the total number of covert secret bits transmitted given by

$$n_{bits} = r \times n \tag{7.13}$$

as the metric of performance of the protocol.

In the following, we investigate the performance of the protocol by simulating the value of n_{bits} over a range of parameters. We begin by setting T and δ to optimistic values, such that our results will constitute an upper bound to what is achievable with realistic parameters. Since the secret key rate decreases with T, we set $T = 0.99$, a high value corresponding to a transmission distance of ~ 200 meters. For the covert parameter δ, we chose a high value of $\delta = 0.1$ in order to tolerate more photons on the quantum channel according to 7.12. This detection bias represents an advantage of 20% for Eve compared to a random guess when she is trying to detect the communication. Therefore this value is arguably high to claim covertness.

With these values of T and δ, we plot in figure 7.2 the value of n_{bits} by varying ξ and n. Above a certain value for ξ the key rate falls to zero because the excess noise is too high. Similarly, above a threshold value for n the key rate falls to zero because there are not enough photons per QKD symbol. Hence the results obtained in the numerical simulation of figure 7.2 constitute an upper bound to the performances of the covert QKD protocol over all realistic parameters.

[1]The quantum relative entropy, noted D here, is the quantum equivalent to the Kullback–Leibler divergence, which is a measure of the distance between two statistical distributions. The quantum relative entropy of state ρ relative to state σ is given by $D(\rho||\sigma) = \text{Tr}\big[\rho(\log\rho - \log\sigma)\big]$

We find a maximal value of $n_{bits} \approx 6.10^{-3}$. Therefore we conclude that the constraint 7.12 on V_A is too strong to achieve any kind of useful covert secret key distribution, and that covert CV-QKD is essentially impractical without some additional resource for Alice and Bob. This was to be expected since a well-known prerequisite for covert communications is the use of a shared secret between Alice and Bob, and we did not exploit this resource here. In the next section we discuss how the shared secret can be used to improve these performances.

7.3 A shared secret as a resource for covert CV-QKD

To the best of our knowledge, all existing studies on covert communications utilize some sort of secret shared between Alice and Bob. Based on the results displayed in figure 7.2 such a resource is mandatory for covert CV-QKD. It is therefore crucial to understand how one could use the shared secret to provide Alice and Bob with an advantage.

In reference [94] the authors spread the signal over a large transmission interval. This should always provide some way to increase the system performances since the communication state can be made arbitrarily close to the idle state by decreasing q, the probability to send a QKD state in each time-bin. What is particularly interesting in this approach is that the shared secret used to encode the communication time-bins has computational security, yet the QKD security can be fully guaranteed even if Eve perfectly knows the time-bins containing the quantum states. Hence their covert QKD protocol is a hybrid protocol from a security perspective, where the covertness is insured with computational security while the key is guaranteed secure regardless of the covertness.

Another interesting usage of a shared secret resource is as a codebook, as is described in the supplementary material of reference [90]. In this case k bits are encoded in 2^k codewords of length n symbols, where the set of codewords can be written as $\{|\alpha_1, ..., \alpha_n\rangle_j\}_{j=1}^{2^k}$. The codebook is constructed by generating the codewords such that each α_i is generated along the complex Gaussian distribution as in the GG02 QKD protocol. From Eve's perspective the codewords are equivalent to a tensor product thermal state over the n modes since she does not have access to the codebook. However it is not clear if in this case we can perform covert CV-QKD in the hybrid security model where the codebook has computational security. For this we must guarantee that revealing the codebook will not lead to security loopholes in the QKD protocol, and further investigation over this question is necessary. However we leave this for future work.

For covert CV-QKD applications, we require a shared secret usage that is compatible with CV-QKD implementation and does not hinder the security of the underlying key distribution protocol. We propose a way to do this in the next section.

7.3.1 Block-coherent encoding

Our proposal stems from the observation that the limiting factor in the the covert setting is the SNR. Therefore, one way to enable covert QKD would be to increase the SNR while maintaining the covert condition of 7.12. Notice that the square-root law imposes that the number of photons per mode, over m modes, scales as $1/\sqrt{m}$. However when we coherently combine photons scattered over m modes into a unique mode, the power in the resulting mode is m times the average power in each mode. This suggests that a coherent gain of $\sqrt{m}$ on the signal power received by Bob can be obtained by combining the power of m modes at Bob's while maintaining covert communications. We precise this idea below.

Let Alice sends her QKD states over $n \times m$ modes with mean number of signal photons per mode of $\bar{n}_A/m$. We denote $\hat{\rho}_s$ the average state in each mode in this case which is the thermal state with mean photon number $\bar{n}_0 + \bar{n}_A/M$. Now suppose Bob has a unitary $\mathcal{U}$ acting on $\hat{\rho}_s^{\otimes nm}$ such that

$$\mathcal{U}(\hat{\rho}_s^{\otimes nm}) = \hat{\rho}_1^{\otimes n} \otimes \hat{\rho}_0^{\otimes n(m-1)}, \tag{7.14}$$

where $\hat{\rho}_0$ and $\hat{\rho}_1$ are the idle and communication states defined in 7.3 and 7.4. Then Bob can use $\mathcal{U}$ to transform the state $\hat{\rho}_s$ received and perform his QKD measurement on the first n modes $\hat{\rho}_1^{\otimes n}$ with an average of $\bar{n}_A$ signal photons per mode. In this case the covert analysis must be conducted with the state transiting on the quantum channel $\hat{\rho}_s^{\otimes nm}$, hence we find the covert condition by substituting V_A/m to V_A and nm to n in equation 7.12 which gives

$$\frac{V_A}{m} \leq \frac{8\epsilon\sqrt{\frac{\xi}{2}(1+\frac{\xi}{2})}}{\sqrt{nm}} = \frac{V_A^{\text{covert}}}{\sqrt{m}}. \tag{7.15}$$

Thus, assuming Alice uses the highest modulation variance possible, when Bob performs his QKD measurement on $\hat{\rho}_1^{\otimes n}$ he measures QKD states with modulation variance

$$V_A = \sqrt{m} V_A^{\text{covert}}. \tag{7.16}$$

This permits a $\sqrt{m}$ increase in the power of the state measured by Bob compared to the case where the states are directly sent and measured. We refer to the method used by Alice to encode her QKD states in a way such that $\mathcal{U}$ exists as *block-coherent encoding* of length m. Let us examine in the next subsection how we could implement block-coherent encoding in a CV-QKD setting and investigate the impact on the distilled key.

7.3.2 Implementation for covert CV-QKD

One way to generate $\hat{\rho}_s^{\otimes nm}$ and to perform the transformation $\mathcal{U}$ is to borrow techniques from spread spectrum communications [97]. These have been developed decades ago for purposes similar to covert communications. The objective is to spread the signal over a larger bandwidth such that it is harder to intercept and to jam by malevolent parties. In this case the legitimate receiver reverts the spreading before measuring the intended signal.

In particular for this work we focus on direct-sequence spread spectrum. In this case the spreading is achieved by digitally multiplying the data by a so-called *spreading sequence* in the time domain before generating the signal. The spreading sequence is constituted of binary $\{-1, 1\}$ symbols, called chips, inducing phase shifts encoded at rate f_{chips} much larger than the symbol rate f. The effect of this is to increase the signal bandwidth by a spreading ratio defined by the quantity

$$T = \frac{f_{\text{chips}}}{f}, \tag{7.17}$$

See figure 7.3 for a representation of the multiplication of the data by the spreading sequence and the effect on the signal bandwidth. The number of modes transmitted during a communication protocol is defined by the time-bandwidth product

$$n = \tau \times B, \tag{7.18}$$

where τ is the communication duration and B is the signal bandwidth. Therefore, controlling the spreading ratio such that $R = m$ will increase the signal bandwidth by a factor m while maintaining the same communication duration, which amounts to transmitting the signal over nm modes. To revert the spreading and reshape the original signal, Bob applies the spreading sequence once more which cancels the phase shifts induced by the modulation of the spreading sequence.

Let us describe the general lines of the covert CV-QKD protocol using this technique to perform block coherent encoding.

1. Alice generates the complex random variables $\{\alpha_i\}_{i=1}^n$ where the real and imaginary parts of each α_i follows a Gaussian distribution with variance $V_A \lesssim \sqrt{m} V_A^{\text{covert}}$
2. Alice uses a spreading sequence $S \in \{-1, 1\}^{nm}$ to generate the sequence of quantum states $Q = \otimes_{i=1}^n \otimes_{j=1}^m |S_{m\times(i-1)+j}\alpha_i\rangle$ sent over the quantum channel at rate $f \times m$.

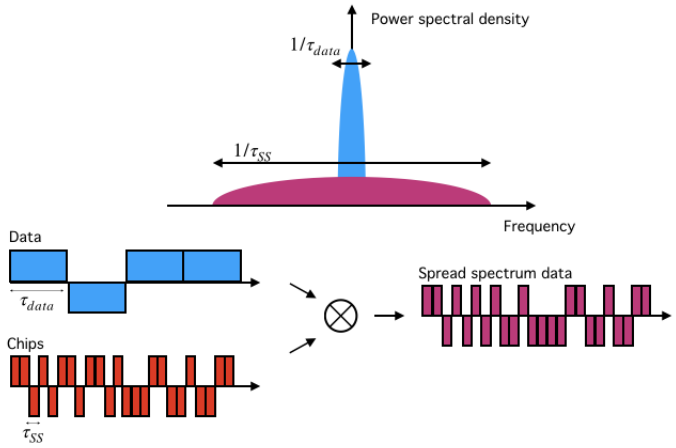


Figure 7.3: Direct Sequence Spread-spectrum consists in multiplying the data by a faster spreading sequence. The spread-spectrum signal's bandwidth is increased by the ratio of the spreading sequence rate and the data rate. The inverse spreading operation consists in the multiplying the spread-spectrum data by the spreading sequence again.

