Continuous Variable Quantum Key Distribution over Long Distances

Masoud Ghalaii

University of Leeds

Faculty of Engineering and Physical Sciences

Doctor of Philosophy

September 2019

12 000 years ago, a couple marked themselves on a rock in Mount Homian, Kuhdasht County[1]*, Lorestan Province, Iran; they were dancing.*

To my wife, Parisa,
And
The dancing seconds
Never-ending on the Homian rocks.

[1] My birthplace.

I declare that the research described in this thesis is original study, which I undertook at the University of Leeds during 2015 - 2019. This work has not previously been presented for an award at this, or any other, university. Except where stated, all of the work contained within this thesis represents the original contribution of the author.

Some parts of the material in this thesis has been published in journals and conference proceedings, or made available online on the arXiv. The author of this thesis acknowledges the input of his collaborators, and has credited them appropriately throughout. A list of papers which overlap with this thesis are presented here.

- *Realistic threat models for satellite quantum key distribution*
Masoud Ghalaii, Sima Bahrani, Carlo Liorni, Alexander Ling, Rupesh Kumar, Bruno Huttner, Stefano Pirandola, Charles Lim Ci Wen, Tim Spiller, Norbert Lütkenhaus, and Mohsen Razavi. In preparation.

The modelling has been conceived in collaboration with Sima Bahrani and Mohsen Razavi. I have analysed the continuous-variable quantum key distribution (CV-QKD) examples, as appear in chapter 6.

- *Discrete-modulation continuous-variable quantum key distribution enhanced by quantum scissors*
Masoud Ghalaii, Carlo Ottaviani, Rupesh Kumar, Stefano Pirandola, and Mohsen Razavi. Published in IEEE Journal on Selected Areas in Communications (JSAC), Digital Object Identifier (DOI): 10.1109/JSAC.2020.2969058.

I have developed the modelling and analysis, and drafted the paper. The results of this work appear in chapter 5.

• *Long-distance continuous-variable quantum key distribution with quantum scissors*
Masoud Ghalaii, Carlo Ottaviani, Rupesh Kumar, Stefano Pirandola, and Mohsen Razavi. Published in for IEEE Journal of Selected Topics in Quantum Electronics (JSTQE), Digital Object Identifier (DOI): 10.1109/JSTQE.2020.2964395.

I have developed the modelling and analysis, and drafted the paper. The results of this work appear in chapter 4.

The following publication is also relevant to this thesis:

• *Quantum-classical access networks with embedded optical wireless links*
Osama Elmabrok, Masoud Ghalaii, and Mohsen Razavi. Published in Journal of the Optical Society of America B **35**, 487-499 (2018).

I have worked out the CV-QKD scenarios in this paper as appear in figures 10 and 11, and contributed to the drafting of this paper.

A list of conference papers relevant to this thesis are presented here.

• Bahrani S, Ghalaii M, Liorni C, Ling A, Kumar R, Huttner B, Pirandola S, Wen C C W, Spiller T, Lütkenhaus N, and Razavi M (August 2019) *Realistic threat models for satellite quantum key distribution*, QCrypt19, Montreal, Canada.

• Bahrani S; Elmabrok O; Curras Lorenzo G; Ghalaii M; Razavi M (July 2019) *Quantum and classical communications on shared infrastructure*, 21st International Conference on Transparent Optical Networks (ICTON), Angers, France.

• Ghalaii M, Kumar R, Ottaviani C, Pirandola S, Razavi M (September 2017) *Long-distance continuous-variable quantum key distribution with quantum scissors*, QCrypt17, Cambridge, UK.

• Ghalaii M, Kumar R, Ottaviani C, Pirandola S, Razavi M (September 2017) *Long-distance continuous-variable quantum cryptography* *by using quantum scissors*, International Conference on Quantum, Atomic, Molecular and Plasma Physics, Glasgow, UK.

- Ghalaii M, Kumar R, Razavi M (2017) *Quantum-scissor amplified continuous-variable quantum key distribution*, CLEO/Europe, Munich, Germany.

Acknowledgements

I would like to express my cordial appreciation and respect to my supervisour, Professor Mohsen Razavi, for his all-inclusive support, insights, patience, and brilliant supervision during my Ph.D. career.

I would like to thank Professor Stefano Pirandola, Dr. Carlo Ottaviani, and Dr. Rupesh Kumar, at the University of York, for the marvellous collaboration, their advices, and prompt replies.

I would like to thank my peers, Dr. Sima Bahrani and Dr. Osama Elmabrok, for the constructive collaboration, as well as fruitful discussions. I would like to thank Carlo Liorni for providing me with the supporting data related to our satellite-based analysis. I would like to thank Aleksandar Demić, who now and again helped me out with MATLAB coding and who has been introducing and offering countless types of tea.

I would like to thank Professor Vahid Karimipour and Dr. Ali T. Rezakhani, at Sharif University of Technology, Tehran, Iran, who, during my M.Sc. major, paved the way for me to step into quantum information science.

I have had wonderful moments with my friends at University of Leeds, and elsewhere. I would like to especially thank Amin Sadeghpour, Marjan Samiepour, Lionel Zayeh Kooktapeh, Kowsar Shahbazi, Mahmood Parsi, Arash Valipour, Saleh Salavati, Aida Payan, Nasser Gohari Kamel, Mohammad Mehboudi, Majid Hassani, Faraj Bakhshinezhad, Maryam Afsary, and Saleh Riahi Samani for their support, kindness, and phone calls during the past four years.

I would like to express my regards towards my family. My mother and father, sister, and brothers, who have always been encouraging. Being fortunate, this year, I have also been receiving the love and support of my parents- and brother-in-law. My unlimited thanks and love to my wife, Parisa, whom I had the pleasure and honour to marry during the last year of my Ph.D. This thesis is dedicated to her for all her love, support, encouragement, and patience.

This work was supported by the UK White Rose Research Studentship and partially by the UK EPSRC Grant No. EP/M013472/1.

Abstract

Quantum key distribution (QKD) is fundamentally different from most classical key distribution schemes, such as Diffie-Hellman key exchange, in the sense that no computational complexity assumption is required on the power of adversaries to prove its security. QKD relies on basic laws of quantum physics and it is proven that it can enable highly secure data communication. Such achievements, however, are facing technological problems that have to be resolved in order to provide a viable solution to a large group of customers. While there are discrete-variable QKD schemes, which rely on encoding data in discrete degrees of freedom, such as polarization of single photons, in this thesis, we focus on the continuous-variable QKD (CV-QKD) protocols, in which data is encoded on the quadratures of light. Currently, one of the major drawbacks of CV-QKD is its poor performance at long distances. Nevertheless, such a limitation in CV-QKD can be overcome with the assistance of quantum repeaters that rely on entanglement distillation via noiseless linear amplifiers (NLAs). Such systems can, in principle, offer large secret key rates over long distances. In this thesis, we aim to provide a realistic analysis of a CV-QKD protocol running over quantum scissors (QSs) as realistic NLAs. We will report the obstacles that one could face in realizing CV-QKD in such a scenario. A review of CV-QKD and QS-based NLAs will be given, based on which QS-assisted CV-QKD is proposed. We, particularly, focus on the modelling of the QSs' structure and their effect on the secret key rate aiming to find operational regimes where the performance of the QKD scheme is enhanced. This study paves the way for implementing long-distance CV-QKD protocols that rely on QS/NLA devices over CV quantum repeaters.

In this thesis, we also consider and account for a realistic analysis of a CV-QKD protocol with non-Gaussian modulation, which is assisted by the means of QSs. We will show that, while we have to deal with similar obstacles as in the Gaussian modulation, we can potentially improve performance of the non-Gaussian modulation protocol.

As an alternative approach to extend the secure distance of CV-QKD protocols, the last part of this thesis is devoted to presenting realistic threat models for satellite QKD, wherein we consider several eavesdropping scenarios by limiting eavesdroppers' access to the trusted ground and/or satellite stations. In such scenarios, the eavesdropper has only limited access to the sender and/or receiver stations. For example, we will explore the case where an eavesdropper can only receive an attenuated version of the transmitted signals. As well, we will focus on the case where Eve's signals would reach the receiver via a lossy channel inaccessible to the eavesdropper. We show that, in the case of both Gaussian and non-Gaussian protocols, this limitation would allow trusted parties to achieve higher key rates than what can be achieved when unrestricted eavesdropping is possible.

Abbreviations

CM	**C**ovariance **M**atrix
CV	**C**ontinuous-**V**ariable (States/Systems/Protocols)
CV-QKD	**C**ontinuous-**V**ariable **Q**uantum **K**ey **D**istribution
DR	**D**irect **R**econciliation
DV	**D**iscrete-**V**ariable (States/Systems/Protocols)
DV-QKD	**D**iscrete-**V**ariable **Q**uantum **K**ey **D**istribution
EB	**E**ntanglement-**B**ased (QKD)
GG02	**G**rosshans and **G**rangier 20**02** (CV-QKD Protocol)
Het	**Het**rodyne Detection
Hom	**Hom**odyne Detection
LEO	**L**ow-**E**arth-**O**rbit (Satellites)
MB-NLA	**M**easurement-**B**ased NLA
NLA	**N**oiseless **L**inear **A**mplifier
P&M	**P**repare-**and**-**M**easure (QKD)
QKD	**Q**uantum **K**ey **D**istribution
QM	**Q**uantum **M**emory
QPSK	**Q**uadrature-**P**hase-**S**hift-**K**eying (CV-QKD Protocol)
QR	**Q**uantum **R**epeater
QS	**Q**uantum **S**cissor
RL-NLA	T. C. **R**alph & A. P. **L**und **N**oiseless **L**inear **A**mplifier
RR	**R**everse **R**econciliation
SNR	**S**ignal-to-**N**oise **R**atio
SNU	**S**hot **N**oise **U**nits
SPS	**S**ignal **P**hoton **S**ource
TMSV	**T**wo-**M**ode **S**queezed **V**acuum

Contents

List of Figures

Chapter 1

Introduction

Cryptography is a set of techniques that allow for secure communication where non-legitimate parties, also called adversaries or eavesdroppers, are present. For instance, an arbitrary plain text message can be converted into a seemingly balderdash cipher text via encryption. In order to encrypt a message, a secret key, which is a piece of random information, is often shared between the two ends of a communications link. Decryption is then used by the receiver to recover the plaintext by using the key. See The Code Book by Singh [2002] for the history of cryptography.

Cryptography has recently been expanded to include new paradigms that rely on the new field of quantum information science. This new field, known as quantum cryptography, contains some of the most well-known applications of quantum communications. The most mature of such applications is quantum key distribution (QKD), which allows two parties to securely exchange a secret key through a quantum channel Gisin *et al.* [2002]. The latter is a physical medium, which is used to send quantum states. The term “quantum” indicates that in such a key distribution protocol quantum properties such as entanglement and/or non-orthogonality are utilized. Although the key is created using quantum features, it can also be used for secure transmission of classical information, e.g., by using the one-time pad encryption technique, which is known as the only information-theoretically secure means of encrypting information in the history of cryptography Shannon [1949]. The significant attribute of QKD, as a key distribution protocol, is that it does not make any assumption on the power of the eavesdroppers except that they are restricted by the laws of quantum mechanics. In contrast, classical key distribution techniques are often only secure against certain groups of adversaries with limited computational power. In this sense, QKD methods are said to be unconditionally secure Renner [2005]. More importantly, QKD offers future-proof security, in the sense that future advancement of technology would not affect its security.

A potential, and viable, candidate for sending quantum information is light. In fact, the very first QKD protocol, the so-called BB84 after Bennett & Brassard [1984, 2014], is based on encoding data on the polarization of single photons. BB84, along with some other methods that use polarization or other degrees of freedom of single photons (or weak coherent light), are typically called discrete-variable quantum key distribution (DV-QKD). In contrast, continuous-variable quantum key distribution (CV-QKD) protocols exploit aspects of light with continuous representation, such as the amplitude and/or the phase of the electromagnetic field.

The recent progress in CV-QKD systems Jouguet *et al.* [2013] has placed them in a competitive position with their conventional DV counterparts. For instance, contrary to DV-QKD protocols, which require single-photon detectors, CV-QKD systems use coherent detection techniques to measure light quadratures. Such measurements can be faster and more efficient than single-photon detection. Moreover, CV-QKD protocols might be the better choice over short distances Pirandola *et al.* [2015b].