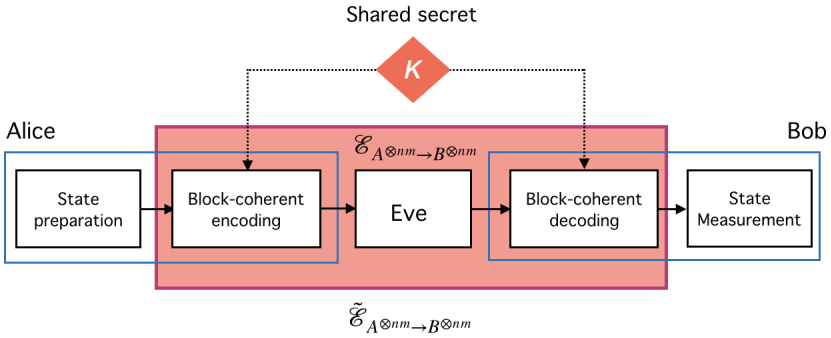


Figure 7.4: Depiction of the QKD protocol using block coherent encoding. The security of the distilled key is guaranteed since the keyrate analysis is made on the equivalent channel $\tilde{\mathcal{E}}_{A^{\otimes n}\to B^{\otimes n}}$, which contains the block coherent encoding process.

3. With the noise photons present on the channel, the average state transiting from Alice to Bob is $\hat{\rho}_s^{\otimes nm}$. Since the modulation variance of the QKD states obeys equation 7.15 the communication is covert.

4. Upon reception, Bob reverts the phase shifts induced by the spreading sequence and generates the sequence of states $\{\otimes_{i=1}^{n} \otimes_{j=1}^{m} |\alpha_i\rangle\}$ received at symbol rate $f \times m$ which amounts to the sequence of states $Q' = \otimes_{i=1}^{n} |\alpha_i\rangle$ at rate f. He then performs his measurement of the QKD states $\{|\alpha_i\rangle\}$

5. Alice & Bob distill their secret covert key via classical post-processing.

Importantly, without knowledge of the spreading sequence it is not possible to revert the spreading. Hence S should be kept secret from Eve, and is the shared secret resource we will assume Alice and Bob share before the covert QKD protocol.

Before moving on, let us briefly show that the block-coherent encoding we propose can be used without impacting QKD security. This is true because the QKD parameter estimation analysis compares

the QKD states before block-coherent encoding at Alice with the measured states after block-coherent decoding at Bob's. Hence the spreading and de-spreading process are considered to be part of the channel, *i.e* under the control of Eve. This is illustrated in the figure 7.4 where the channel from Alice to Bob, noted $\mathcal{E}_{A^{\otimes nm}\to B^{\otimes nm}}$ is completely controlled by Eve. However, the QKD analysis considers a larger channel $\tilde{\mathcal{E}}_{A^{\otimes nm}\to B^{\otimes nm}}$ containing the block-coherent encoding and decoding.

7.3.3 Enabling covert CV-QKD

Now that we have derived a way to give some advantage to Alice and Bob through block-coherent encoding, let us investigate the performances of covert CV-QKD with this new method. To do this, we use a similar approach to the one used in 7.2.2. However let us begin by giving an upper bound to the spreading ratio that can be experimentally achieved, which amounts to providing an upper bound for m when using block-coherent encoding.

The number of modes over which the n QKD states can be spread depends on the speed of the electronics in the arbitrary waveform generators (AWGs) used by Alice and Bob, which will ultimately limit the chip rate f_{chips} and therefore the spreading ratio R based on equation 7.17. Here we will assume a maximal chip rate of 50 GBaud, which is a conservative value considering the achievable rates by modern AWGs. Then the maximal spreading ratio is entirely defined by the symbol rate, which is typically of the order of $\sim$ 100 MBaud for CV-QKD protocols. However we will consider lower symbol rates of $f = 1$ MBaud here to allow for larger block-coherent encoding lengths up to $m_{\max} = 50\ 000$.

We examine in figure 7.5 the increase in the number of covert secret bits that can be distilled by using block-coherent encoding. Our approach is similar to our previous analysis of figure 7.2 without the block-coherent encoding. This time we chose to investigate the performances over a distance of 10 km ($T = 0.631$) and used the same detection bias $\delta = 0.1$. Then we varied the values of n and ξ_A and plotted in each case the value n_{bits}.

Our results show that, thanks to block-coherent encoding, the maximal amount of covert and secret bits which can be distilled over 10 km is non negligible and could be potentially useful. When $m = 4 \times 10^4$ we find a maximal value $n_{\text{bits}} = 142$ bits. The optimisation over ξ_A shows that the optimal channel noise over a 10 km link is approximately of $\xi_A = 0.01$ SNU, which would yield an excess noise measurement of $\xi_B = 0.0063$ SNU at the channel output. This value is certainly a low value from an experimental point of view but by no means unachievable, see for instance reference [98]. Therefore the set of parameters enabling covert CV-QKD with block-coherent encoding are realistic parameters for a CV-QKD experiment. Note here that we implicitly assumed that the channel noise dominated QKD system noise sources.

Interestingly, we also observe a linear relation between n_{bits} and m : doubling the block-coherent encoding length also doubles n_{bits}. By curiosity we also investigated how the detection bias was related to n_{bits} and found that the relation was quadratic. We plot these results in the figure 7.6. A reason for the linear and quadratic relations of m and δ with n_{bits} can be found from the respective roles of m and δ in the expression 7.15.

7.4 Towards practical covert QKD schemes

Our previous results show that covert CV-QKD is possible thanks to block-coherent encoding, but a frustration remains because of the limited amount of secret bits that can be distilled covertly. Indeed as long as the square-root law pilots the power of the quantum states transiting on the channel, there is necessarily a finite amount of covert and secret bits that can be exchanged because the keyrate becomes zero above a certain threshold for n. Although some applications can be satisfied with this, it is interesting to investigate how we can relax this constraint through additional assumptions.

In the following we develop two models which achieve this. In the first we give Alice some control over the noise. Then she can reduce the noise power when she sends her QKD states to avoid

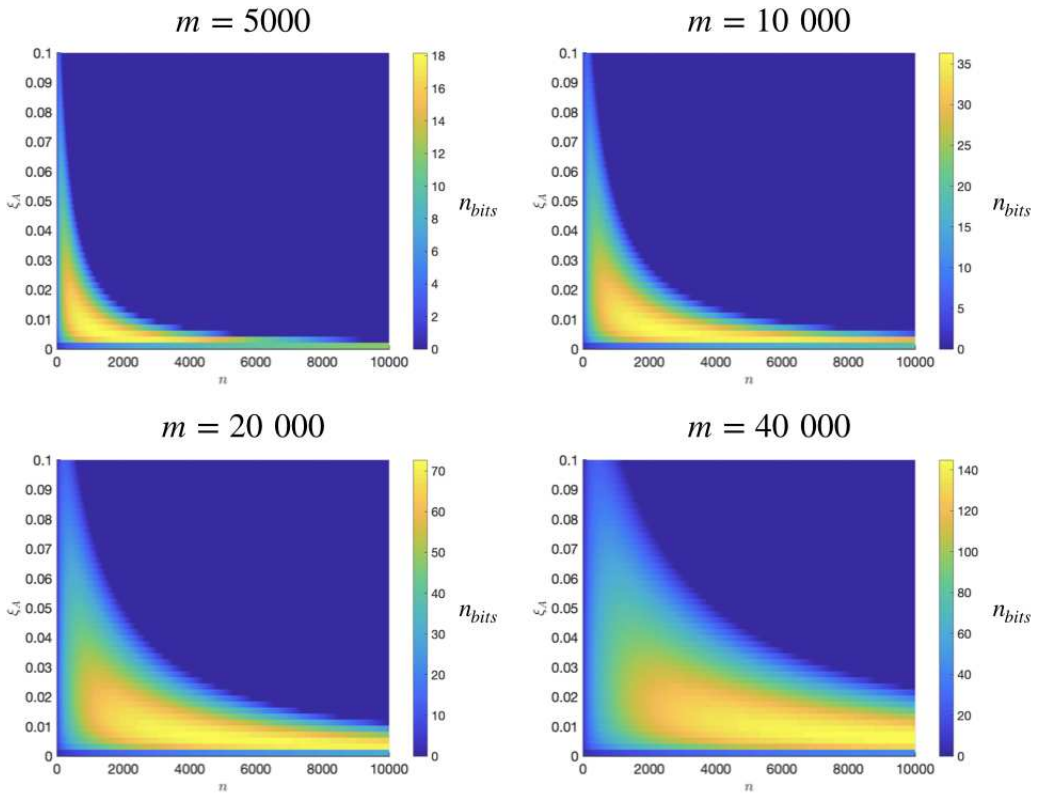


Figure 7.5: We plot n_{bits} over a range of values for ξ_A and n for 4 different values of block-coherent encoding length m. Other parameters were taken as $T = 0.631$, which corresponds to the losses of a 10 km fiber link with loss 0.2 dB/km, and $\delta = 0.1$.

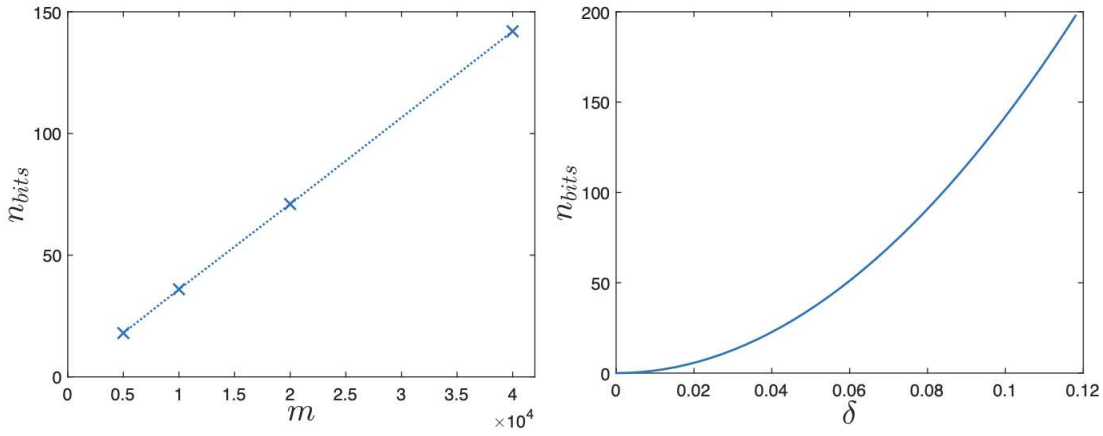


Figure 7.6: Scaling of the maximal value of n_{bits} with respect to m (left) and δ (right). In the left plot δ was set to 0.1 and in the right plot m was set to 4×10^4.

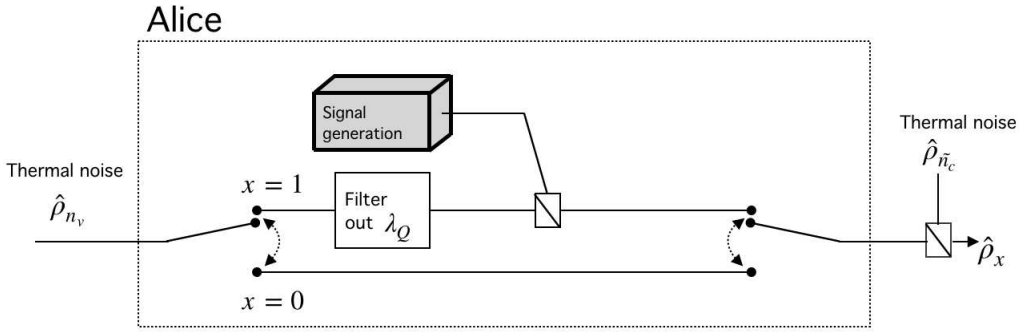


Figure 7.7: Alternate covert QKD model in which Alice can choose whether to transmit the full noise state $\hat{\rho}_{n_v}$ (case $x = 0$) or to filter out the noise around the quantum channel wavelength λ_Q and substitute her QKD signal instead (case $x = 1$). In any case an additional constant noise source $\hat{\rho}_{\bar{n}_c}$ is injected in the channel after Alice's lab. The resulting state is denoted $\hat{\rho}_x$ and is $\hat{\rho}_0$ when $x = 0$ and $\hat{\rho}_1$ when $x = 1$.

detection. The second model inspired from [99] supposes there is some source of fluctuating noise on the channel, generating an uncertainty on the total noise power for Eve and making her discrimination more difficult.

7.4.1 Model 1 : Alice controls some of the noise

Let us assume Alice has some control over the channel noise. This is represented by writing the noise photons $\bar{n}_0$ as a sum of a variable $\bar{n}_v$ and a constant $\bar{n}_c$ amount of noise photons such that

$$\bar{n}_0 = \bar{n}_c + \gamma \bar{n}_v, \tag{7.19}$$

where $\gamma \in [0, 1]$ is controlled by Alice. Assume Alice sets $\gamma = \gamma_0$ when she is idle and $\gamma = \gamma_1$ during the communication phase. Then we can write the idle and communication states as

$$\hat{\rho}_0 = \sum_{i=1}^{\infty} \frac{(\bar{n}_c + \gamma_0 \bar{n}_v)^i}{(1 + \bar{n}_c + \bar{n}_v)^{i+1}} |i><i| \tag{7.20}$$

$$\hat{\rho}_1 = \sum_{i=1}^{\infty} \frac{(\bar{n}_c + \gamma_1 \bar{n}_v + \bar{n}_A)^i}{(1 + \bar{n}_c + \bar{n}_A)^{i+1}} |i><i| \tag{7.21}$$

Both states are equal for $\bar{n}_A = (\gamma_0 - \gamma_1)\bar{n}_v$. Logically the best strategy for Alice is to set $\gamma_0 = 1$ and $\gamma_1 = 0$, which amounts to substituting her signal photons to the variable amount of noise photons.

In this case Eve cannot discriminate between $\hat{\rho}_0^{\otimes n}$ and $\hat{\rho}_1^{\otimes n}$, thus for her the best strategy is limited to a random guess regardless of the number of QKD states transmitted on the channel. In this model the square-root law is circumvented and an asymptotic number of QKD states can be transmitted. Hence as long as the keyrate is positive, which can be determined by the values of $\bar{n}_v$, $\bar{n}_c$ and T, then an arbitrary number of covert and secret bits can be distilled.

The question of whether this scenario is realistic in practice is legitimate. For this reason let us imagine a setting where it could be verified. Consider the case where Alice's laboratory located inside a WDM backbone link. Classical channels generate Raman noise before and after Alice's lab who can act on the noise generated before her lab using spectral filters. A schematic representation of this setting is given in the figure 7.7.

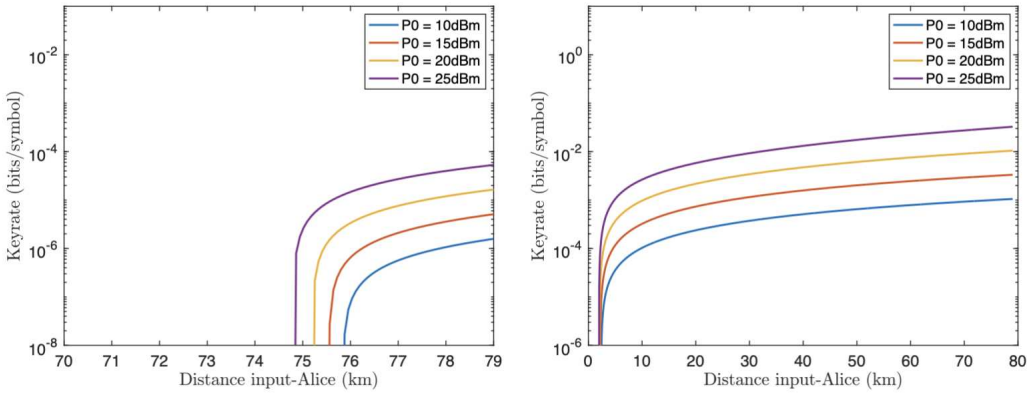


Figure 7.8: We plot the covert secret key rates in our model where Alice can control part of the noise. We simulated some realistic values of variable and constant excess noise based on a quantum/classical WDM setting described in reference [80]. (left) Without block-coherent encoding. (right) With block-coherent encoding of length $m = 500$. The distance between Alice and Bob is given by $L_{\mathrm{AB}} = 80 - L_{\mathrm{IA}}$. The keyrate is given in bits/symbol

In the rest of this subsection we will attempt to roughly simulate the covert secret key rate in the setting described above. Given a fixed wavelengths for the quantum and classical channels, the Raman noise is entirely defined by three parameters :

1. The total input power of the classical channels P_0
2. The distance between the channel Input and Alice L_{IA}
3. The distance between Alice and Bob L_{AB}

And the relation between these parameters and the Raman noise, defined at the WDM link input, is given by [80] :

$$\xi_{\mathrm{Ram,input}} = \zeta P_0 (L_{\mathrm{AB}} + L_{\mathrm{IA}}), \tag{7.22}$$

where ζ is a parameter which depends on the wavelengths of the classical channels and of the quantum channel. Note here we have neglected the contribution of the stimulated Raman scattering since it is expected to be orders of magnitude below the spontaneous Raman scattering [80]. From $\xi_{\mathrm{Ram,input}}$ we can express the Raman noise at Alice's lab by multiplying this value by the attenuation on the input-Alice link which is given by $\exp(-\alpha L)$ where α is the attenuation coefficient equal to 0.2 dB/km. Hence we have

$$\begin{aligned} \xi_{\mathrm{Ram,Alice}} &= \zeta P_0 L_{\mathrm{IA}} \exp(-\alpha L_{\mathrm{IA}}) + \zeta P_0 \exp(-\alpha L_{\mathrm{IA}}) L_{\mathrm{AB}}, \\ &= \xi_{\mathrm{Ram}}^{\mathrm{IA}} + \xi_{\mathrm{Ram}}^{\mathrm{AB}}, \end{aligned} \tag{7.23}$$

which is the sum of the Raman noise generated on the input-Alice and Alice-Bob links.

In our model where Alice can control part of the noise, $\xi_{\mathrm{Ram}}^{\mathrm{IA}}$ plays the role of the variable noise term while $\xi_{\mathrm{Ram}}^{\mathrm{AB}}$ is the constant noise term. The only parameter missing to simulate these for different values of P_0, L_{IA} and L_{AB} is the parameter ζ. Since ζ depends on the "layout" of the quantum/classical WDM channels, we infer this value from an experimental implementation of QKD in a WDM setting. Here we use reference [80], where the quantum channel is located in the $S-$band and the classical

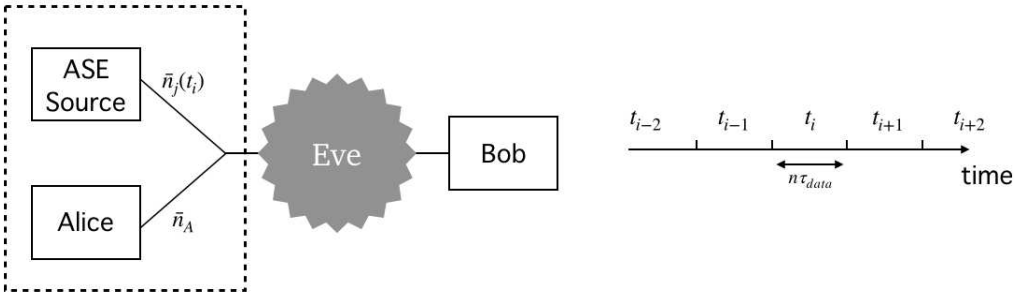


Figure 7.9: In this model the noise is generated by a time-dependant ASE noise source outside of Eve's control. The noise has constant power over time interval t_i but varies between intervals. The new mean noise photon number is drawn according to a uniform distribution over $[\bar{n}_j^{min}, \bar{n}_j^{min}]$.

channels are located towards the longer wavelengths of the $C-$band corresponding to the "Red WDM" setting of the paper.

We can now run our covert secret key rate simulation in this setting. For this we will consider the WDM link is of length $L_{\mathrm{AB}} + L_{\mathrm{IA}} = 80$ km and we plot our results for different values of P_0 in the figure 7.8. We compared the two cases with and without using block-coherent encoding with a conservative value of $m = 500$. Without surprise block-coherent encoding greatly improves the performances. Note that since the square-root law does not apply in this case, the signal power at Bob's scales with m instead of $\sqrt{m}$.

Our results indicate that a covert secret key can be distributed over large distances, up to ~ 70 km, by allowing Alice to control the noise generated before her lab and combining this with block-coherent encoding. Contrarily to usual quantum and classical coexistence in WDM links, here it is advantageous to use a higher launch power for the classical channels. The reason behind this is that higher Raman noise generated before Alice allows for higher modulation variances V_A while not contributing to the excess noise measured at Bob. Hence we have presented a joint quantum and classical architecture which profits from the coexistence to provide covertness, an interesting and original security primitive.