Continuous-variable QKD at long distances is not, however, as easy as it sounds. Despite the above progress, once it comes to long distances, CV-QKD has its own challenges to go beyond hundreds of kilometres Jouguet *et al.* [2011]. The main physical limitations, apart from imperfection of transmitter and receiver devices, are path loss and environmental noise. In response to the above concerns, attractive candidates have been introduced for long-distance QKD that can be examined. For instance, similar to DV systems, one can think of using quantum repeaters (QRs) Briegel *et al.* [1998]. In fact, a CV version of QRs has recently been proposed by Dias & Ralph [2017], which relies on CV teleportation techniques Braunstein & Kimble [1998], Pirandola *et al.* [2015a] and noiseless linear amplifiers (NLAs) Caves *et al.* [2012]. In this dissertation, we will study the performance of CV-QKD systems that run over components of such continuous-variable QRs (CV QRs).

The alternative approach to enabling long-distance CV-QKD, in order to increase the secure distance of QKD, is to use satellite-based communications links Bonato *et al.* [2009], Bourgoin *et al.* [2014], Liao *et al.* [2017b]. Here, the scenarios such as ground-to-satellite Liao *et al.* [2017a], satellite-to-ground Ren *et al.* [2017], and/or satellite-to-satellite quantum communications channels can be considered. Satellite-based QKD, in company with a reliable QR infrastructure, can then be seen as a part of a global solution to quantum cryptography networks Razavi [2018] that enables quantum internet Kimble [2008], Azuma [2019].

In the following, we present an overview of CV-QKD as well as the CV QR scheme and satellite-based QKD. Next, at the end of the chapter, we introduce research objectives and the scope of this study.

1.1 Continuous-variable quantum key distribution: Overview

Key distribution is a technique that is used by two parties, traditionally named Alice and Bob, to share a random sequence of bits, such that no adversary, Eve, can get any information about the values of the light sent. Such a key can then be used to encrypt and decrypt data between Alice and Bob in “classical” cryptographic protocols, e.g., the one-time pad encryption. QKD is a key distribution method that relies on the laws of quantum physics, based on which Eve may not gain information about the key without disturbing the system. This feature, which can make her presence exposed to the other parties, is studied under the no-cloning theorem Gisin *et al.* [2002]. QKD requires two kinds of channel: a quantum channel and a classical one. The former is used to send quantum states and the latter to perform classical post-processing, such as error correction and privacy amplification.

Every QKD protocol relies on certain encoding and decoding techniques, which in the case of CV-QKD are often called modulation and demodulation, respectively. Most of CV-QKD protocols use Gaussian modulation to encode and coherent quadrature measurements to decode the information. Gaussian modulation involves choosing quantum states, such as squeezed or coherent states of light, by using Gaussian distributions to be sent over a quantum channel. Early CV-QKD protocols relied on the discrete modulation of Gaussian states Ralph [1999] or the modulation of squeezed states Cerf *et al.* [2001]. Subsequently, the so-called GG02 protocol, which relies on the Gaussian modulation of coherent states and homodyne detection, was proposed by Grosshans & Grangier [2002], and developed by Grosshans *et al.* [2003]. Another CV-QKD scheme that uses coherent states is called no-switching, in which heterodyne detection is used to perform the encoding Weedbrook *et al.* [2004].

In this thesis, we mostly focus on the GG02 protocol (it is schematically sketched in figure 2.7, in chapter 2, where we will communicate more detail). In order to implement GG02, Alice chooses coherent states, using a Gaussian modulation with mean zero and a certain variance, and sends them to Bob through a quantum channel. Then, using homodyne detection, Bob randomly measures one of the quadratures of the received signal. These constitute the quantum phase of the GG02 protocol, which distributes correlated data between Alice and Bob. In the next stage of the protocol, classical post-processing techniques are used by Alice and Bob to reconcile the correlated data and establish a secret key, where the data obtained by measuring both quadratures of light are used for key extraction.

Although the protocol has successfully been implemented in several experiments, its implementation over long distances faces many technological challenges. For example, a few works so far successfully demonstrated long-distance CV-QKD with positive key rates over a channel length of 80-100 km Jouguet *et al.* [2013], Huang *et al.* [2016]. This compares with over 400 and 1200 km for DV-QKD with optical fibre Boaron *et al.* [2018] and satellite-to-ground links Liao *et al.* [2017a], respectively. This limitation in secure distance is mainly caused by, apart from communication loss, the existence of excess noise in the quantum channel and non-ideal reconciliation efficiency. Excess noise can be a result of interacting with the environment and/or loss in the optical channels, which also decreases the signal-to-noise ratio (SNR). A received signal with a low SNR would only reproduce a noisy version of the transmitted signal. In addition, the reconciliation efficiency highly relies on the SNR Jouguet *et al.* [2013]. Low SNR values make reconciliation difficult and reduce its efficiency, which is the Achilles heel of the Gaussian-modulated CV-QKD. One solution to fight back this limitation is to realize a discrete-modulated version of the protocol such as quadrature-phase-shift-keying (QPSK) protocol Leverrier & Grangier [2009].

In order to be able to use CV-QKD over long distances, one may think of QRs and/or satellites. Such scenarios can, in principle, allow for several thousand of kilometres of secure distance Razavi [2018]. But, the loss in a satellite link is typically more than what a CV-QKD system can tolerate, and it is not clear if CV QRs would be possible at realistic values of noise in the system. This thesis is an attempt to address such issues by providing a realistic account of system's performance when CV-QKD is run over CV QRs as well as finding practical regimes of operation when satellite-based CV-QKD is possible.

We will further discuss the mathematical groundwork of CV systems, as well as the Gaussian and non-Gaussian CV-QKD protocols in chapter 2.

1.2 Long-distance continuous-variable quantum key distribution

1.2.1 Quantum amplifiers and repeaters: Overview

In principle, CV-QKD can be implemented by using coherent states of light. However, the channel loss, along with the excess noise in the system, which are the two main impediments that affect the performance of CV-QKD, prevent perfect realization. As we mentioned earlier, both loss and excess noise affect the SNR of the received states. One may think of using QRs to overcome these issues. Several QR proposals have been proposed for both DV and CV quantum communications Briegel *et al.* [1998], Dias & Ralph [2017], Furrer & Munro [2018]. The majority of these protocols are proposed for DV systems, while there is less work towards designing CV QRs and their use in CV-QKD.

The recent probabilistic CV QR scheme proposed by Dias & Ralph [2017] relies on teleportation of CV states and NLAs Ralph & Lund [2009], Caves *et al.* [2012]. This protocol, in principle, can dramatically compensate for the loss in communication channels; hence, allowing to send quantum data over longer distances. Nevertheless, this result may not be valid in the presence of noise in the channels. In addition, NLA operation must be accurately modelled for realistic devices. Note that building an NLA can be a challenging task. For instance, the NLA setup in Ralph & Lund [2009] requires on-demand single photon sources among other circumstances.

Chapter 3 deals with the building block of the CV QR that uses NLAs, in this thesis quantum scissors, as its innermost part. We further discuss the use of a quantum scissor in Gaussian and non-Gaussian modulation CV-QKD protocols in chapters 4 and 5, respectively.

1.2.2 Satellite-based quantum communications: Overview

Similar to classical communication implementations, an alternative to achieve noticeable rates over long distances is to take advantage of satellites. By launching a network of satellites, accompanied by a corresponding number of ground stations, we can overcome large terrestrial losses. In addition, we can avoid large amounts of excess noise since the noisy part of the free-space communication link is limited to roughly the first ten kilometres of the atmosphere.

In the last few years, several satellite-based quantum protocols have been studied both theoretically and experimentally, including quantum teleportation Ren *et al.* [2017] and QKD Bonato *et al.* [2009], Meyer-Scott *et al.* [2011], Nauerth *et al.* [2013], Vallone *et al.* [2015], Bedington *et al.* [2017], Liao *et al.* [2017a,b]. Note that the security proofs for the satellite-equipped QKD protocols are akin to that of ground-based scenarios, though proper adjustments may need to be applied.

We further delve into some scenarios that consider realistic threat models of satellite CV-QKD and review the results obtained for each scenario in chapter 6.

1.3 Scope of this study

Continuous-variable QKD is a promising technique that allows unconditionally secure communication over a certain distance. In practice, it is, however, limited to short distances in comparison to DV-QKD schemes Pirandola *et al.* [2015b]. This work investigates the possibility of merging existing CV-QKD proposals such as GG02 with QRs and satellites, hoping to attain large secret key rates at long distances.

In this thesis, we are aiming to provide a complete and realistic analysis of the CV QR protocol in Dias & Ralph [2017] and explore if they would, in practice, enable long-distance CV-QKD. We will model the system by considering a realistic model of the QS-based NLA setup in Ralph & Lund [2009], where we need to consider a model for sources that inject single photons into the QSs. We believe a device based on quantum dots can be a suitable candidate. We also would include the inevitable excess noise in the telecom channels in our study. Moreover, we estimate the success probability of the NLA setup based on more realistic assumptions. That is needed to evaluate the success probability of the whole CV QR setup. This can eventually pave the way to compare CV QR results with that of DV QR systems and also to make a cost study. Ultimately, whether the QS-based CV-QKD protocol would succeed in boosting secret key rates over long distances is what we investigate in our work. Particularly, we investigate the performance of a specific CV-QKD system, the GG02 protocol, and its non-Gaussian discrete modulation version, using a QS at the receiver.

In the second part of this thesis, we look at realistic threat models in satellite CV-QKD, where we put limitations on eavesdroppers' power. This is expected to result in higher key rates than what can be obtained when unrestricted eavesdropping is assumed. By applying assumptions made on physical channels between the satellite and the eavesdropper and that with the ground station, which can be verified by certain detection systems, such as LIDAR, we study the security of satellite QKD in several settings. Again, we investigate the security proofs of both Gaussian- and discrete-modulated GG02 protocols.

1.4 Main contributions of this thesis

In chapter 3, we derive exact input-output relationship and exact success probability for a QS for input coherent and two-mode squeezed vacuum (TMSV) states. We also investigate the building block of the CV QR, for TMSV input states and thermal-loss channels, followed by a QS. We then extend the above to input thermal states, by means of which we explore the non-Gaussian behaviour of the QS-assisted channel.

In chapter 4, by focusing on the prepare-and-measure (entanglement-based) scheme of our QS-assisted CV-QKD system, we work out its exact mutual information (an upper bound on its Holevo information). We, therefore, lower bound the secret key rate of the QS-assisted CV-QKD system under Gaussian attacks. We show that secret key rate of the QS system beats the no-QS one at certain regimes of operation. Our results drafted in chapter 3 and 4 have been published in IEEE Journal of Selected Topics in Quantum Electronics (DOI: 10.1109/JSTQE.2020.2964395); and made available on the arXiv [arXiv:1808.01617]. They have also been presented in The Seventh Conference on Quantum Cryptography (QCrypt17), Cambridge, UK (2017); International Conference on Quantum, Atomic, Molecular and Plasma Physics (QuAMP17), Glasgow, UK (2017); and CLEO/Europe, Munich, Germany (2017). Also, relevant to this thesis, a part of our results is published in Journal of the Optical Society of America B **35**, 487-499 (2018), which is not presented here.

In chapter 5, we perform a similar study as in chapter 4 on the QPSK protocol, whose receiver unit is equipped with a QS. The results presented in chapter 5 have been published in IEEE Journal on Selected Areas in Communications (DOI: 10.1109/JSAC.2020.2969058); and made available on the arXiv [arXiv:1907.13405].

In chapter 6, we model a satellite-to-ground QKD link, by assuming non-ideal links between (i) Alice and Eve; and (ii) Eve and Bob. By using such a model, we limit Eve's access to Alice and/or Bob stations. Next, based on the above model, we introduce several scenarios that we may need to deal with in a real-world setup. We work out bounds on the secret key rate for the majority of the scenarios, in which we examine both GG02 and QPSK protocols. We show that Alice and Bob can obtain higher key rates as compared to when an unrestricted Eve is assumed. We observe that as Eve's access to the transmitted signal becomes less and less, we approach a classical limit, at which Alice and Bob can exchange secret keys. Our findings drafted in chapter 6 have been presented in The Ninth Conference on Quantum Cryptography (QCrypt19), Montreal, Canada (2019).