7.4.2 Model 2 : fluctuating total noise power inducing uncertainty at Eve's

We investigate here a second model to circumvent the square-root law. Here we use previous works in wireless covert communications [99, 100] as inspiration to derive our model. In these works, the authors have considered the case where a jammer randomly modifies the noise distribution and have shown that we are not limited by the square-root law in this case.

We derive a similar model for fiber-based communications and consider using random amplified spontaneous emission (ASE) noise source as the jammer. ASE noise is for example generated by amplifiers in fiber-based optical communications. The model is as follows.

Consider several time intervals t_i of length $n\tau_{data}$ corresponding to the duration of the communication required for Alice to send n quantum states to Bob. The ASE noise source, or jammer, generates noise with mean photon number $\bar{n}_j(t_i)$ that depends on the current t_i and drawn at random from $[\bar{n}_j^{min}, \bar{n}_j^{max}]$ according to the uniform distribution. See figure 7.9 for a representation. The covert QKD protocol always begins when a new time interval begins. During t_i, the number of noise photons on the channel is $\bar{n}_A + \bar{n}_j(t_i)$ if Alice sends QKD states and is $\bar{n}_j(t_i)$ if she does nothing. The idle and communication states over t_i are written as n copies of the same thermal state $\hat{\rho}(k)$ with mean photon number k and drawn from a uniform density probability distribution. Hence we have

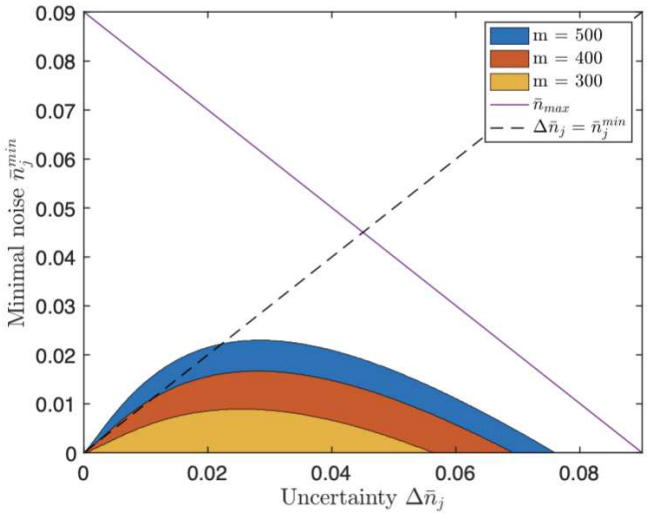


Figure 7.10: Set of parameters $(\Delta\bar{n}_j, \bar{n}_j^{min})$ for which the keyrate is positive (colored area) at a distance of 10km with fiber loss coefficient of 0.2 dB/km. Block coherent encoding of minimal length ≈ 200 is necessary to obtain a positive key rate. Increasing the block coherent encoding length expands the set of positive keyrate parameters. The dashed green line represents $\Delta\bar{n}_j = \bar{n}_j^{min}$ and the solid purple line is the maximal number of noise photons that can tolerated for the GG02 protocol.

$$\hat{\rho}_0 = \frac{1}{\Delta\bar{n}_j}\int_{\bar{n}_j^{min}}^{\bar{n}_j^{max}} \hat{\rho}(k)^{\otimes n} dk,$$
$$\hat{\rho}_1 = \frac{1}{\Delta\bar{n}_j}\int_{\bar{n}_j^{min}+\bar{n}_A}^{\bar{n}_j^{max}+\bar{n}_A} \hat{\rho}(k)^{\otimes n} dk,$$

where $\Delta\bar{n}_j = \bar{n}_j^{max} - \bar{n}_j^{min}$. Separating both states into overlapping and non-overlapping mean photon numbers gives:

$$\hat{\rho}_0 = \frac{\bar{n}_A}{\Delta\bar{n}_j}\hat{\rho}_{[\bar{n}_j^{min};\bar{n}_j^{min}+\bar{n}_A]} + \frac{\Delta\bar{n}_j - \bar{n}_A}{\Delta\bar{n}_j}\hat{\rho}_{[\bar{n}_j^{min}+\bar{n}_A;\bar{n}_j^{max}]}$$
$$\hat{\rho}_1 = \frac{\Delta\bar{n}_j - \bar{n}_A}{\Delta\bar{n}_j}\hat{\rho}_{[\bar{n}_j^{min}+\bar{n}_A;\bar{n}_j^{max}]} + \frac{\bar{n}_A}{\Delta\bar{n}_j}\hat{\rho}_{[\bar{n}_j^{max};\bar{n}_j^{max}+\bar{n}_A]}$$

With $\hat{\rho}_{[\bar{n}_1;\bar{n}_2]} = \frac{1}{\bar{n}_2-\bar{n}_1}\int_{\bar{n}_1}^{\bar{n}_2}\hat{\rho}(k)^{\otimes n}dk$.

The discrimination process between both states, similarly to equation 7.8, requires Eve to build optimal POVMs $(\hat{\Lambda}_0, \hat{\Lambda}_1)$ acting on the mixed states $\hat{\rho}_0$ and $\hat{\rho}_1$. Then Eve's error probability becomes :

$$\mathbb{P}_e = \frac{1}{2} - \frac{\bar{n}_A}{2\Delta\bar{n}_j}\mathrm{Tr}\big[\hat{\Lambda}_0(\hat{\rho}_{[\bar{n}_j^{min};\bar{n}_j^{min}+\bar{n}_A]} - \hat{\rho}_{[\bar{n}_j^{max}+\bar{n}_A;]})\big] \tag{7.24}$$

Coarsely bounding the trace by 1 gives a lower-bound on $\mathbb{P}_e$:

$$\mathbb{P}_e \geq \frac{1}{2} - \frac{\bar{n}_A}{2\Delta\bar{n}_j} \tag{7.25}$$

Thus when $\bar{n}_A = 2\delta\Delta\bar{n}_j$ the protocol is covert with detection bias δ. Notice the condition on $\bar{n}_A$ does not scale in $1/\sqrt{n}$, and it stems from the fact Eve can discriminate between communication and no-communication events only if the resulting states cannot be generated from the conjugate event. When $n \to \infty$ an arbitrary number of QKD states can be sent. Therefore as long as the keyrate is positive any desired amount of covert and secret bits can be transmitted. We plot in figure 7.10 the set of parameters $(\Delta\bar{n}_j, \bar{n}_j^{min})$ allowing for positive covert key rates over metropolitan distances up to 10km with different block-coherent encoding lengths. Our results show that for reasonable block-coherent encoding length it is possible to achieve positive covert key rates generally in the regime where there is more uncertainty on the noise level than fixed noise levels. By increasing the block-coherent encoding length and the detection bias we can extend to the regime where there is a larger part of fixed noise.

7.5 Discussion

We presented in this chapter our research on covert QKD, where our motivation is to harness the coexistence between quantum and classical channels in order to turn a detrimental effect –such as the Raman noise– into a new security primitive : covertness.

An interrogation we have not yet answered is whether QKD is really necessary when we have the ability to reliably send covert signals. Indeed, what about sending a secret key directly via the covert communication channel ? Wouldn't this circumvent the need for the whole post-processing phase of the QKD protocol ? In fact for DV-QKD, previous work has shown that ϵ-covertness implied 2ϵ-security in the QKD protocol [101].

We need to keep in mind however that the covert protocol consumes a secret key and more than it can generate, hence it relies on computational methods to share the key before the covert protocol begins. Ultimately the covertness holds as long as the shared secret is safe, hence with computational security. In this picture, covert communications can never replace QKD protocols for ITS key distribution, and covertness can not be a substitute to QKD but only an addition to the protocol.

Another way to consider covert-QKD is to look at QKD as a protocol where Alice sends an unbreakable safe containing a secret key to Bob. Providing covertness to the QKD protocol amounts to making the safe invisible, in addition of being unbreakable. However, the invisibility only holds if Eve has some limited amount of computing resources *i.e.* with computational security.

Circling back to our work, here we have investigated how to use a shared secret –in the form of a spreading sequence used in spread spectrum communications– to enable covert CV-QKD. We showed that a limited number of covert secret bits can be obtained even with a very large spreading ratio because of the square-root law. Our approach was then to study under which conditions covert QKD would be possible with an asymptotic number of covert secret bits shared between Alice and Bob.

We showed that in two practical models the requirements for covert signaling do not follow the square-root law and therefore enable any amount of covert secret bits to be transmitted as long as the assumptions made in the model hold. In the first model we suppose Alice can control some noise, thus she can substitute her GG02 QKD states to some on the noise. In the second model we allow a time-dependant noise source on the channel which generates an uncertainty on the total noise power at Eve's. We showed that in both cases covert signalling can be achieved with an unlimited number of signal states, therefore paving the way towards practical covert QKD.

More generally this work shows that careful design of joint quantum and classical systems can be beneficial for the QKD channel by providing covertness to the quantum communication, which is a desirable security primitive for ultra-secure applications.

Perspectives

The quantum computing revolution.

A promising research field today concerns the development of the quantum computer, with the objective of harnessing the unique physical properties of quantum systems to perform certain calculations which would be intractable for classical computers. This has the potential to lead to major breakthroughs in many other scientific domains where the tractability of classical simulations is a limiting factor. Such fields are for example weather forecasting [102], molecular simulation [103], artificial intelligence [104], particle physics [105] and more.

Another foreseen consequence of quantum computing is also the tractability of currently intractable mathematical problems such as the factoring problem and the discrete logarithm. These constitute the cornerstones on which are built public-key cryptographic primitives, vital to the modern cryptographic infrastructure since they are used to distribute the symmetric keys necessary to encrypt data. Therefore new solutions need to be found to solve the key distribution problem, and fast (see our discussion in subsection 3.3.1).

Quantum key distribution : a quantum-safe key distribution protocol.

In their seminal paper [1] published in 1984, Charles Bennett and Gilles Brassard proposed a new method to perform key distribution based on the laws of quantum mechanics : QKD. Contrarily to current cryptographic primitives QKD provides ITS security on the distributed key, hence QKD is a future-proof key distribution protocol since no future developments in technology or algorithms can help an attacker obtain the secret key, not even a quantum computer.

The strong security guarantees of QKD –and perhaps the beautiful theoretical foundations providing them– have spurred increasing interest of the quantum information community for this technology. However to this day, several important challenges remain in the field.

Theoretical vs practical security. The strong security guarantees QKD provides on the final key are only valid in the model used to derive the security proof, which is often an idealized representation of the real experiment. Unfortunately, there can exist some side-channel attacks which exploit some factors which are not considered in the security proofs. We discussed in subsection 5.5.1 one such attack exploiting the TLO design for CV-QKD, but many more examples exist [106].

Note however that security proofs have been consistently refining their model to account for device imperfections. For example the security proof we used for the PCS-64QAM format [48] showed that discrete modulation formats could yield positive key rates. This closes a loophole where many CV-QKD experiments considered Alice employed a Gaussian modulation while in reality we can only approximate a Gaussian distribution in practice due to the finite resolution of the digital-to-analog converters. More recently, new security proofs have also accounted for the fact that the detection process can also only yield a finite number of discrete values [107]. In time and as the technology develops, more device imperfections will find a way into the formalism of the security proofs.

Reach. QKD protocols suffer from fundamental limitations in terms of point-to-point achievable

distance. We plotted in subsection 5.5.3 the reach and keyrate of different CV-QKD implementations, where we observe that the longest reach of a CV-QKD experiment in the LLO regime, to the best of our knowledge, is of 50 km. Recently a new study has managed a positive key rate at 60 km [108] with machine learning aided carrier recovery. The record for DV-QKD, which is better suited than its CV counterpart for long distances, is currently of 421 km [60]. While this constitutes a considerable technological feat, it is also not sufficient to enable a global QKD without using trusted relays. Note that a true breakthrough in this area would be the successful demonstration of a quantum repeater. These (at the moment) theoretical devices act as nodes on a network and are connected via entanglement swapping [109] which achieves the required long-range entanglement enabling QKD.

Cost. The fact that QKD operates on the physical layer implies that the deployment costs of the technology is also considerably higher than for classical cryptographic primitives operating at the software level. Making QKD a more affordable technology is a central concern for the development of the field.

One approach to solving this problem is to pursue the coexistence of quantum and classical signals. Since most of the costs of fiber-based communications lie in the optical fiber network itself, integrating QKD on the current optical fiber infrastructure would drastically cut expenses. For this particular problem CV-QKD is arguably better suited, and this is a strong argument of the community to push their technology forwards compared to other QKD solutions. Here the holy grail would be to demonstrate QKD over a dense WDM backbone link [16], where the typical length of the link is about 80 km and the classical channels have nominal input power around 0 dBm each. For the moment coexistence of QKD with classical channels has only been achieved over short distances and for sub-nominal classical channel power [71, 80].

Work achieved during the course of the thesis.

This thesis was conducted in the context of the European project CiViQ, which aimed at developing CV-QKD technology and pursuing its integration on emerging optical telecommunication networks in order to develop cost-effective QKD systems. To this end it regrouped 21 partners involving major telecoms, integrators and developers of QKD. In the scope of this project, our contributions were directed towards CV-QKD system design and development, and our approach was to consider how classical and quantum communication links can be designed jointly in order to enable secret key distribution and classical communications over the same fiber. Our work can be divided into one main project where we demonstrated joint classical and quantum communications over the same fiber, leveraging the classical DSP to correct phase and frequency impairements on the quantum channel, and a side project where we investigated how to harness channel noise to provide covertness to the QKD states.

Experimental implementation of a joint quantum and classical communication system. The large part of our efforts were directed towards the experimental realisation of our joint quantum and classical communication system described in chapter 6. This proved to be quite the adventure since it was the first time that quantum communications were performed on the modern high-rate optical communication platform of Telecom Paris (GTO). We started from an existing single polarisation classical coherent communication system and added the components we needed to perform QKD on the other polarisation. The first step was carefully choosing the low-noise detectors for the quantum channel, and characterising their behavior and performance. From there, the roadmap towards implementing the target system was clear on paper : deploy a second AWG on the Y-polarisation to generate the quantum data, achieve the desired attenuation on the quantum channel, and use the phase and frequency estimators of the classical data to perform the quantum channel DSP. I naively thought this would be solved rather quickly, which highlights how little I knew about experimental work. In reality, every step forward required long series of troubleshooting, but these became easier over time as my understanding of the manifestation of different experimental problems developed.

Unfortunately a couple events out of our control delayed our work. First, in November 2019, the school moved from Paris to Palaiseau in order to join a large campus of schools which will, in time, enable exciting collaborations between different areas of expertise. However this also meant we had to pack our experimental devices and setup in the new location, and this caused a halt in our experimental work for a couple months. The second event was the global pandemic of coronavirus which froze the nation for another couple months.

Nonetheless we managed to reach our goal of enabling joint classical and quantum communications, over the same fiber, using the classical channel phase and frequency estimator to correct the quantum data. Our experimental work led to the following contributions :

- **Poster at OFC2022 :** *Symbiotic joint operation of quantum and classical coherent communications.* In this contribution we demonstrate our joint quantum and classical communication system using the QPSK modulation on the quantum channel, and achieve a positive key rate in the asymptotic regime at 15 km. Our paper submission to OFC was then published by IEEE.

- **Conference presentation at SPIE Europe 2022 :** *Quantum key distribution and classical communication coherent deployment with shared hardware and joint digital signal processing.* Here we used the novel security proof [48] giving an explicit key rate formula for discrete modulations and applied it to a PCS-64QAM format on the quantum channel. The higher order modulation format yielded much better key rates and our results were compatible secret key distribution and reliable classical communications over 40 km in the asymptotic regime, and 10 km using a finite-size analysis.

- **European patent demand :** *Joint classical and quantum optical communications.* Patent number EP22305158.2 filed on February 11^{th} 2022.

The experiment now works consistently in a regime of low SNR, compatible with positive key rates. It will be the basis for future investigations of CV-QKD systems undertaken by the next generation of PhD students, notably to refine our understanding of noise processes and better control them, but also to test and demonstrate more complex quantum cryptographic protocols than QKD, including covert quantum communications.

Covert CV-QKD. Our second project, presented in chapter 7, was initially undertaken during the time where the experiment was inaccessible. In this work we showed that we could design hybrid quantum and classical systems in which the channel noise –due for example to classical channels– detrimental to the key rate could also be harnessed to provide an exiting new security primitive called *covertness*. Unfortunately because of the "square-root law" covert QKD is essentially limited in practice. For this reason we explore additional assumptions –which can be verified in some practical settings– under which covert QKD is *practical* in the sense that an arbitrary number of covert and secret bits can be transmitted. This project led to the following contributions :

- **Poster at QCrypt 2020 :** *Covert continuous-variable quantum key distribution.* We presented in this poster our initial results regarding covert CV-QKD.

- **Future paper submission :** *Covert CV-QKD.* We plan to submit the work on covert CV-QKD presented in this thesis to a journal in the near future.

Other work. In addition to my research duties, I had the opportunity to teach classes in cryptography and supervise student lab work on coherent detection. This experience was very enriching as it helped me develop as a person and as a researcher.

What future for QKD ?

There is currently a strong and continuous support on the institutional side for the development of QKD, and therefore research in the field of QKD is bound to continue to thrive in the foreseeable future. In addition, many QKD companies and startups exist today which contributes to the development of commercial QKD and brings the technology at the application frontier. The work already achieved in the field has led to major breakthroughs in our understanding of QKD and more generally in the related fields of quantum information, quantum communications and quantum computation. Future work will undoubtedly continue to strengthen our understanding over these questions.

Yet, a the moment, many national cybersecurity agencies reject QKD as a key distribution method [110, 111, 112, 113] because of the challenges we discussed above. From a classical cryptography perspective, post-quantum cryptography primitives are quantum-safe and do not suffer from the implementation difficulties of QKD. In addition the certification of classical primitives is well understood hence it is easier to deploy these solutions according to existing classical security models. By comparison, the theoretical versus real security of QKD constitutes a grey zone for classical cryptographers since the potential side-channel attacks do not resemble to the well known ones targeting classical primitives.

It is nonetheless undeniable that QKD can offer an advantage over classical methods. Moving forward, collaborations between teams versed in classical cryptography and in QKD can lead to the identification on specific cases where QKD –in its current state of cost and performance tradeoff– is desirable compared to other quantum-safe primitives. Such collaborations have already begun, as for example can be seen in reference [114] where QKD is used to provide long term security in stored data in the cloud. Our experimental work could find an application in this aspect, for example if QKD is deployed on inter-datacenter backbone links.

Another exciting direction to explore is to study how we can reasonably limit Eve's capabilities to propose a future-proof key distribution protocol with better performances than QKD and more practical. The interested reader is referred to the work of [115] where the Quantum Computational Timelock (QCT) model is developed.

In general, I believe that developing *practical* QKD and real-life implementation will be beneficial for QKD in general in two aspects. First, it will bring QKD into practical cryptography, which will stimulate the assimilation of QKD as a cryptographic primitive by the classical cryptography field. Second, it will provide an ecosystem for the development of future QKD technologies. What is certain is that the field has an exciting future.

Appendix A

Upper bound on the differential entropy

This appendix concerns the derivation of the upper-bound on the differential entropy used in chapter 7. The upper-bound on the differential entropy between idle and communication states $D(\hat{\rho}_0||\hat{\rho}_1)$ was taken from the supplementary material of reference [90] and is given here for completeness. To find the bound, we proceed in two steps. First we find the expression for $D(\hat{\rho}_0||\hat{\rho}_1)$ and then we use Taylor's theorem with remainder to find the upper-bound.