1.5 Thesis outline

Chapter 2 of this thesis briefly introduces the basic concepts of CV systems as well as CV-QKD. It gives a sketch of the security proof and the secret key rate of the coherent-state CV-QKD scheme, GG02, as well as its non-Gaussian modulation version. In chapter 3, NLAs are discussed. It also details the QS-based NLA setup. Also, we describe the building blocks of the CV QR in full and provide an exact model. In chapters 4 and 5, we analyse, respectively, the integration of the Gaussian- and discrete-modulated CV-QKD and NLAs. It explains how the NLA techniques can, in principle, increase the distance range of the CV-QKD scheme. In chapter 6, we study CV-QKD protocols in satellite-to-ground links, where, considering several eavesdropping scenarios, realistic threat models are examined. The thesis is summarized in chapter 7, where we also present future work.

Chapter 2

Continuous-variable quantum key distribution

In this chapter, we review the key concepts and techniques in the continuous-variable systems. Here we consider Gaussian systems as they are most relevant to our study. Subsequently, we present a well-known protocol of CV-QKD, which uses coherent states, i.e., the so-called GG02 protocol, as well as its discrete modulation version. For such protocols, we assess the possible use of quantum scissors for long-distance CV-QKD in chapters 4 and 5, and study realistic threat models for satellite CV-QKD in chapter 6.

2.1 Nomenclature for continuous-variable quantum systems

In this section, we define the notation that will be used in this manuscript. A continuous-variable system of M bosonic modes is described by a Hilbert space $\mathbb{H} = \bigotimes_{j=1}^{M} \mathbb{H}_j$, where each $\mathbb{H}_j$ represents an infinite-dimensional single-mode Fock space. Each bosonic mode j is described by a pair of bosonic field operators Glauber [1963], Gerry & Knight [2005], the so-called annihilation and creation operators, denoted, respectively, by $\hat{a}_j$ and $\hat{a}_j^\dagger$, satisfying the following canonical commutation relation

$$[\hat{a}_j, \hat{a}_k^\dagger] = \delta_{jk} \mathbb{1}_\infty, \tag{2.1}$$

where δ_{jk} is the Kronecker delta function. Note that throughout this dissertation we identify the identity operator by the notation, $\mathbb{1}_{\mathsf{d}}$, where d specifies the dimension of the corresponding Hilbert space. The infinite-dimensional single-mode Hilbert space $\mathbb{H}_j$ is spanned by Fock basis $\{|n_j\rangle\}_{n_j=1}^{\infty}$ satisfying

$$\hat{n}_j|n_j\rangle = n_j|n_j\rangle, \tag{2.2}$$

where $\hat{n}_j = \hat{a}_j^\dagger \hat{a}_j$ is the number operator. The action of annihilation and creation operators on the Fock number states are given by

$$\hat{a}_j|n_j\rangle = \sqrt{n_j}|n_j - 1\rangle \quad \text{and} \quad \hat{a}_j^\dagger|n_j\rangle = \sqrt{n_j + 1}|n_j + 1\rangle, \tag{2.3}$$

with $\hat{a}_j|0\rangle = 0$, where $|0\rangle$ is the so-called vacuum state.

Alternatively, an M-mode CV system can be represented by a general vector

$$\hat{A} := (\hat{a}_1, \hat{a}_1^\dagger, \ldots, \hat{a}_M, \hat{a}_M^\dagger)^T, \tag{2.4}$$

where $\hat{A}^T$ is the transpose of the quadrature vector and $[\hat{A}_j, \hat{A}_k^\dagger] = \Omega_{jk}\mathbb{1}_\infty, \quad j, k = 1, \ldots, M$. In above, $\hat{A}_j$ is the ith element of the vector $\hat{A}$, and Ω_{jk} is the element of the jth row and kth column of the so-called symplectic matrix

$$\Omega = \bigoplus_{m=1}^{M} \omega_m, \quad \omega_m = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \forall\, m, \tag{2.5}$$

where $\bigoplus$ is the block-diagonal direct sum over ω_ms.

The quadrature representation is another way to describe CV systems Braunstein & van Loock [2005]. It is based on the position, $\hat{X}_j$, and momentum, $\hat{P}_j$, quadratures of a quantum harmonic oscillator Gerry & Knight [2005]. The quadratures are related to the bosonic field operators as follows

$$\hat{a}_j = \frac{\hat{X}_j + i\hat{P}_j}{2} \quad \text{and} \quad \hat{a}_j^\dagger = \frac{\hat{X}_j - i\hat{P}_j}{2}, \tag{2.6}$$

which implies the quadrature commutation relation $[\hat{X}_j, \hat{P}_k] = 2i\Omega_{jk}\mathbb{1}_\infty$, where we have chosen the reduced Planck constant $\hbar \equiv 2$ (the value is in accord with normalizing vacuum noise to 1, as we will shortly explain). One can also introduce the eigenstates of the quadrature operators $|X_j\rangle$ and $|P_j\rangle$ by $\hat{X}_j|X_j\rangle = X_j|X_j\rangle$

and $\hat{P}_j|P_j\rangle = P_j|P_j\rangle$, where $X_j, P_j \in \mathbb{R}$ are continuous eigenvalues for the position and momentum eigenstates, which are related via the following Fourier transforms

$$|X_j\rangle = \frac{1}{\sqrt{\pi}} \int dP_j e^{iX_jP_j}|P_j\rangle \quad \text{and} \quad |P_j\rangle = \frac{1}{\sqrt{\pi}} \int dX_j e^{-iX_jP_j}|X_j\rangle. \tag{2.7}$$

The integration above is from $-\infty$ to $+\infty$, as will be the case for all integrals hereafter unless stated otherwise. For each optical mode j, the position-momentum pairs (X_j, P_j) can be associated with a Cartesian coordinate system and make the so-called phase space.

Furthermore, the quadrature representation can easily be extended to describe an M-mode CV system. Similar to (2.4), we can define

$$\hat{Q} := (\hat{X}_1, \hat{P}_1, \dots, \hat{X}_M, \hat{P}_M)^T \tag{2.8}$$

having $\hat{Q}|Q\rangle = Q|Q\rangle$, where $|Q\rangle := (|Q_1\rangle, \dots, |Q_{2M}\rangle)^T$, with the commutation relation $[\hat{Q}_j, \hat{Q}_k] = 2i\Omega_{jk}$ holding between each pair of $\hat{Q}$.

We now define two notions that are used to describe CV states. The first, which is called the displacement vector, is the mean value of the quadratures of the CV state $\hat{\rho}$, given by $\bar{Q} = (Q_1, \dots, Q_{2M})$, where

$$Q_j := \mathrm{tr}(\hat{\rho}\hat{Q}_j), \quad j = 1, \dots, 2M, \tag{2.9}$$

and $\hat{Q}_j$ is the jth element of $\hat{Q}$. The second is called the covariance matrix (CM), denoted by V, which is a $2M \times 2M$ real and symmetric matrix defined as

$$V_{jk} \equiv V(\hat{Q}_j, \hat{Q}_k) := \frac{1}{2}\langle \hat{Q}_j\hat{Q}_k + \hat{Q}_k\hat{Q}_j\rangle - \langle \hat{Q}_j\rangle\langle \hat{Q}_k\rangle. \tag{2.10}$$

The mean vector and CM elements are also called the first and second statistical moments of quantum states, respectively. The variance of a single quadrature $\hat{Q}_j$, $V(\hat{Q}_j) \equiv V(\hat{Q}_j, \hat{Q}_j)$, is a diagonal element of the CM, i.e.,

$$V(\hat{Q}_j) = \langle \hat{Q}_j^2\rangle - \langle \hat{Q}_j\rangle^2. \tag{2.11}$$

The symplectic matrix and the CM must satisfy the following relation $V + i\Omega \geq 1$ Simon *et al.* [1994]. From the diagonal elements of such an inequality we can find the typical Heisenberg relation for position and momentum, i.e., $V(\hat{X}_j)V(\hat{P}_j) \geq 1$. We define $A_j = V(\hat{X}_j)V(\hat{P}_j)$ as the *uncertainty area* of a single-mode quantum state. As an example, for the vacuum state we have $V(\hat{X}) = V(\hat{P}) = 1$; hence, the uncertainty area of such a state is $A_0 = 1$. With this result and the fact that its mean value reads $\bar{Q} = (0, 0)$, we can now "visualize" the vacuum state on the position-momentum phase space; see figure 2.1.

In addition, if a real matrix, $\mathcal{E}$, exists such that $\Omega = \mathcal{E}\Omega\mathcal{E}^T$, then for a Gaussian quantum state, corresponding to the CM V, we have

$$V = \mathcal{E}V^{\text{diag}}\mathcal{E}^T, \quad V^{\text{diag}} = \bigoplus_{m=1}^{M} v_m \mathbb{1}_2, \tag{2.12}$$

where v_ms are the *symplectic eigenvalues* of the CM. In fact, for any CM V, there exists a proper symplectic transformation, $\mathcal{E}$, that diagonalizes the CM. It implies that the Gaussian quantum state associated with the CM is decomposed into M thermal states; see section 2.1.2. This fact makes computing Holevo information, as a crucial part in key rate analysis of CV-QKD protocols, manageable as we show in section 2.2.3.

2.1.1 Characteristic functions and quasi-probability distributions

Mathematical objects such as characteristic functions are tools that help us to describe quantum systems. As we will see later, it is convenient to introduce characteristic functions, whereby we can uniquely define an arbitrary quantum state. The most common ones are normally-, symmetric-, and antinormally-ordered characteristic functions, which, for the single-mode state $\hat{\rho}$ are defined, respectively, as follows:

$$\begin{aligned}\chi_N^{\hat{\rho}}(\xi) =&\text{tr}(\hat{\rho}\hat{D}_N(\hat{a}, \xi)),\\ \chi_S^{\hat{\rho}}(\xi) =&\text{tr}(\hat{\rho}\hat{D}(\hat{a}, \xi)),\\ \chi_A^{\hat{\rho}}(\xi) =&\text{tr}(\hat{\rho}\hat{D}_A(\hat{a}, \xi)),\end{aligned} \tag{2.13}$$

where, for $\xi \in \mathbb{C}$, $\hat{D}(\hat{a}, \xi) = e^{\xi\hat{a}^\dagger - \xi^*\hat{a}}$ is the displacement operator Glauber [1963] and $\hat{D}_N(\hat{a}, \xi) = e^{\xi\hat{a}^\dagger}e^{-\xi^*\hat{a}}$ and $\hat{D}_A(\hat{a}, \xi) = e^{-\xi^*\hat{a}}e^{\xi\hat{a}^\dagger}$ are its normally- and antinormally-ordered versions, respectively.

Knowing one of the above functions, one can uniquely find its associated quantum state. For instance, by using the antinormally-ordered characteristic function one can work out the state in the optical mode $\hat{a}$, as follows

$$\hat{\rho} = \int \frac{d^2\xi}{\pi} \chi_A^{\hat{\rho}}(\xi) \hat{D}_N(\hat{a}, \xi), \tag{2.14}$$

where $\int d^2\xi \equiv \int d\xi_{\mathsf{r}} \int d\xi_{\mathsf{i}}$, assuming that $\xi = \xi_{\mathsf{r}} + i\xi_{\mathsf{i}}$ with $\xi_{\mathsf{r}} = \mathrm{Re}(\xi)$ and $\xi_{\mathsf{i}} = \mathrm{Im}(\xi)$ being the real and imaginary parts of the complex number ξ, respectively.

The Fourier transform of the above functions are also ubiquitously used in quantum optics, so that they have their own given names. Perhaps the most well-known of which is the Wigner function, $W_{\hat{\rho}}(\beta)$, defined by using marginal (reduced) position and momentum probability distributions[1] Leonhardt [1997]. Also, one can show that Wigner function is related to the symmetric characteristic function via the following Fourier transform:

$$W_{\hat{\rho}}(\beta) = \int \frac{d^2\xi}{(2\pi)^2} \chi_S^{\hat{\rho}}(\xi) e^{\frac{1}{2}(\beta\xi^* - \beta^*\xi)}, \tag{2.15}$$

where ξ^* is the complex conjugate of ξ. Wigner functions characterize the statistics of the field components X and P in the phase space, and help to *visualize* the quantum state of light Leonhardt [1997]. However, such functions can take negative values and/or become ill-behaved; hence, they represent *quasi*-probability distribution functions.

The other two known quasi-probability distributions are Glauber-Sudarshan $P_{\hat{\rho}}(\beta)$ Glauber [1963], Sudarshan [1963] and Husimi $Q_{\hat{\rho}}(\beta)$ Husimi [1940] distribution functions, which are defined based on normally- and antinormally-ordered characteristic functions, respectively. Note that, similar to Wigner functions, $P_{\hat{\rho}}(\beta)$ and $Q_{\hat{\rho}}(\beta)$ can also become ill-behaved for some optical quantum states, e.g., a single-photon Fock state.