A.1 Expression of the relative entropy $D(\hat{\rho}_0||\hat{\rho}_1)$

Let the idle and communication states $\hat{\rho}_0$ and $\hat{\rho}_1$ be the thermal states with mean photon number $\bar{n}_0$ and $\bar{n}_1$ respectively. The relative entropy between these states is given by $D(\hat{\rho}_0||\hat{\rho}_1) = \hat{\rho}_0 \ln \hat{\rho}_0 - \hat{\rho}_0 \ln \hat{\rho}_1 = -S(\hat{\rho}_0) - \hat{\rho}_0 \ln \hat{\rho}_1$. We have :

$$-S(\hat{\rho}_0) = \sum_{i=0}^{\infty} \frac{\bar{n}_0^i}{(1+\bar{n}_0)^{i+1}} \ln \frac{\bar{n}_0^i}{(1+\bar{n}_0)^{i+1}} \tag{A.1}$$

$$= \frac{1}{1+\bar{n}_0} \sum_{i=0}^{\infty} \left(\frac{\bar{n}_0}{1+\bar{n}_0} \right)^i \left[i \ln \frac{\bar{n}_0}{\bar{n}_0+1} + \ln \frac{1}{\bar{n}_0+1} \right] \tag{A.2}$$

which is the sum of two terms. First, $\frac{1}{1+n_0} \sum_{i=1}^{\infty} i \left(\frac{\bar{n}_0}{1+\bar{n}_0} \right)^{i-1} = 1 + \bar{n}_0$ as it can be seen as the mean of a geometrically distributed random variable X with success probability $\frac{1}{1+\bar{n}_0}$. Multiplying by $\frac{\bar{n}_0}{1+\bar{n}_0} \ln \frac{\bar{n}_0}{1+\bar{n}_0}$ gives the term in the left of the above equation. Second, the term $\frac{1}{1+\bar{n}_0} \sum_{i=0}^{\infty} \left(\frac{\bar{n}_0}{1+\bar{n}_0} \right)^i = 1$ because it is the geometric series of first term $\frac{1}{1+n_0}$ and common ratio $\frac{n_0}{1+n_0}$. Injecting these results in the above equation, we have :

$$-S(\hat{\rho}_0) = \bar{n}_0 \ln \frac{\bar{n}_0}{1+\bar{n}_0} + \ln \frac{1}{1+\bar{n}_0} \tag{A.3}$$

We can compute the second term of the relative entropy in a similar fashion :

$$-\hat{\rho}_0 \ln \hat{\rho}_1 = \sum_{i=0}^{\infty} \frac{\bar{n}_0^i}{(1+\bar{n}_0)^{i+1}} \ln \frac{(1+\bar{n}_1)^{i+1}}{\bar{n}_1^i} \tag{A.4}$$

$$= \frac{1}{1+\bar{n}_0} \sum_{i=0}^{\infty} \left(\frac{\bar{n}_0}{1+\bar{n}_0} \right)^i \left[i \ln \frac{1+\bar{n}_1}{\bar{n}_1} + \ln(1+\bar{n}_1) \right] \tag{A.5}$$

$$= \bar{n}_0 \ln \frac{1+\bar{n}_1}{\bar{n}_1} + \ln(1+\bar{n}_1) \tag{A.6}$$

The relative entropy $D(\hat{\rho}_0||\hat{\rho}_1)$ is the sum of these two terms :

$$D(\hat{\rho}_0||\hat{\rho}_1) = \bar{n}_0 \ln \frac{\bar{n}_0(1+\bar{n}_1)}{\bar{n}_1(1+\bar{n}_0)} + \ln \frac{1+\bar{n}_1}{1+\bar{n}_0} \tag{A.7}$$

A.2 Upper-bound by expansion in Taylor series

Let $\bar{n}_1 = \bar{n}_0 + x$ where x is the number of signal photons employed by Alice. The idle and communication states relative entropy is expressed as :

$$D(\hat{\rho}_0||\hat{\rho}_1) = \bar{n}_0 \ln \frac{\bar{n}_0(1+\bar{n}_0+x)}{(\bar{n}_0+x)(1+\bar{n}_0)} + \ln \frac{1+\bar{n}_0+x}{1+\bar{n}_0} \tag{A.8}$$

We find an upper-bound to this expression when x is close to 0 via a Taylor series expansion. Let $D(\hat{\rho}_0||\hat{\rho}_1) = f(x)$ and let us compute the successive derivatives of f :

$$f'(x) = \frac{x}{(\bar{n}_0+x)(1+\bar{n}_0+x)} \tag{A.9}$$

$$f^{(2)}(x) = \frac{\bar{n}_0 + \bar{n}_0^2 - x^2}{(\bar{n}_0+x)^2(1+\bar{n}_0+x)^2} \tag{A.10}$$

$$f^{(3)}(x) = \frac{-2x(\bar{n}_0+x)^2(1+\bar{n}_0+x)^2 - 2(\bar{n}_0+\bar{n}_0^2-x^2)\big[(\bar{n}_0+x)(1+\bar{n}_0+x)^2 + (\bar{n}_0+x)^2(1+\bar{n}_0+x)\big]}{(\bar{n}_0+x)^4(1+\bar{n}_0+x)^4} \tag{A.11}$$

When $x = 0$, the first two terms of the Taylor expansion are zero because $f(0) = f'(0) = 0$ and the fourth term is negative. Therefore we can upper-bound f by the third term which gives :

$$f(x) \leq f^2(0)\frac{x^2}{2} \tag{A.12}$$

$$= \frac{x^2}{2\bar{n}_0(1+\bar{n}_0)} \tag{A.13}$$

$$\tag{A.14}$$

By replacing $\bar{n}_0$ and x by $\bar{n}_{\text{th}}$ and $\bar{n}_A$ respectively we find the bound on the relative entropy valid when $\bar{n}_A$ is close to 0 :

$$D(\hat{\rho}_0||\hat{\rho}_1) \leq \frac{\bar{n}_A^2}{2\bar{n}_{\text{th}}(1+\bar{n}_{\text{th}})} \tag{A.15}$$

Which is the bound **??** given in the main document.

Bibliography

[1] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7 – 11, 2014.

[2] Richard P Feynman. Simulating physics with computers. In *Feynman and computation*, pages 133–153. CRC Press, 2018.

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

[4] John Preskill. Quantum computing in the nisq era and beyond. *Quantum*, 2:79, 2018.

[5] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A Buell, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.

[6] Lars S Madsen, Fabian Laudenbach, Mohsen Falamarzi Askarani, Fabien Rortais, Trevor Vincent, Jacob FF Bulmer, Filippo M Miatto, Leonhard Neuhaus, Lukas G Helt, Matthew J Collins, et al. Quantum computational advantage with a programmable photonic processor. *Nature*, 606(7912):75–81, 2022.

[7] Jay Gambetta. Ibm's roadmap for scaling quantum technology. 2020.

[8] Michele Mosca. Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, 16(5):38–41, 2018.

[9] Douglas Stebila and Michele Mosca. Post-quantum key exchange for the internet and the open quantum safe project. In *International Conference on Selected Areas in Cryptography*, pages 14–37. Springer, 2016.

[10] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 88:057902, Jan 2002.

[11] Richard J Hughes, Jane E Nordholt, Kevin P McCabe, Raymond T Newell, Charles G Peterson, and Rolando D Somma. Network-centric quantum communications with application to critical infrastructure protection. *arXiv preprint arXiv:1305.0305*, 2013.

[12] Masahide Sasaki, Mikio Fujiwara, H Ishizuka, W Klaus, K Wakui, M Takeoka, S Miki, T Yamashita, Z Wang, A Tanaka, et al. Field test of quantum key distribution in the tokyo qkd network. *Optics express*, 19(11):10387–10409, 2011.

[13] Damien Stucki, Matthieu Legre, Francois Buntschu, B Clausen, Nadine Felber, Nicolas Gisin, Luca Henzen, Pascal Junod, Gérald Litzistorf, Patrick Monbaron, et al. Long-term performance of the swissquantum quantum key distribution network in a field environment. *New Journal of Physics*, 13(12):123001, 2011.

[14] Rachel Courtland. China's 2,000-km quantum link is almost complete [news]. *IEEE Spectrum*, 53(11):11–12, 2016.

[15] Momtchil Peev, Christoph Pacher, Romain Alléaume, Claudio Barreiro, Jan Bouda, W Boxleitner, Thierry Debuisschert, Eleni Diamanti, Mehrdad Dianati, JF Dynes, et al. The secoqc quantum key distribution network in vienna. *New Journal of Physics*, 11(7):075001, 2009.

[16] Romain Alléaume, Raphaël Aymeric, Cédric Ware, and Yves Jaouën. Technology trends for mixed qkd/wdm transmission up to 80 km. In *2020 Optical Fiber Communications Conference and Exhibition (OFC)*, pages 1–3. IEEE, 2020.

[17] Fabian Laudenbach, Bernhard Schrenk, Christoph Pacher, Michael Hentschel, Chi-Hang Fred Fung, Fotini Karinou, Andreas Poppe, Momtchil Peev, and Hannes Hübel. Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator. *Quantum*, 3:193, 2019.

[18] Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.

[19] Rodney Loudon. *The quantum theory of light*. OUP Oxford, 2000.

[20] Fabian Laudenbach, Christoph Pacher, Chi-Hang Fred Fung, Andreas Poppe, Momtchil Peev, Bernhard Schrenk, Michael Hentschel, Philip Walther, and Hannes Hübel. Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations (adv. quantum technol. 1/2018). *Advanced Quantum Technologies*, 1(1):1870011, 2018.

[21] Robert B Ash. *Information theory*. Courier Corporation, 2012.

[22] Michele Mosca. The quantum threat to cryptography - cryptoexperts. *https://cryptoexperts.com/*.

[23] Robert J McEliece. A public-key cryptosystem based on algebraic. *Coding Thv*, 4244:114–116, 1978.

[24] Tsutomu Matsumoto and Hideki Imai. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 419–453. Springer, 1988.

[25] Richard Lindner and Chris Peikert. Better key sizes (and attacks) for lwe-based encryption. In *Cryptographers' Track at the RSA Conference*, pages 319–339. Springer, 2011.

[26] Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology*, 8(3):209–247, 2014.

[27] Yi Zhao, Chi-Hang Fred Fung, Bing Qi, Christine Chen, and Hoi-Kwong Lo. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Physical Review A*, 78(4):042333, 2008.

[28] Feihu Xu, Bing Qi, and Hoi-Kwong Lo. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New Journal of Physics*, 12(11):113026, 2010.

[29] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature photonics*, 4(10):686–689, 2010.

[30] Paul Jouguet, Sébastien Kunz-Jacques, and Eleni Diamanti. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. *Physical Review A*, 87(6):062313, 2013.

[31] Xiang-Chun Ma, Shi-Hai Sun, Mu-Sheng Jiang, and Lin-Mei Liang. Local oscillator fluctuation opens a loophole for eve in practical continuous-variable quantum-key-distribution systems. *Physical Review A*, 88(2):022339, 2013.

[32] Jing-Zheng Huang, Christian Weedbrook, Zhen-Qiang Yin, Shuang Wang, Hong-Wei Li, Wei Chen, Guang-Can Guo, and Zheng-Fu Han. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. *Phys. Rev. A*, 87:062329, Jun 2013.