[1] Assuming a Wigner function $W_{\hat{\rho}}(\beta) \equiv W_{\hat{\rho}}(X, P)$, marginal distributions $f_{\mathcal{X}}(X) = \int dP W_{\hat{\rho}}(X, P)$ and $f_{\mathcal{P}}(P) = \int dX W_{\hat{\rho}}(X, P)$ can, respectively, be defined for position and momentum.

Such a formulation in (2.13) and (2.14) can be straightforwardly extended to M-mode systems. For later use in this thesis, we focus on the antinormally-ordered functions. For a joint M-mode state $\hat{\rho}$, the antinormally-ordered characteristic function is given by

$$\chi_A^{\hat{\rho}}(\xi_1, \ldots, \xi_M) = \mathrm{tr}\Big(\hat{\rho} \bigotimes_{j=1}^{M} \hat{D}_A(\hat{a}_j, \xi_j)\Big). \tag{2.16}$$

The density matrix $\hat{\rho}$ and its antinormally-ordered characteristic function are then related via the following Fourier-like transformation relationship:

$$\hat{\rho} = \int \frac{d^2\xi_1}{\pi} \cdots \int \frac{d^2\xi_M}{\pi} \chi_A^{\hat{\rho}}(\xi_1, \ldots, \xi_M) \bigotimes_{j=1}^{M} \hat{D}_N(\hat{a}_j, \xi_j). \tag{2.17}$$

2.1.2 Gaussian states

An optical state is called Gaussian if its Wigner function on the quantum phase space has a Gaussian form Leonhardt [1997], Weedbrook *et al.* [2012]. The vacuum state $|0\rangle$ is a well-known Gaussian state with $W_0(\beta) = \frac{2}{\pi} e^{-|\beta|^2}$. In fact, majority of optical quantum states that are currently available in laboratories are Gaussian. In the following, we will introduce the ubiquitously used Gaussian states in quantum information and communications theory.

We would like to remark that a Gaussian CV state can be completely described by only its first-order (mean value) and second-order (CM) moments. This can be seen by the fact that the Wigner function of Gaussian states can uniquely be written by using only its mean value $\bar{Q}$ and covariance matrix V, as follows:

$$W_{\hat{\rho}}(Q) = \frac{1}{(2\pi)^{2M}\sqrt{\det V}} \exp\{-\frac{1}{2}(Q - \bar{Q})^T V^{-1} (Q - \bar{Q})\}, \tag{2.18}$$

where $Q = (Q_1, \ldots, Q_M)$ and V^{-1} is inverse of the CM.

Hereafter, we will consider only single-mode and two-mode CV systems unless we need to deal with more optical modes.

Figure 2.1: The vacuum state with uncertainty area $A_0 = 1$ is represented at the centre of the phase space. A coherent state $|\alpha\rangle$ is in fact a displaced vacuum state, with uncertainty area $A_\alpha = A_0$.

Coherent states

In a single-mode Hilbert space $\mathbb{H}$, the eigenstates of the annihilation operator $\hat{a}$, denoted by $|\alpha\rangle$s, are defined as coherent states, i.e.,

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle, \tag{2.19}$$

where $\alpha \in \mathbb{C}$. As an important property, one can then find the mean photon number of a coherent state: $\bar{\mathsf{n}} = \mathrm{tr}(|\alpha\rangle\langle\alpha|\hat{n}) = |\alpha|^2$. Also, in the Fock basis, a coherent state is written as the following Gerry & Knight [2005]:

$$|\alpha\rangle = \sum_{n=0}^{\infty} \mathcal{F}_n(\alpha)|n\rangle, \tag{2.20}$$

where $\mathcal{F}_n(\alpha) = \frac{\alpha^n e^{-|\alpha|^2/2}}{\sqrt{n!}}$ is a Poissonian distribution.

A coherent state can also be defined as a result of applying the displacement operator on the vacuum state, i.e., $\hat{D}(\hat{a}, \alpha)|0\rangle = |\alpha\rangle$. We note that for a coherent state the variance of both quadratures are unity and equal to those of the vacuum state. As its name indicates, the displacement operator only shifts a coherent state in the phase space; see figure 2.1.

The set of coherent states is *overcomplete* over $\mathbb{H}$, meaning that

$$\int d^2\alpha|\alpha\rangle\langle\alpha| = \pi\mathbb{1}_\infty; \tag{2.21}$$

therefore, any quantum state $\hat{\rho}$ can be written in the basis of coherent states as follows

$$\hat{\rho} = \int d^2\alpha P_{\hat{\rho}}(\alpha)|\alpha\rangle\langle\alpha|, \tag{2.22}$$

where $P_{\hat{\rho}}(\alpha)$ is the Glauber-Sudarshan P function of $\hat{\rho}$ Walls & Milburn [2008]. For example, one can easily check that for a coherent state $|\beta\rangle$ we have that $P_{|\beta\rangle}(\alpha) = \delta^2(\alpha - \beta)$, where $\delta^2(\xi) = \delta(\xi_{\mathsf{r}})\delta(\xi_{\mathsf{i}})$.

Vacuum state

Vacuum state is perhaps the most important state in quantum physics. It is involved in a fairly large number of physical phenomena, such as spontaneous emission, Lamb shift, and Casimir effect, to name a few. In quantum optics, vacuum state is the only coherent state with zero photons, i.e., $\bar{\mathsf{n}}_{|0\rangle} = 0$. The covariance matrix of the, single-mode, vacuum state reads $V_{|0\rangle} = \mathbb{1}_2$. Also, as earlier mentioned, the vacuum state has the minimum variance in both quadratures, i.e., $V_{|0\rangle}(\hat{X}) = V_{|0\rangle}(\hat{P}) = 1$, the shot noise unit (SNU). We briefly explain how it can be measured in section 2.1.4.

Thermal states

A thermal state (also known as chaotic light) is a quantum state with no phase dependence[1], which in the Fock basis has the form

$$\hat{\rho}_{\mathsf{th}} = \frac{1}{1+\bar{\mathsf{n}}} \sum_{n=0}^{\infty} (\frac{\bar{\mathsf{n}}}{1+\bar{\mathsf{n}}})^n |n\rangle\langle n|, \tag{2.23}$$

where $\bar{\mathsf{n}} = \mathrm{tr}(\hat{\rho}_{\mathsf{th}}\hat{n})$ is the mean photon number of the state. One can also write such a state in the basis of coherent states by using its P function as below:

$$\hat{\rho}_{\mathsf{th}} = \int d^2\alpha \frac{e^{-\frac{|\alpha|^2}{\bar{\mathsf{n}}}}}{\pi\bar{\mathsf{n}}} |\alpha\rangle\langle\alpha|, \tag{2.24}$$

with the same mean photon number as in (2.23). One can show that the uncertainty area for the thermal state is proportional to its mean photon number squared; in fact, $A_{\mathsf{th}} = (1+2\bar{\mathsf{n}})^2$, which is blown up compared to that of coherent states with unity uncertainty area; see figure 2.2(a).

Thermal states are crucial in CV-QKD using coherent stats as these are exactly the states that are provided by the sender when she uses a Gaussian modulation. We will see later how this can be shown from (2.24).

[1] In quantum optics Gerry & Knight [2005], Walls & Milburn [2008], a phase distribution, $\mathcal{P}(\phi)$, can be associated with a density operator, $\hat{\rho}$, such that $\mathcal{P}(\phi) = 1/(2\pi)\langle\phi|\hat{\rho}|\phi\rangle$, where $|\phi\rangle = \sum_{n=0}^{\infty} e^{in\phi}|n\rangle$. For a thermal state we have that $\mathcal{P}(\phi) = 1/(2\pi)$.

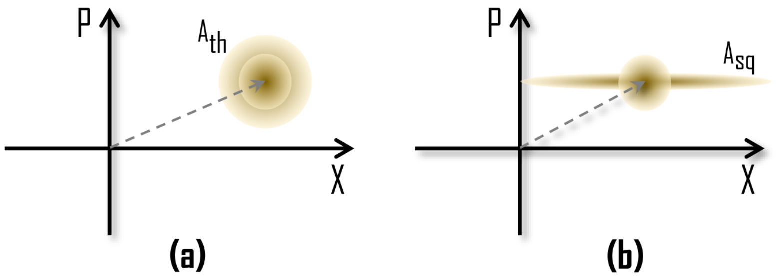

Figure 2.2: **(a)** A thermal state has an uncertainty area $A_{\mathsf{th}} > A_0$. **(b)** A squeezed state can have less variance in one quadrature than the vacuum state, yet $A_{\mathsf{sq}} \geq A_0$.

Single-mode squeezed states

Squeezed states were introduced while quantum physicists where trying to find states with minimum uncertainty Stoler [1970], Caves [1981]. They were eager to answer this fundamental question whether or not it is possible to have quantum states with lower uncertainty values than that of coherent states $A_0 = 1$ (upon simultaneous measurement of both quadratures) Leonhardt [1997]. The answer was no. However, it was shown that while we cannot have a state with an uncertainty area less than A_0, we can indeed attain a state with less uncertainty/noise in only one of the quadratures. In fact, one quadrature can have reduced noise compared to the vacuum while, in consequence, the other quadrature will have increased noise, with the product of both still saturating the lower bound on the Heisenberg uncertainty relation. This means that the uncertainty area is squeezed in one direction, while $A_{\mathsf{sq}} \geq A_0$; see figure 2.2(b). Therefore, A_0 was introduced as the standard quantum limit for noise level.

The way to attain such squeezed states is to apply the single-mode unitary squeezing operator, $\hat{S}_1(r) = e^{\frac{r}{2}(\hat{a}^2 - \hat{a}^{\dagger 2})}$, on quantum states, where $r \geq 0$ is the squeezing parameter. For example, we obtain a squeezed vacuum state by applying the squeezing operator on the vacuum state, i.e., $\hat{S}_1(r)|0\rangle$, where r specifies how squeezed the resultant state is.

Two-mode squeezed states

The single-mode squeezing idea can also be applied to multi-mode quantum states, where an operator can jointly act on more than one mode Caves & Schumaker [1985]. Such an operation involves two or more optical modes that can possibly result in creating correlations between them. This is therefore of particular importance for quantum information and quantum communication applications. We are here particularly interested in the case where two modes A and B, represented, respectively, by $\hat{a}$ and $\hat{b}$, are involved. The associated two-mode squeezing operator is defined as $\hat{S}_2(r) = e^{r(\hat{a}\hat{b}-\hat{a}^\dagger\hat{b}^\dagger)}$ Walls & Milburn [2008]. Of particular interest is when $\hat{S}_2(r)$ is applied to the double vacuum state, $|0\rangle_A|0\rangle_B$. This operation will generate the so-called two-mode squeezed vacuum state (TMSV):

$$\begin{aligned}|\mathrm{TMSV}\rangle :=&\hat{S}_2(r)|0\rangle_A|0\rangle_B\\ =&\sqrt{1-\kappa^2}\sum_{n=0}^{\infty}(-\kappa)^n|n\rangle_A|n\rangle_B,\end{aligned} \tag{2.25}$$

where $\kappa = \tanh(r) \in [0,1]$. Such a TMSV state can experimentally be obtained by pumping a non-linear crystal through the process of parametric down-conversion Villar *et al.* [2005].

Note that this state is a two-mode CV state with two pairs of quadratures for modes $\hat{a} = (\hat{X}_A, \hat{P}_A)$ and $\hat{b} = (\hat{X}_B, \hat{P}_B)$. In fact, assuming $\hat{Q} = (\hat{X}_A, \hat{P}_A, \hat{X}_B, \hat{P}_B)^T$, one can show that a TMSV state is a Gaussian CV state with the mean value zero and the following CM

$$V_{\mathrm{TMSV}} = \begin{pmatrix} V\mathbb{1}_2 & \sqrt{V^2-1}\,\sigma_z \\ \sqrt{V^2-1}\,\sigma_z & V\mathbb{1}_2 \end{pmatrix}, \tag{2.26}$$

where $V = \cosh(2r)$ and $\sigma_z = \mathrm{diag}(1,-1)$.