[33] John S Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1(3):195, 1964.

[34] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47(10):777, 1935.

[35] Samuel L Braunstein and Stefano Pirandola. Side-channel-free quantum key distribution. *Physical review letters*, 108(13):130502, 2012.

[36] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Physical review letters*, 108(13):130503, 2012.

[37] Robert Bedington, Juan Miguel Arrazola, and Alexander Ling. Progress in satellite quantum key distribution. *npj Quantum Information*, 3(1):1–13, 2017.

[38] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. *Nature communications*, 8(1):1–15, 2017.

[39] Frédéric Grosshans, Nicolas J Cerf, Jérôme Wenger, Rosa Tualle-Brouri, and Ph Grangier. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. *arXiv preprint quant-ph/0306141*, 2003.

[40] Margaret D Reid. Quantum cryptography with a predetermined key, using continuous-variable einstein-podolsky-rosen correlations. *Physical Review A*, 62(6):062308, 2000.

[41] Timothy C Ralph. Security of continuous-variable quantum cryptography. *Physical Review A*, 62(6):062306, 2000.

[42] Andrew M Lance, Thomas Symul, Vikram Sharma, Christian Weedbrook, Timothy C Ralph, and Ping Koy Lam. No-switching quantum key distribution using broadband modulated coherent light. *Physical review letters*, 95(18):180503, 2005.

[43] Christian Weedbrook, Andrew M Lance, Warwick P Bowen, Thomas Symul, Timothy C Ralph, and Ping Koy Lam. Coherent-state quantum key distribution without random basis switching. *Physical Review A*, 73(2):022316, 2006.

[44] Frédéric Grosshans, Gilles Van Assche, Jérôme Wenger, Rosa Brouri, Nicolas J Cerf, and Philippe Grangier. Quantum key distribution using gaussian-modulated coherent states. *Nature*, 421(6920):238–241, 2003.

[45] Matthias Christandl, Robert König, and Renato Renner. Postselection technique for quantum channels with applications to quantum cryptography. *Physical review letters*, 102(2):020504, 2009.

[46] Anthony Leverrier. Security of continuous-variable quantum key distribution via a gaussian de finetti reduction. *Physical review letters*, 118(20):200501, 2017.

[47] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and engineering sciences*, 461(2053):207–235, 2005.

[48] Aurélie Denys, Peter Brown, and Anthony Leverrier. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. *Quantum*, 5:540, 2021.

[49] Raúl García-Patrón and Nicolas J Cerf. Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution. *Physical review letters*, 97(19):190503, 2006.

[50] Anthony Leverrier and Philippe Grangier. Simple proof that gaussian attacks are optimal among collective attacks against continuous-variable quantum key distribution with a gaussian modulation. *Physical Review A*, 81(6):062314, 2010.

[51] Shouvik Ghorai, Philippe Grangier, Eleni Diamanti, and Anthony Leverrier. Asymptotic security of continuous-variable quantum key distribution with a discrete modulation. *Physical Review X*, 9(2):021059, 2019.

[52] Jie Lin, Twesh Upadhyaya, and Norbert Lütkenhaus. Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution. *Physical Review X*, 9(4):041064, 2019.

[53] Renato Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 6(01):1–127, 2008.

[54] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *Proceedings 42nd IEEE Symposium on Foundations of Computer Science*, pages 136–145. IEEE, 2001.

[55] Anthony Leverrier, Frédéric Grosshans, and Philippe Grangier. Finite-size analysis of a continuous-variable quantum key distribution. *Physical Review A*, 81:062343, 2010. 12 pages, 4 figures, updated references.

[56] Renato Renner. Symmetry of large physical systems implies independence of subsystems. *Nature Physics*, 3(9):645–649, 2007.

[57] Marco Tomamichel and Renato Renner. Uncertainty relation for smooth entropies. *Physical review letters*, 106(11):110506, 2011.

[58] Frederic Dupuis, Omar Fawzi, and Renato Renner. Entropy accumulation. *Communications in Mathematical Physics*, 379(3):867–913, 2020.

[59] Renato Renner and J Ignacio Cirac. de finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Physical review letters*, 102(11):110504, 2009.

[60] Alberto Boaron, Gianluca Boso, Davide Rusca, Cédric Vulliez, Claire Autebert, Misael Caloz, Matthieu Perrenoud, Gaëtan Gras, Félix Bussières, Ming-Jun Li, et al. Secure quantum key distribution over 421 km of optical fiber. *Physical review letters*, 121(19):190502, 2018.

[61] Bernd Fröhlich, Marco Lucamarini, James F Dynes, Lucian C Comandar, Winci W-S Tam, Alan Plews, Andrew W Sharpe, Zhiliang Yuan, and Andrew J Shields. Long-distance quantum key distribution secure against coherent attacks. *Optica*, 4(1):163–167, 2017.

[62] Shuang Wang, Wei Chen, Jun-Fu Guo, Zhen-Qiang Yin, Hong-Wei Li, Zheng Zhou, Guang-Can Guo, and Zheng-Fu Han. 2 ghz clock quantum key distribution over 260 km of standard telecom fiber. *Optics letters*, 37(6):1008–1010, 2012.

[63] Boris Korzh, Charles Ci Wen Lim, Raphael Houlmann, Nicolas Gisin, Ming Jun Li, Daniel Nolan, Bruno Sanguinetti, Rob Thew, and Hugo Zbinden. Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nature Photonics*, 9(3):163–168, 2015.

[64] Yichen Zhang, Ziyang Chen, Stefano Pirandola, Xiangyu Wang, Chao Zhou, Binjie Chu, Yijia Zhao, Bingjie Xu, Song Yu, and Hong Guo. Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. *Physical review letters*, 125(1):010502, 2020.

[65] Duan Huang, Peng Huang, Dakai Lin, and Guihua Zeng. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Scientific reports*, 6(1):1–9, 2016.

[66] Danna Rosenberg, Charles G Peterson, JW Harrington, Patrick R Rice, N Dallmann, KT Tyagi, KP McCabe, Sae Nam, Burm Baek, RH Hadfield, et al. Practical long-distance quantum key distribution system using decoy levels. *New Journal of Physics*, 11(4):045009, 2009.

[67] Max Rückmann and Christian G. Schaeffer. 1 gbaud heterodyne continuous variable quantum key distribution over 26 km fiber. In *2019 Conference on Lasers and Electro-Optics (CLEO)*, pages 1–2, 2019.

[68] Cédric Bruynsteen, Michael Vanhoecke, Johan Bauwelinck, and Xin Yin. Integrated balanced homodyne photonic–electronic detector for beyond 20 ghz shot-noise-limited measurements. *Optica*, 8(9):1146–1152, 2021.

[69] Bing Qi, Wen Zhu, Li Qian, and Hoi-Kwong Lo. Feasibility of quantum key distribution through a dense wavelength division multiplexing network. *New Journal of Physics*, 12(10):103042, 2010.

[70] Rupesh Kumar, Hao Qin, and Romain Alléaume. Coexistence of continuous variable qkd with intense dwdm classical channels. *New Journal of Physics*, 17(4):043027, 2015.

[71] Tobias A Eriksson, Takuya Hirano, Benjamin J Puttnam, Georg Rademacher, Ruben S Luís, Mikio Fujiwara, Ryo Namiki, Yoshinari Awaji, Masahiro Takeoka, Naoya Wada, et al. Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 tbit/s data channels. *Communications Physics*, 2(1):1–8, 2019.

[72] James F Dynes, Winci WS Tam, Alan Plews, Bernd Fröhlich, Andrew W Sharpe, Marco Lucamarini, Zhiliang Yuan, Christian Radig, Andrew Straw, Tim Edwards, et al. Ultra-high bandwidth quantum secured data transmission. *Scientific reports*, 6(1):1–6, 2016.

[73] Kazuro Kikuchi. Fundamentals of coherent optical fiber communications. *Journal of lightwave technology*, 34(1):157–179, 2015.

[74] Paul Jouguet, Sébastien Kunz-Jacques, Anthony Leverrier, Philippe Grangier, and Eleni Diamanti. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature photonics*, 7(5):378–381, 2013.

[75] Tao Wang, Peng Huang, Lang Li, Yingming Zhou, and Guihua Zeng. Boosting higher secret key rate in quantum key distribution over mature telecom components. 2021.

[76] Yichen Zhang, Zhengyu Li, Ziyang Chen, Christian Weedbrook, Yijia Zhao, Xiangyu Wang, Yundi Huang, Chunchao Xu, Xiaoxiong Zhang, Zhenya Wang, et al. Continuous-variable qkd over 50 km commercial fiber. *Quantum Science and Technology*, 4(3):035006, 2019.

[77] Yan Pan, Heng Wang, Yun Shao, Yaodi Pi, Yang Li, Bin Liu, Wei Huang, and Bingjie Xu. Experimental demonstration of high-rate discrete-modulated continuous-variable quantum key distribution system. *arXiv preprint arXiv:2203.08470*, 2022.

[78] François Roumestan, Amirhossein Ghazisaeidi, Jeremie Renaudier, Luis Trigo Vidarte, Eleni Diamanti, and Philippe Grangier. High-rate continuous variable quantum key distribution based on probabilistically shaped 64 and 256-qam. In *2021 European Conference on Optical Communication (ECOC)*, pages 1–4. IEEE, 2021.

[79] Shengjun Ren, Shuai Yang, Adrian Wonfor, Ian White, and Richard Penty. Demonstration of high-speed and low-complexity continuous variable quantum key distribution system with local local oscillator. *Scientific Reports*, 11(1):1–13, 2021.

[80] Sebastian Kleis, Joachim Steinmayer, Rainer H Derksen, and Christian G Schaeffer. Experimental investigation of heterodyne quantum key distribution in the s-band embedded in a commercial dwdm system. In *Optical Fiber Communication Conference*, pages Th1J–3. Optical Society of America, 2019.

[81] Sebastian Kleis and Christian G Schaeffer. Improving the secret key rate of coherent quantum key distribution with bayesian inference. *Journal of Lightwave Technology*, 37(3):722–728, 2018.

[82] Hou-Man Chin, Nitin Jain, Darko Zibar, Ulrik L Andersen, and Tobias Gehring. Machine learning aided carrier recovery in continuous-variable quantum key distribution. *npj Quantum Information*, 7(1):1–6, 2021.

[83] HJ Landau. Sampling, data transmission, and the nyquist rate. *Proceedings of the IEEE*, 55(10):1701–1706, 1967.

[84] Sebastian Kleis, Max Rueckmann, and Christian G Schaeffer. Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals. *Optics letters*, 42(8):1588–1591, 2017.

[85] Darko Zibar, Molly Piels, Rasmus Jones, and Christian G Schäeffer. Machine learning techniques in optical communication. *Journal of Lightwave Technology*, 34(6):1442–1452, 2015.

[86] B. A. Bash, D. Goeckel, and D. Towsley. Square root law for communication with low probability of detection on awgn channels. In *2012 IEEE International Symposium on Information Theory Proceedings*, pages 448–452, 2012.

[87] L. Wang, G. W. Wornell, and L. Zheng. Fundamental limits of communication with low probability of detection. *IEEE Transactions on Information Theory*, 62(6):3493–3503, 2016.

[88] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha. Hiding information in noise: fundamental limits of covert wireless communication. *IEEE Communications Magazine*, 53(12):26–31, 2015.

[89] B. A. Bash, D. Goeckel, and D. Towsley. Limits of reliable communication with low probability of detection on awgn channels. *IEEE Journal on Selected Areas in Communications*, 31(9):1921–1930, 2013.

[90] Patel M. et al. Bash B., Gheorghe A. Quantum-secure covert communication on bosonic channels. *Nat Commun*, 6(8626), 2015.

[91] Michael S. Bullock, Christos N. Gagatsos, Saikat Guha, and Boulat A. Bash. Fundamental limits of quantum-secure covert communication over bosonic channels. In *2019 57th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 56–63, 2019.

[92] M. Tahmasbi and M. R. Bloch. Toward undetectable quantum key distribution over bosonic channels. *IEEE Journal on Selected Areas in Information Theory*, 1(2):585–598, 2020.

[93] Mehrdad Tahmasbi and Matthieu R. Bloch. Framework for covert and secret key expansion over classical-quantum channels. *Phys. Rev. A*, 99:052329, May 2019.

[94] Juan Miguel Arrazola and Valerio Scarani. Covert quantum communication. *Phys. Rev. Lett.*, 117:250503, Dec 2016.

[95] Yang Liu, Juan Miguel Arrazola, Wen-Zhao Liu, Weijun Zhang, Ignatius William Primaatmaja, Hao Li, Lixing You, Zhen Wang, Valerio Scarani, Qiang Zhang, and Jian-Wei Pan. Experimental unconditionally secure covert communication in dense wavelength-division multiplexing networks, 2017.

[96] Mark M. Wilde. *Quantum Information Theory*. Cambridge University Press, 2013.

[97] Marvin K. Simon, Jim K. Omura, Robert A. Scholtz, and Barry K. Levitt. *Spread Spectrum Communications Handbook (Revised Ed.)*. McGraw-Hill, Inc., USA, 1994.

[98] François Roumestan, Amirhossein Ghazisaeidi, Haik Mardoyan, Jérémie Renaudier, Eleni Diamanti, and Philippe Grangier. 6 mb/s secret key rate transmission over 13.5 km smf using pcs-256qam super-channel continuous variable quantum key distribution. In *Optical Fiber Communication Conference*, pages Tu3I–4. Optica Publishing Group, 2022.

[99] T. V. Sobers, B. A. Bash, S. Guha, D. Towsley, and D. Goeckel. Covert communication in the presence of an uninformed jammer. *IEEE Transactions on Wireless Communications*, 16(9):6193–6206, 2017.

[100] Ramin Soltani, Dennis Goeckel, Don Towsley, Boulat A. Bash, and Saikat Guha. Covert wireless communication with artificial noise generation. *IEEE Transactions on Wireless Communications*, 17(11):7252–7267, 2018.

[101] Juan Miguel Arrazola and Ryan Amiri. Secret-key expansion from covert communication. *Phys. Rev. A*, 97:022325, Feb 2018.

[102] Frank Gaitan. Finding flows of a navier–stokes fluid through quantum computing. *npj Quantum Information*, 6(1):1–6, 2020.

[103] Yudong Cao, Jonathan Romero, Jonathan P Olson, Matthias Degroote, Peter D Johnson, Mária Kieferová, Ian D Kivlichan, Tim Menke, Borja Peropadre, Nicolas PD Sawaya, et al. Quantum chemistry in the age of quantum computing. *Chemical reviews*, 119(19):10856–10915, 2019.

[104] Vedran Dunjko and Hans J Briegel. Machine learning & artificial intelligence in the quantum domain: a review of recent progress. *Reports on Progress in Physics*, 81(7):074001, 2018.

[105] Esteban A Martinez, Christine A Muschik, Philipp Schindler, Daniel Nigg, Alexander Erhard, Markus Heyl, Philipp Hauke, Marcello Dalmonte, Thomas Monz, Peter Zoller, et al. Real-time dynamics of lattice gauge theories with a few-qubit quantum computer. *Nature*, 534(7608):516–519, 2016.

[106] Valerio Scarani and Christian Kurtsiefer. The black paper of quantum cryptography: real implementation problems. *Theoretical Computer Science*, 560:27–32, 2014.

[107] Cosmo Lupo and Yingkai Ouyang. Quantum key distribution with nonideal heterodyne detection: Composable security of discrete-modulation continuous-variable protocols. *PRX Quantum*, 3(1):010341, 2022.

[108] Adnan AE Hajomer, Hossein Mani, Nitin Jain, Hou-Man Chin, Ulrik L Andersen, and Tobias Gehring. Continuous-variable quantum key distribution over 60 km optical fiber with real local oscillator. *arXiv preprint arXiv:2205.15161*, 2022.

[109] William J Munro, Koji Azuma, Kiyoshi Tamaki, and Kae Nemoto. Inside quantum repeaters. *IEEE Journal of Selected Topics in Quantum Electronics*, 21(3):78–90, 2015.

[110] ANSSI. L'avenir des communications sécurisées passe-t-il par la distribution quantique de clés ?

[111] BSI. Quantum-safe cryptography–fundamentals, current developments and recommendations.

[112] NCSC. Quantum security technologies.

[113] NSA. Quantum key distribution (qkd) and quantum cryptography qc.

[114] Johannes Braun, Johannes Buchmann, Denise Demirel, Matthias Geihs, Mikio Fujiwara, Shiho Moriai, Masahide Sasaki, and Atsushi Waseda. Lincos: A storage system providing long-term integrity, authenticity, and confidentiality. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, pages 461–468, 2017.

[115] Nilesh Vyas and Romain Alléaume. Everlasting secure key agreement with performance beyond qkd in a quantum computational hybrid security model. *arXiv preprint arXiv:2004.10173*, 2020.

ECOLE DOCTORALE

Titre : Convergence des communications quantique et classique

Mots clés : quantique, télécommunications, cryptographie, qkd

Résumé : Les protocoles de distribution de clé quantique (QKD) permettent de construire des canaux de communications sensibles à l'espionage grace aux propriétés quantiques fondamentales de la lumière. L'un des principaux défis à surpasser pour déployer de tels protocoles à grande échelle est le coût de déployement de la technologie. Une solution attrayante en ce sens serait d'exploiter l'infrastructure de fibre optique déjà existante pour executer mettre en oeuvre de tels protocoles.
Cela implique cependant de faire coexister des signaux quantiques avec des signaux télécoms classiques, ce qui peut être un défi de part la sensibilité des états quantiques aux perturbations. Ici, nous nous intéressons plus particulièrement aux protocoles de distribution de clé quantique à variables continues (CV-QKD), car leur proximité avec les communications cohérentes classiques indiquent qu'ils sont de bons candidats pour coexister sur une même fibre.
En partant du principe que les protocoles CV-QKD sont destinés, à terme, à être déployés de manière conjointe avec des protocoles de communication classique, la question qui se pose est la suivante. Cette coexistence avec des signaux classiques est-elle forcément un désavantage pour la CV-QKD ? Nous montrons qu'en construisant de façon conjointe des protocoles de communication quantique et classique, alors la coexistence peut présenter des avantages exploitables pour la CV-QKD.
Dans un premier travail, nous démontrons expérimentalement que le signal classique peut servir de signal pilote au signal quantique, ce qui permet notamment de s'affranchir de signaux pilotes auxiliaires généralement nécessaires en CV-QKD.
Dans un second travail, nous montrons que le bruit généré par des canaux classiques peut servir à dissimuler le signal quantique. La communication quantique peut alors être réalisée de façon indétectable, ou « covert », ce qui, combiné à une échange de clé par QKD permet d'envisager des garanties de sécurité extrêmement élevées. Nous analysons les conditions nécessaires, à la faisabilité du déploiement covert de la CV-QKD.

Title : Convergence of quantum and classical communications

Keywords : quantum, telecommunications, cryptography, qkd

Abstract : Quantum key distribution (QKD) protocols harness fundamental quantum properties of the light to construct communication channels sensitive to eavesdropping. In order to develop the technology at large scale, one of the main challenges to overcome is the deployment cost of such systems. A significant step towards reducing deployment costs would be to use the existing optical fiber infrastructure to perform QKD, since this would relax the need to use dark (and expensive !) fiber. However this also means we must insure QKD protocols can coexist with classical communications, which can be challenging as quantum states are very sensitive to perturbations. Here, we focus particularly on continuous-variable (CV) QKD because their natural proximity to classical coherent communication systems indicates that they are good candidates for coexistence over the same fiber.
Assuming CV-QKD is destined to be incorporated in classical communication links, an interesting question is whether the coexistence with classical channels will necessarily be detrimental to the CV-QKD protocol. We show that in some cases, coexistence can actually provide an advantage to the CV-QKD protocol.
In a first project, we experimentally demonstrate that a classical channel can be used as a pilot signal for the quantum channel. Thus, the need for pilot-tones, mandatory in a typical CV-QKD protocol, can be relaxed.
In a second project, we show that the noise generated by classical channels can be used to "hide" the quantum signal. The quantum communication therefore can become covert thanks to the classical channels. Covert QKD protocols are interesting because they provide extreme security guarantees. We investigate the necessary conditions for covert CV-QKD as well as scenarios for its deployment in a practical setting.

Institut Polytechnique de Paris
91120 Palaiseau, France