The existence of quantum correlation between modes A and B is clear in the Fock representation of a TMSV state given in (2.25). The correlation between quadratures of modes A and B can also be revealed by defining the following operators Weedbrook *et al.* [2012]

$$\hat{\mathfrak{x}} := \frac{\hat{X}_A - \hat{X}_B}{\sqrt{2}} \quad \text{and} \quad \hat{\mathfrak{p}} := \frac{\hat{P}_A + \hat{P}_B}{\sqrt{2}}. \tag{2.27}$$

By using (2.11) and (2.26), we can show that the variance of $\hat{\mathpzc{x}}$ and $\hat{\mathpzc{p}}$ obey (note that $[\hat{\mathpzc{x}}, \hat{\mathpzc{p}}] = 0$)

$$V(\hat{\mathpzc{x}}) = V(\hat{\mathpzc{p}}) = e^{-2r}. \tag{2.28}$$

We see that at the limit of infinite squeezing, i.e., $r \to \infty$ (corresponds to $\kappa \to 1$ in (2.25)), we have that $\hat{X}_A = \hat{X}_B$ and $\hat{P}_A = -\hat{P}_B$. These perfect correlations allow to teleport a CV state, such as a coherent state, using a TMSV state Braunstein & Kimble [1998].

It is interesting to remark that by tracing over one mode of a TMSV state (2.25), the other mode collapses to a thermal state in the form of (2.24), with a mean photon number

$$\bar{\mathsf{n}} = \frac{\kappa^2}{1 - \kappa^2}. \tag{2.29}$$

In fact, this is the ground where equivalence between prepare-and-measure (P&M) and entanglement-based (EB) schemes for CV-QKD lays. We will later come back to this fact in section 2.2. In addition, parameters κ and $\bar{\mathsf{n}}$ are linked with that of the CM picture, i.e., V. One can work out that $\kappa = \sqrt{(V-1)/(V+1)}$ and $\bar{\mathsf{n}} = (V-1)/2$.

As we earlier discussed, any quantum state can uniquely be specified by its characteristic functions. Since we build some of our analysis based on these functions, we would like to here represent a TMSV state in the terms of antinormally-ordered characteristic functions. Using (2.17), we can then write a TMSV state in the following form Razavi [2006]:

$$\hat{\rho}_{\text{TMSV}} = \int \frac{d^2\lambda_a}{\pi} \int \frac{d^2\lambda_b}{\pi} \chi_A^{\text{TMSV}}(\lambda_a, \lambda_b) \hat{D}_N(\hat{a}, \lambda_a) \hat{D}_N(\hat{b}, \lambda_b), \tag{2.30}$$

where

$$\chi_A^{\text{TMSV}}(\lambda_a, \lambda_b) = e^{-\delta^2(|\lambda_a|^2 + |\lambda_b|^2) - 2\delta\sqrt{\delta^2 - 1}\,\text{Re}(\lambda_a^* \lambda_b^*)} \tag{2.31}$$

is its antinormally-ordered characteristic function, with $\delta = -\sinh(r) = -(V - 1)/2 = \kappa^2/(\kappa^2 - 1)$.

2.1.3 Continuous-variable modulation

In a P&M CV-QKD protocol, the sender (referred to as Alice) should encode her key bits into quantum states. Coherent states are natural choices for such a purpose as information can be encoded in their amplitude and phase, or, alternatively, in their two quadratures.

There are different ways to choose what coherent states to use for this encoding, or, "modulation" task. In classical optical communications, we often use a finite set of states in the form of a constellation. While this technique is extendable to CV-QKD, and we will consider it in this thesis, CV-QKD started with a rather strange encoding that covers the entire phase space; that is the transmitted signals can be any coherent state. In order to benefit from the optimality of Gaussian distributions when it comes to the channel capacity, Gaussian modulation is extensively used in CV-QKD; see figure 2.3(a). To put is precisely, Alice uses a pair of zero-mean independent Gaussian variables with an equal variance. The variance is considered as a free parameter, which at the end is optimised such that the communication rate is maximum. We remark that a Gaussian-modulated set of coherent states has a well-known physical realization: a thermal state similar to that given in (2.24). Nevertheless, in practice, the Gaussian-modulated assumption we make can be impossible to achieve since we are bounded by the resolution of our devices, and the set of coherent states that can be generated may be discrete. Fortunately, it is shown that this is not practically significant Jouguet *et al.* [2012]. Moreover, an unavoidable laser diode phase noise at Alice can occur during the preparation stage of the protocol. This means that in each run Alice prepares a thermal state instead of a coherent state. However, it is again shown that by precise characterization and calibration, this can even lead to an increased secret key generation rate Jouguet *et al.* [2012].

As was mentioned earlier, there is another, rather broad, class of modulation techniques that can be used in CV-QKD, known as non-Gaussian or discrete modulation; see figure 2.3(b). Such techniques have their own advantages such as offering high error reconciliation efficiencies Leverrier & Grangier [2009, 2011]. In such a modulation, a finite set of coherent sates is considered, from which Alice can choose. For example, a set of four and eight coherent states, with a fixed

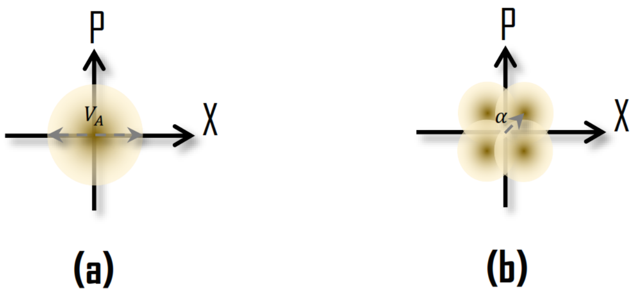

Figure 2.3: **(a)** Gaussian modulation of coherent states makes a thermal state with a certain variance (V_A). **(b)** A discrete, or non-Gaussian, modulation that is made of only four different coherent states. This specific modulation is also called quadrature-phase-shift-keying (QPSK) modulation, whose variance is a function of α.

amplitude are studied in Leverrier & Grangier [2011] and Zhang *et al.* [2018a]. We will consider this class of modulation, which is also known as quadrature-phase-shift-keying (QPSK) modulation, in section 2.3 as well as chapter 5.

2.1.4 Continuous-variable measurements

In any CV-QKD protocol, at some point, we need to perform measurements. In DV-QKD protocols, where we need to measure polarization, photon number, or other discrete degrees of freedom, one can use single photon detectors. However, in order to measure other—continuous—properties of the light, such as its quadratures, one would need a different technique. Such measurement methods are called coherent detection and include homodyne detection and heterodyne detection Leonhardt [1997].

Homodyne detection is applied to measure a specific quadrature, e.g., $\hat{X}_{\mathsf{s}}$ or $\hat{P}_{\mathsf{s}}$, of the signal field $\hat{a}_{\mathsf{s}}$. In order to do so, the signal is combined with a highly stable reference beam, the so-called local oscillator (LO), at a 50:50 beam splitter; see figure 2.4. The local oscillator must be in the matching mode to what $\hat{a}_{\mathsf{s}}$ represents. Alternatively, the local oscillator effectively filters the incoming signal by only measuring the mode that is matched, temporally and spectrally, to itself. Two photodetectors are then used to measure the intensity of light in each of them. It can then be shown that the difference between the

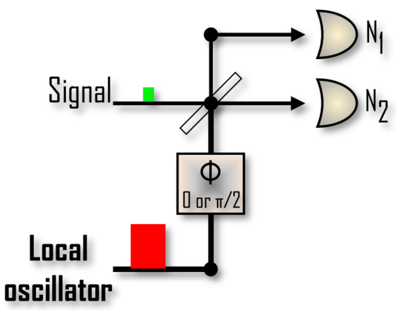

Figure 2.4: Homodyne detection. An on-off phase shifter allows to choose which quadrature to measure.

resulting photocurrents provides us with a value proportional to a measurement on quadrature $\hat{Q}_{\mathsf{s}}(\phi) = e^{i\phi}\hat{a}_{\mathsf{s}}^{\dagger} + e^{-i\phi}\hat{a}_{\mathsf{s}}$, where ϕ is phase of the local oscillator. In above, we assumed a *balanced* homodyne detection, meaning that the beam splitter used in figure 2.4 is 50:50. One can then choose which quadrature, $\hat{X}_{\mathsf{s}}$ or $\hat{P}_{\mathsf{s}}$, to measure by setting the phase ϕ to either 0 or $\pi/2$, respectively. Note that running a homodyne detection can face imperfections in practice; we refer to the recent work by Qin *et al.* [2018].

Also, the fundamental physical phenomenon of minimum amount of uncertainty/noise, which belongs to the vacuum state, can be measured by means of homodyne detection. For that the signal port is blocked and kept clear of any environment photons Kunz-Jacques & Jouguet [2015]. It is worth mentioning that, in the above, a semi-quantum model of homodyne detection is considered, i.e., the local oscillator is assumed to behave as a classical field. A fully quantum picture of coherent detection is studied in Zhou *et al.* [2018], where the local oscillator is modelled with a pure coherent state.

Now let us assume that one aims to simultaneously measure both position and momentum quadratures (or, alternatively, phase and amplitude) of light. Such a coherent detection task can be performed by using heterodyne detection Walker & Carroll [1984]. Heterodyne measurement is basically assembled by means of two homodyne detection modules. To do so, the signal is split to two parts via a 50:50 beam splitter. Then, one homodyne module measures $\hat{X}_{\mathsf{s}}$ and the other measures $\hat{P}_{\mathsf{s}}$ of the optical field $\hat{a}_{\mathsf{s}}$. Using a 50:50 beam splitter, however, adds at least a minimum amount of noise, the vacuum noise coming from the signal-free part of the beam splitter, to the signals. In fact, this is the reason why one cannot measure both quadratures simultaneously without adding extra noise.

It is also interesting to remark that by performing a heterodyne measurement on one part of a TMSV state, the other part collapses to a thermal state, as discussed in section 2.1.2. This is the same state generated by Gaussian modulation. We will use this fact to find correspondence between P&M and EB CV-QKD.

Homodyne efficiency and electronic noise

A realistic homodyne detection module, which includes both optical and electronic equipment, may attenuate the input signal that it is going to measure. We assume that this attenuation happens by a factor η_{D}, which is called efficiency of the homodyne measurement. The measurement module can also add thermal noise to the photoelectric currents. This basically originates from the detection electronics; hence, called electronic noise and denoted by ν_{elec}. In CV-QKD, both η_{D} and ν_{elec} are assumed to be inaccessible to the eavesdropper, and are measured and calibrated by the receiver prior to the quantum communication runs.

We would also like to take this opportunity to mention that in CV-QKD all kinds of noise are reported in SNU, which is the noise associated with the vacuum state. As well, electronic noise expressed in SNU and is typically on the order of 10^{-2} SNU. In Kumar *et al.* [2015] is reported electronic noise values as low as 0.003 SNU.

In addition, for the purposes of CV-QKD, a realistic/noisy homodyne detection can be modelled by using a TMSV state that interferes with an incoming signal at a beam splitter García-Patrón & Cerf [2009].

2.1.5 Quantum communication channels

Quantum communication enables two distant parties to communicate over a quantum channel. Since optical signals are used for encoding data, a bosonic channel is considered for signal transmission. The most important example of such channels are Gaussian quantum channels, which, by definition, preserve Gaussianity of their (Gaussian) inputs. In CV-QKD, it is often assumed that the quantum communication channel between trusted parties, i.e., the sender (Alice) and receiver (Bob), is characterized by a Gaussian channel. The reason is that, for a given set of observation, it is shown that the optimal collective attack by the eavesdropper (Eve) is the one that corresponds to a Gaussian channel García-Patrón & Cerf [2006], Navascués *et al.* [2006]. Therefore, we can assume that, in the worst case scenario, Eve's attack leaves us with a Gaussian channel. Thus, if we assume that the original channel is also Gaussian, Alice and Bob can then assume that their quantum channel is a Gaussian *thermal-loss* channel, which can be modelled by using a beam splitter, with transmissivity T, that couples a thermal state to the input state (which, in the case of coherent-state CV-QKD, is another thermal state).

Figure 2.5 shows a schematic of a thermal-loss channel. We use the fact that the variance of the output state, $\widetilde{V}_B$, is the summation of variances of two input thermal states (V_A and ε) that are coupled using a beam splitter; hence, the following relationship holds:

$$\widetilde{V}_B = TV_A + (1-T)\varepsilon. \tag{2.32}$$

The corresponding variance upon a homodyne measurement is then given by

$$\begin{aligned} V_B =& \widetilde{V}_B + 1 \\ =& T\underbrace{(V_A+1)}_{V} + \underbrace{(1-T)}_{\text{vacuum noise}} + \underbrace{(1-T)\varepsilon}_{T\varepsilon_{\mathsf{tm}}} \\ =& T(V + \chi_{\mathsf{line}}), \end{aligned} \tag{2.33}$$

where $\chi_{\mathsf{line}} = \frac{1-T}{T} + \varepsilon_{\mathsf{tm}}$ is the so-called channel noise and $\varepsilon_{\mathsf{tm}}$ is the *excess* noise, referred to the channel input and expressed in SNU. Channel excess noise corresponds to quantum bit error rate in DV-QKD. It is named excess noise because it is added by the adversaries, beyond the fundamental shot noise and any other kind of noise that trusted parties expect—often called trusted noise. If a homodyne measurement is going to happen at the end of the channel, one can also take into account detection noise and efficiency, which gives: $V_B = \eta_{\mathsf{D}} T(V + \chi_{\mathsf{tot}})$, where $\chi_{\mathsf{tot}} = \chi_{\mathsf{line}} + \frac{\chi_{\mathsf{Hom}}}{T}$, with $\chi_{\mathsf{Hom}} = \frac{1-\eta_{\mathsf{D}}}{\eta_{\mathsf{D}}} + \frac{\nu_{\mathsf{elec}}}{\eta_{\mathsf{D}}}$. The parameters T and $\varepsilon_{\mathsf{tm}}$ that characterize the quantum channel are estimated at the end of the CV-QKD protocol. In our numerical simulations, for a channel with length L, we assume that $T = 10^{-\alpha L/10}$, where α, measured in dB/km, is the channel loss factor.

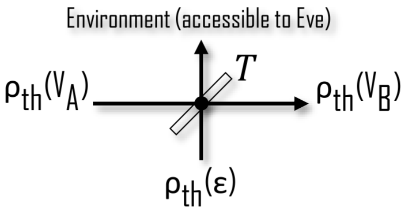

Figure 2.5: Schematic of a thermal-loss channel. It couples a thermal state, with variance ε, with an input state (here another thermal state with variance V_A). The thermal-loss channel reduces to a pure-loss channel for $\varepsilon = 0$.

We would like to also introduce the notion of signal-to-noise ratio (SNR) for a channel. It is basically a measure for comparing the received power to the noise power added during the channel and is defined as the ratio of the signal variance to the added noise variance, often expressed in decibels (dB). Signal-to-noise ratio also quantifies, or more precisely, bounds, the Shannon mutual information between the sender and the receiver. In the case of a loss-less thermal-loss channel, Alice and Bob have, respectively, stored a set of correlated quadratures X_A and $X_B = X_A + X_\mathrm{N}$, where X_N represents (Gaussian) added noise, in registers $\mathcal{X}_A$ and $\mathcal{X}_B$, of a Gaussian channel; see figure 2.6. By following the definition of Shannon mutual information, i.e.,

$$I(\mathcal{X}_A : \mathcal{X}_B) = H(\mathcal{X}_B) - H(\mathcal{X}_B|\mathcal{X}_A), \tag{2.34}$$

one can show that

$$I(\mathcal{X}_A : \mathcal{X}_B) = \frac{1}{2}\log_2(1 + \mathrm{SNR}), \tag{2.35}$$

where $\mathrm{SNR} = \frac{V_A}{V_N}$, with V_A and V_N being the variance of the signal quadrature, X_A, and added noise quadrature, X_N, respectively. In above, it is assumed that the added noise quadrature is independent of the signal one, and that a Gaussian distribution $f_\mathcal{X}(X) = \frac{e^{-\frac{X^2}{V/2}}}{\sqrt{\pi V/2}}$ has a Shannon entropy as $H(\mathcal{X}) = \frac{1}{2}\log_2(\pi e V/2)$ Cover & Thomas [2006].

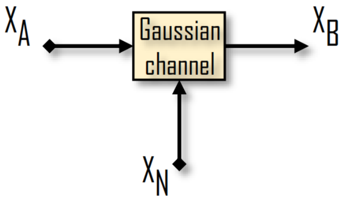

Figure 2.6: Schematic of a Gaussian channel with added noise.

2.2 Continuous-variable QKD using Gaussian modulation of coherent states

Continuous-variable QKD is a technique which enables secret key exchange by modulating and demodulating information in CV states. The final aim of a CV-QKD protocol is for the two legitimate parties to agree on a secret key. Any other party is desired to be unable to learn the key. In fact, if she does, the trusted parties should be able to detect her presence. The first CV-QKD protocols utilized squeezed states of light Ralph [1999], Cerf *et al.* [2001]. Soon after, Grosshans and co-workers introduced a CV-QKD protocol that relied on coherent states Grosshans & Grangier [2002], Grosshans *et al.* [2003]. These protocols mostly use homodyne detection to decode information, where the receiver randomly measures one of the light quadratures. No-switching CV-QKD is another method that uses coherent states, yet the receiver performs heterodyne detection, where both quadratures are measured simultaneously Weedbrook *et al.* [2004]. All the mentioned protocols above are based on the Gaussian modulation in the quadratures $\hat{X}$ and $\hat{P}$.

Continuous-variable QKD protocols can be classified into two categories, called prepare-and-measure (P&M) and entanglement-based (EB) CV-QKD, details of which are discussed in the following.

2.2.1 Prepare-and-measure scheme

A typical CV-QKD protocol using coherent states is sketched in figure 2.7. It runs along the same lines as the protocol first proposed by Grosshans and Grangier in

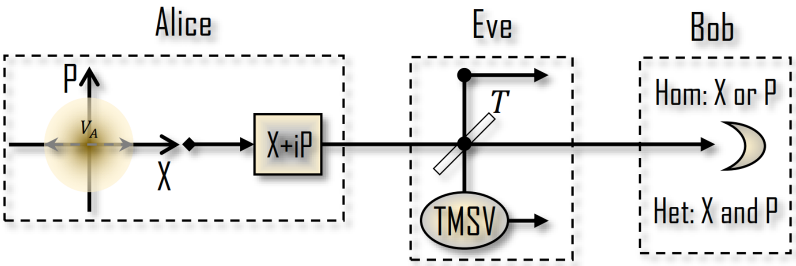

Figure 2.7: Schematic of a P&M CV-QKD protocol with Gaussian modulation (also known as GG02). The GM box prepares Gaussian-modulated coherent states $X+iP$ as inputs to the quantum channel. The states are assumed at Eve's disposal immediately after they leave Alice's realm (this might not be the case in, e.g., a realistic satellite QKD link; see chapter 6). To her benefit, Eve can couple her states to Alice's states. Bob then measures the received signals that might have been transmitted by either Alice, Eve, or both.

2002 (GG02) Grosshans & Grangier [2002]. In GG02, the sender, Alice (A), prepares a coherent state $|\alpha\rangle$, where $\alpha = X_A + iP_A$, with $X_A, P_A \in \mathbb{R}$, is randomly chosen and modulated by a pair of zero-mean independent Gaussian variables $\{\mathcal{X}_A, \mathcal{P}_A\}$, with variance V_A. This variance determines the power that Alice can use in running the system. In order to reach the optimal and asymptotic performance, usually very large power values, i.e., large modulation variance is assumed[1] Grosshans *et al.* [2003].

The prepared modulated coherent state is then sent to the receiver, Bob (B), through a quantum channel, which can be manipulated by a potential eavesdropper, Eve (E). Under the optimal Gaussian attack assumptions, Eve's attack would be to make herself entangled to the transmitted signal, possibly, without being detected. In order to do so, as schematically shown in figure 2.7, she can couple one arm of a TMSV state, generated by Eve with variance Z, with Alice's output signal. This is called entangling quantum cloner Navascués & Acín [2005]. See section 2.2.2 for the details of such a quantum cloner.

[1] Note that the optimal modulation variance is not necessarily infinity. In particular, for a less-than-unity reconciliation efficiency, which we will shortly acquaint with, $V_A \approx 2.5$ optimizes the key rate.

Next, upon receiving a signal, Bob detects the state through either a single quadrature measurement (a homodyne detection, denoted by Hom) or a joint measurement of $\hat{X}$ and $\hat{P}$ (a heterodyne detection, denoted by Het). To put it precisely, in the homodyne measurement, Bob randomly measures one of the quadrature $\hat{X}$ or $\hat{P}$ and subsequently obtains a real outcome X_B or P_B. In a heterodyne protocol, however, Bob simultaneously measures both quadratures, obtaining two real outcomes X_B and P_B. In principle, Bob's outcomes are correlated to the encoded signals X_A or P_A sent by Alice, which might have been manipulated by Eve along the way. We restrict ourselves to only homodyne detection in this dissertation.

Finally, Alice and Bob have shared correlated classical information, i.e., two sets of variables $\{\mathcal{X}_A, \mathcal{X}_B\}$ and/or $\{\mathcal{P}_A, \mathcal{P}_B\}$, which is called a raw key. Their obtained data might have also been jointly correlated to Eve's quantum states Maurer [1993], Navascués & Acín [2005]. In this way, Eve can potentially obtain some information exchanged by Alice and Bob over the quantum channel. Since both quadratures are treated the same, we consider only the X one.

From the correlated data, Alice and Bob can extract a secret key using classical communication over a public channel and applying post-processing techniques. The extraction stage is usually divided into three steps. First, by revealing a random sample of the raw key, Alice and Bob evaluate the characteristics of the quantum channel Jouguet *et al.* [2012]. Based on observed values of channel loss and excess noise, the amount of information that is leaked to Eve can be bounded. Second, the two parties correct the transmission errors via error correction methods. In fact, reconciliation is a technique that allows trusted parties to obtain an identical random string from their correlated data by means of classical communication. We remark that there are two reconciliation strategies: direct and reverse. In direct reconciliation (DR), Alice's key is the main key and Bob tries to correct his raw key to become identical to Alice's. In reverse reconciliation (RR), however, Bob's key is the main key and Alice corrects her key to make it similar to that of Bob. The third step is privacy amplification, through which, Alice and Bob extract a secret key which is unknown to Eve within a failure probability Bennett *et al.* [1995]. In fact, privacy amplification is a technique for obtaining a secret key string from the identical random strings obtained in the reconciliation step.

A physical quantity that can characterize the information shared by Alice and Bob's variables is Shannon mutual information $I(\mathcal{X}_A : \mathcal{X}_B)$ Cover & Thomas [2006]. This quantity can be estimated by Alice and Bob sharing part of their data. One can also bound this quantity, using Gaussian assumptions, once excess noise and channel loss are derived from their observations. Moreover, they would be able to bound the potentially leaked information to Eve when direct or reverse reconciliation is used. In DR, where Eve tries to guess Alice's message, the maximum amount of information Eve can obtain is denoted by χ_{AE}. In the RR case, Eve needs to guess Bob's measurement outcomes. The amount of information that Eve gains in this case is denoted by χ_{BE}. As χ_{AE} and χ_{BE} are the upper bounds on the amount of information obtained by Eve at each case, they are, by definition, named Holevo information Holevo [1973]. Note, however, that the amount of information Alice and Bob can share is the same for both DR and RR. Indeed, it is assumed that Eve has access to all classical channels and that she interacts as much as she wishes with the quantum states, yet being limited by the laws of quantum mechanics.

Therefore, the secret key rate[1], i.e., the accessible secret information, is given by

$$R_{\mathsf{DR}} = \beta I(\mathcal{X}_A : \mathcal{X}_B) - \chi_{AE} \tag{2.36}$$

for direct reconciliation and by

$$R_{\mathsf{RR}} = \beta I(\mathcal{X}_A : \mathcal{X}_B) - \chi_{BE} \tag{2.37}$$

for reverse reconciliation, where $\beta \leq 1$ is the reconciliation efficiency. Note that the term $\beta I(\mathcal{X}_A : \mathcal{X}_B)$ simply quantifies the amount of information Alice and Bob are able to extract.

[1] In physics, usually, *rate* refers to the change of a quantity in a certain amount of *time*. For instance, velocity is the rate of change of position in a time interval. Here, however, by rate we mean a quantity with dimension bits per *pulse* (and not bits per unit of time). Notwithstanding, when multiplied by the *clock rate*, at which a transmitter can generate pulses, the rate would have the dimension of bits per unit of time.

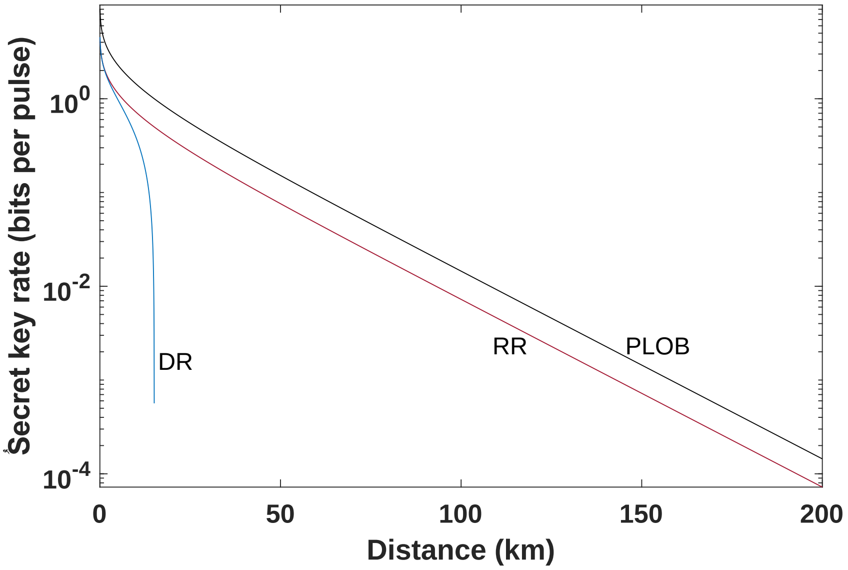

Figure 2.8: Asymptotic secret key rate of CV-QKD protocols using Gaussian modulation of coherent states and homodyne detection over a pure-loss channel. Here we assume $\beta = 1$.

Figure 2.8 shows asymptotic, i.e., when $V_A \to +\infty$, secret key rates versus distance simulated for both direct and reverse reconciliation methods. These are the security bounds against collective Gaussian attacks. Here we assume a pure-loss channel with loss factor $\alpha = 0.2$ dB/km corresponding to optical fibres (homodyne measurement is assumed ideal). For the sake of comparison the ultimate secrete key rate for a repeaterless QKD, the so-called PLOB bound Pirandola *et al.* [2017], is also shown in figure 2.8. As can be seen, the DR rate cannot exceed 15 km, which is known as the 3 dB limit. In contrast, the RR rate, in principle, never vanishes.

In this dissertation, we will focus on and consider mostly the reverse reconciliation. The reason is that at high-loss regimes, where an amplifier can be advantageous, its performance outperforms direct reconciliation, as seen in figure 2.8. In addition, we limit ourselves to only protocols with homodyne detection at the receiver side.

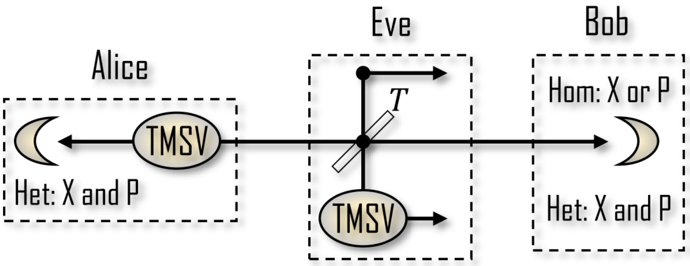

Figure 2.9: Schematic of an EB CV-QKD protocol, equivalent to the setup in figure 2.7.

2.2.2 Entanglement-based scheme

We now turn to the entanglement-based (EB) version of the protocol in figure 2.7, as it is often the scheme that is used in security proofs. This equivalence is at the heart of security proofs for this type of QKD protocols, because theoretical analysis of the EB scheme is more convenient in comparison to the P&M version, though its experimental realization is more difficult.

Therefore, as an alternative, we consider the equivalent EB scheme of figure 2.9, where Alice's source in figure 2.7 is substituted with a TMSV source, characterized by variance V. In the EB version, Alice measures one mode of a TMSV state in (2.26) by heterodyne detection and sends the other mode through a channel to Bob. The origin of the equivalence relies on the fact that, as we discussed in section 2.1.2, heterodyne detection on one mode reduces the other mode of a TMSV state to a bi-Gaussian modulation (thermal) state with a certain variance. Thus, from the point of view of Bob and Eve a Gaussian combination of coherent states, i.e., a thermal state, is leaving Alice's box.

Entangling quantum cloner

In the security proofs for QKD protocols, one typically considers a purification of Eve's state, $\hat{\rho}_E$, with that of Alice and Bob, $\hat{\rho}_{AB}$. It means that their global tripartite state can be represented as a pure state, $|\Psi\rangle_{ABE}$, such that $\hat{\rho}_{AB} = \mathrm{tr}_E(|\Psi\rangle_{ABE}\langle\Psi|)$. Upon such a purification, optimality of Gaussian attacks is proven García-Patrón & Cerf [2006], Navascués *et al.* [2006], where Eve's information was shown maximized for Gaussian attacks. Therefore, by having only

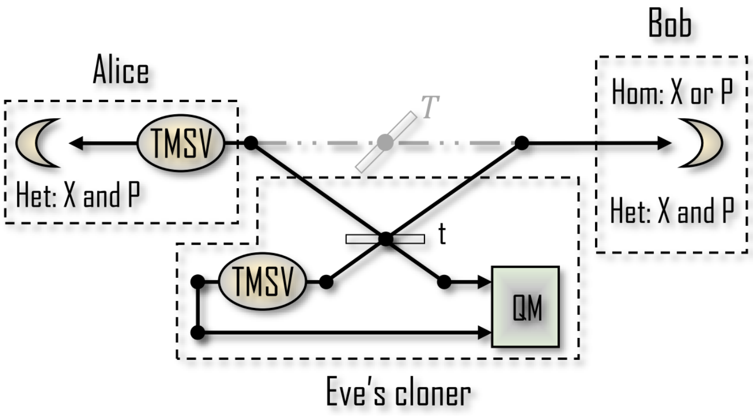

Figure 2.10: Schematic of an EB CV-QKD protocol, equivalent to the setup in figure 2.7. The QM box represents Eve's quantum memories.

first and second momenta of the involved quadratures, Alice and Bob can then the amount of information that can potentially leak to Eve.

A Gaussian attack as such can be realized by Eve using an entangling quantum cloner Navascués & Acín [2005], which perfectly simulates a thermal-loss channel; see figure 2.10. This device combines Alice's output with one mode of a TMSV state, with variance Z, by using a beam splitter with transmissivity t. She then stores one output, along with the other mode of her TMSV state, in her quantum memories, while allowing Bob to have the other (with exactly the same statistics as the Alice-Bob channel) through a lossless channel to Bob. It is shown that Eve can simulate the channel by simply placing $t = 1 - T$ and $Z = 1 + T\varepsilon_{\mathsf{tm}}/(1-T)$, where T and $\varepsilon_{\mathsf{tm}}$ are, respectively, the observer parameters for channel transmissivity and input excess noise.

2.2.3 Secret key rate analysis

Based on limitations imposed on Eve, one can come up with different secret key rate analyses. Such limitations, in fact, define the type of attacks that an eavesdropper can manage to perform. Based on Eve's interaction with the signals, three types of attacks are defined: individual Grosshans & Cerf [2004], Grosshans *et al.* [2003], collective García-Patrón & Cerf [2006], Navascués *et al.*

[2006], and coherent Renner & Cirac [2009] attacks (we provide another classification on eavesdropper limitations in the context of satellite QKD; see chapter 6). In an individual attack, Eve overlaps each transmitted signal with an ancillary state and, subsequently, measures each output ancilla system. In a delayed-choice strategy, Eve may prefer to postpone her individual measurements, so as to optimizes over Alice and Bob's classical communication. In a collective attack, Eve stores output of each ancillary system in a quantum memory but she waits until Alice and Bob's classical communication is finished. She then performs a collective measurement on her memory registers. In a general/coherent attack, it is assumed that the signal and ancilla systems undergo a joint unitary process. Eve then stores the ancillary output in her quantum memories. We here review the security proofs against collective attacks, which we will use in this dissertation. Note that, in the asymptotic scenario, coherent attacks were shown to not be necessarily more powerful than collective attacks Kraus *et al.* [2005], Renner & Cirac [2009]. We also assume that Eve does not have access to Bob's apparatus and that Alice and Bob use reverse reconciliation.

The security proof against collective attacks is based on the EB scheme of GG02, shown in figure 2.10. Based on this model, the final secret key that Alice and Bob can extract is given by (2.37). It is assumed that the part of the signals that are not received by Bob is available to Eve. In the case of reverse reconciliation, in order to estimate the secret key rate against collective attacks, we need to evaluate Eve's accessible information bounded by the Holevo information χ_{BE} Holevo [1973], which, as we discuss in the following, can be computed using channel purification and optimality of Gaussian attacks. We, therefore, can achieve a lower bound on the secret key rate given in (2.37).

The Holevo quantity between Bob's variable and Eve's quantum memories is expressed through the von Neumann entropies, defined as $H_{\text{vN}}(\hat{\rho}) := \text{tr}(-\hat{\rho}\log_2 \hat{\rho})$ Nielsen & Chuang [2000], as follows:

$$\chi_{BE} = H_{\text{vN}}(\hat{\rho}_E) - H_{\text{vN}}(\hat{\rho}_{E|B}), \tag{2.38}$$

where $\hat{\rho}_E$ is the density matrix of Eve's state and

$$H_{\text{vN}}(\hat{\rho}_{E|B}) = \int dX_B p(X_B) H_{\text{vN}}(\hat{\rho}_E^{X_B}), \tag{2.39}$$

with $p(X_B)$ being the probability distribution of Bob's homodyne outcome X_B and $\hat{\rho}_E^{X_B}$ is the state of Eve's system conditional on X_B. As stated in section 2.2.2, the best Eve can do is to purify the global state between herself, Alice, and Bob. Such a purification of the system implies that $H_{\text{vN}}(|\Psi_{ABE}\rangle) = 0$, which, following the Araki-Lieb triangle inequality Araki & Lieb [1970], directly asserts that $H_{\text{vN}}(\hat{\rho}_E) = H_{\text{vN}}(\hat{\rho}_{AB})$. Similarly, when Bob (Alice) performs a projective measurement on the respective sub-state $\hat{\rho}_B$ ($\hat{\rho}_A$), the state of the system $\hat{\rho}_{AE}$ ($\hat{\rho}_{BE}$) is pure[1], which follows that $H_{\text{vN}}(\hat{\rho}_{E|B}) = H_{\text{vN}}(\hat{\rho}_{A|B})$ ($H_{\text{vN}}(\hat{\rho}_{E|A}) = H_{\text{vN}}(\hat{\rho}_{B|A})$). This allows us to calculate the Holevo bound from the entropic aspects of the state shared between Alice and Bob García-Patrón & Cerf [2006], Navascués *et al.* [2006]:

$$\chi_{BE} = H_{\text{vN}}(\hat{\rho}_{AB}) - H_{\text{vN}}(\hat{\rho}_{A|B}). \tag{2.40}$$

This is practically important, compared to the expression in (2.39), since Alice and Bob can now estimate the amount of leaked information to Eve by processing their own data statistics. The entropy $H_{\text{vN}}(\hat{\rho}_{AB})$ is calculated from the symplectic eigenvalues, Λ_js, of the shared CM between Alice and Bob, $V_{AB} = \begin{pmatrix} \sigma_A & \sigma_{AB} \\ \sigma_{AB}^T & \sigma_B \end{pmatrix}$ (see section 2.1):

$$H_{\text{vN}}(\hat{\rho}_{AB}) = \sum_j g(\Lambda_j), \tag{2.41}$$

where $g(x) = (\frac{x+1}{2}) \log_2(\frac{x+1}{2}) - (\frac{x-1}{2}) \log_2(\frac{x-1}{2})$. Note that we assume that the channel is Gaussian; thus, the bipartite state between Alice and Bob is described only by its first and second order moments. Even if the actual channel is non-Gaussian, optimality of Gaussian attacks allows us to upper bound Holevo information.

It turns out that the symplectic eigenvalues are the roots of the following equation: $\Lambda^4 - \Delta\Lambda^2 - \det V_{AB} = 0$, where $\Delta = \det \sigma_A + \det \sigma_B + 2 \det \sigma_{AB}$. Also, the term $H_{\text{vN}}(\hat{\rho}_{A|B})$ can be obtained from the eigenvalue of the conditional CM of Alice's mode conditioned on the Bob's homodyne measurement, i.e.,

$$V_{A|B} = \sigma_A - \sigma_{AB}(\Pi_{\mathsf{X}}\sigma_B\Pi_{\mathsf{X}})^{\text{MP}}\sigma_{AB}^T, \tag{2.42}$$

[1] The conditional states remain pure because we assume a projective measurement is performed on the tripartite—pure—state.

where $\Pi_{\mathsf{X}} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and S^{MP} is the Moore-Penrose pseudo-inverse of the singular matrix S. Based on this description, when the effect of imperfect homodyne detection is also considered García-Patrón & Cerf [2009], it is shown that for a link shown in figure 2.9 we have: $\sigma_A = V\mathbb{1}_2$, $\sigma_{AB} = \sqrt{\eta_{\mathsf{D}} T(V^2-1)}\,\sigma_{\mathsf{z}}$, and $\sigma_B = T(V+\chi_{\mathsf{tot}})\mathbb{1}_2$, where $\chi_{\mathsf{tot}} = \chi_{\mathsf{line}} + \frac{\chi_{\mathsf{Hom}}}{T}$, with $\chi_{\mathsf{line}} = \frac{1-T}{T} + \varepsilon_{\mathsf{tm}}$ and $\chi_{\mathsf{Hom}} = \frac{1-\eta_{\mathsf{D}}}{\eta_{\mathsf{D}}} + \frac{\nu_{\mathsf{elec}}}{\eta_{\mathsf{D}}}$. The Holevo bound then reads:

$$\chi_{BE} = g(\Lambda_1) + g(\Lambda_2) - g(\Lambda_3) - g(\Lambda_4), \tag{2.43}$$

where

$$\Lambda_{1/2} = \sqrt{\frac{1}{2}\left(A \pm \sqrt{A^2 - 4B^2}\right)} \quad \text{and} \quad \Lambda_{3/4} = \sqrt{\frac{1}{2}\left(C \pm \sqrt{C^2 - 4D}\right)}, \tag{2.44}$$

with

$$\begin{cases} A = V^2(1-2T) + 2T + T^2(V+\chi_{\mathsf{line}})^2 \\ B = T(1+V\chi_{\mathsf{line}}) \\ C = \frac{VB + T(V+\chi_{\mathsf{line}}) + A\chi_{\mathsf{Hom}}}{T(V+\chi_{\mathsf{tot}})} \\ D = \frac{B(V+B\chi_{\mathsf{Hom}})}{T(V+\chi_{\mathsf{tot}})}. \end{cases} \tag{2.45}$$

In addition, the mutual information between Alice's and Bob's quadratures for the protocol is given as a function of total noise and input variance:

$$I(\mathcal{X}_A : \mathcal{X}_B) = \frac{1}{2}\log_2\left(\frac{V+\chi_{\mathsf{tot}}}{1+\chi_{\mathsf{tot}}}\right). \tag{2.46}$$

2.3 Continuous-variable QKD using discrete modulation of coherent states

As discussed in section 2.1.3, Alice and Bob can use a finite number of coherent states. Such a decision relies on the poor error reconciliation efficiency for the Gaussian modulation compared to that of a discrete modulation Leverrier & Grangier [2011]. We review here the well-known protocol of this type, which was first studied by Leverrier & Grangier [2009]. All steps of this protocol are the same as GG02 except for the modulation part, where a quadrature-phase-shift-keying (QPSK) modulation is used.

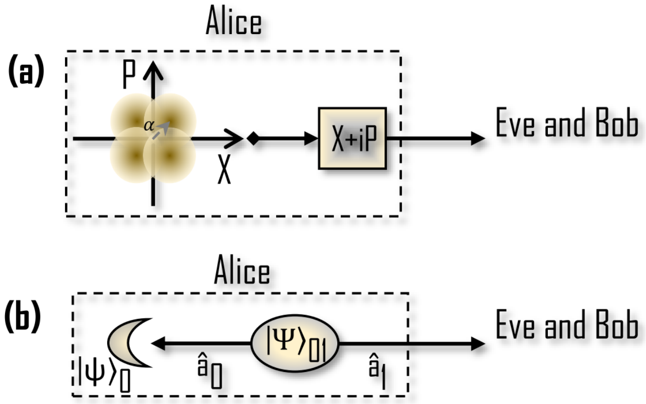

Figure 2.11: CV-QKD with discrete modulation. **(a)** P&M and **(b)** EB schemes.

More precisely, the P&M scheme of the protocol runs as follows. First, Alice randomly chooses a coherent state from the finite set $\{|\alpha_k\rangle = |\dot{\alpha} e^{(2k+1)i\pi/4}\rangle\}_{k=0}^{3}$, with $\dot{\alpha} \in \mathbb{R}^+$, and sends it to Bob through a quantum channel; see figure 2.11(a). Such a constellation can be generated by the rotation of a coherent state in position-momentum phase space. The parameter $\dot{\alpha}$ can be optimized to give the maximum secret key rate. The prepared quantum state from the viewpoint of Bob and Eve is:

$$\hat{\rho} = \frac{1}{4} \sum_{k=0}^{3} |\alpha_k\rangle\langle\alpha_k|. \tag{2.47}$$

In addition, we assume $\alpha_k = (X_{Ak} + iP_{Ak})/2, k = 0, \ldots, 3$, with parameters $X_{Ak}, P_{Ak} \in \mathbb{R}$ being chosen randomly according to the following uniform probability mass functions: $f_{X_A}(X_{Ak}) = f_{P_A}(P_{Ak}) = 1/4$. At the receiver, Bob randomly measures one quadrature, $\hat{X}_B = \hat{a}_B^\dagger + \hat{a}_B$ or $\hat{P}_B = i(\hat{a}_B^\dagger - \hat{a}_B)$, using homodyne detection.

Here again, in order to establish a security proof of the protocol, one can switch to the equivalent EB version shown in figure 2.11(b). In this picture, Alice would provide and send to Bob one leg of the following bipartite state Leverrier

& Grangier [2011]:

$$
\begin{aligned}
|\Psi\rangle_{01} =& \sum_{k=0}^{3} \sqrt{\lambda_k}\, |\phi_k\rangle_0 |\phi_k\rangle_1 \\
=& \frac{1}{2} \sum_{k=0}^{3} |\psi_k\rangle_0 |\alpha_k\rangle_1,
\end{aligned} \tag{2.48}
$$

where

$$
|\phi_k\rangle_j = \frac{-\frac{\dot{\alpha}^2}{2}}{\sqrt{\lambda_k}} \sum_{n=0}^{\infty} (-1)^n \frac{\dot{\alpha}^{4n+k}}{\sqrt{(4n+k)!}} |4n+k\rangle_j, \quad j = 0, 1,
$$

and

$$
|\psi_k\rangle_0 = \frac{1}{2} \sum_{m=0}^{3} e^{(2k+1)im\pi/4} |\phi_m\rangle_0
$$

are orthogonal non-Gaussian states, with

$$
\begin{aligned}
\lambda_{0,2} =& \frac{e^{-\dot{\alpha}^2/2}}{2} \Big(\cosh\big(\dot{\alpha}^2\big) \pm \cos\big(\dot{\alpha}^2\big) \Big), \\
\lambda_{1,3} =& \frac{e^{-\dot{\alpha}^2/2}}{2} \Big(\sinh\big(\dot{\alpha}^2\big) \pm \sin\big(\dot{\alpha}^2\big) \Big).
\end{aligned} \tag{2.49}
$$

The subscripts 0 and 1 refer to the optical modes represented by $\hat{a}_0$ and $\hat{a}_1$, respectively. In the end, the equivalence of P&M and EB schemes of the protocols is obtained via a proper projective measurement in $\{|\psi_k\rangle_0\}$, $k = 0, \ldots, 3$, basis. Note that upon Alice's projective measurement on the orthogonal states $\{|\psi_k\rangle_0\}_{k=0}^{3}$, the bipartite state collapses to the thermal-like state in (2.47).

2.3.1 Secret key rate analysis

The security analysis of discrete-modulation CV-QKD has turned out to be more challenging than its Gaussian counterpart. The reported analysis in Leverrier & Grangier [2009] relies on the linearity of the channel for its security. But, the authors admit that this is not an easy condition to verify. In order to rectify this problem, in Leverrier & Grangier [2011], they come up with a modified scheme in which they can relax the assumption on the channel linearity by requiring Alice to send three types of signals: Gaussian modulated ones for channel estimation, discrete-modulation ones for key generation, and a range of decoy states to conceal the discrepancy between the latter two in the eyes of an eavesdropper. The decoy states would, effectively, make the modulated signals to look Gaussian, which makes the security analysis more manageable. This approach, however, to a large extent, takes away the practical aspects of discrete-modulation CV-QKD. Very recently, new analyses have emerged, which rely on numerical optimization of the key rate based on certain constraints obtained from the measurement results Ghorai *et al.* [2019], Lin *et al.* [2019]. In this dissertation, we focus only on the key generation part, which results from the state in (2.48), and do not consider the parameter estimation task, for which we should either send Gaussian modulated states Leverrier & Grangier [2011], or use numerical techniques Ghorai *et al.* [2019].

Security of the QPSK protocol against collective attacks has been proven by Leverrier & Grangier [2011], where the relevant CM of the protocol was found as follows:

$$V_{AB} = \begin{pmatrix} V_{\dot{\alpha}} \mathbb{1}_2 & \sqrt{T} Z_4 \sigma_{\mathsf{z}} \\ \sqrt{T} Z_4 \sigma_{\mathsf{z}} & T(V_{\dot{\alpha}} + \chi_{\mathsf{tot}}) \mathbb{1}_2 \end{pmatrix}, \tag{2.50}$$

where $V_{\dot{\alpha}} = V_A(\dot{\alpha}) + 1$, with $V_A(\dot{\alpha}) = 2\dot{\alpha}^2$ being the variance of the prepared state in (2.47). The parameter

$$Z_4 = 2\dot{\alpha}^2 \sum_{k=0}^{3} \frac{\lambda_{k-1}^{3/2}}{\lambda_k^{1/2}} \tag{2.51}$$

characterizes the amount of correlation of the bipartite state in (2.48) and can be compared to that of a TMSV state with the same variance, $Z_{\mathrm{G}} = \sqrt{V_{\dot{\alpha}}^2 - 1}$, where 'G' stands for Gaussian as opposed to the non-Gaussian case (Z_4). We have that $Z_4 < Z_{\mathrm{G}}$, but their difference is negligible for small values of $\dot{\alpha}$. As discussed in Leverrier & Grangier [2011], this difference can be interpreted in terms of excess noise so that $\varepsilon_{\mathsf{tm}}^{Z_4} = z\varepsilon_{\mathsf{tm}} + (z-1)V_A$, where $z = (Z_4/Z_{\mathrm{G}})^2$. Note that the difference of the excess noise is very small for small values of $\dot{\alpha}$ (note also that values as small as $\dot{\alpha} \approx 0.3$ maximizes the key rate of the QPSK protocol).

We can then numerically compute the secret key rate of the QPSK protocol using the set of equations (2.43)-(2.46), and performing an optimization over input intensity, $\dot{\alpha}^2$.

2.4 Summary

In this chapter, the basic physics of CV quantum systems as well as a CV-QKD protocol, GG02, were presented, and its secret key rate was discussed. Notwithstanding the significant improvements in CV-QKD during the last two decades Jouguet *et al.* [2013], the realization of CV-QKD over long distances is still challenging due to optical loss and environmental noise in free-space and optical fibres. As the loss scales exponentially with the length of the fibre, over a rather long distance it makes the input signal too weak that its information content cannot be recovered at the receiver in the presence of noise. Therefore, one should make use of CV quantum repeaters Dias & Ralph [2017] and/or establish satellite-based QKD protocols Bonato *et al.* [2009] to overcome this limitation, thereby improving the performance of CV-QKD over long distances. As we will later discuss in chapter 3, a CV quantum repeater uses noiseless linear amplifiers (NLAs) in their design. We will also see that one prominent implementation of such NLAs has quantum scissors (QSs) as its inmost essential component. In fact, QSs are "tiny NLA" devices that can amplify input signals very nearly, but not perfectly, noiselessly. Hence, we investigate QSs, upon which we study the building block of such CV quantum repeater in chapters 4 and 5 and see that under what conditions they would enhance the performance of Gaussian- and discrete-modulated CV-QKD protocols over noisy channels and at long distances. In addition, in chapter 6, by assuming realistic restrictions on Eve's power, we evaluate the security of several real-world threat models for satellite-based CV-QKD.

Chapter 3

Quantum scissors, quantum amplifiers, and quantum repeaters

In this chapter, we review the physics of signal amplification, in general, and noiseless linear amplification, in particular. We will also review and analyse quantum scissors (QSs) as well as the noiseless linear amplifier (NLA) that is built based on them. Moreover, we represent CV quantum repeaters (CV QRs) that can be built by using NLAs.

Our main contributions in this chapter

- We derive exact input-output relationship for a QS as well as probability of success for input coherent and two-mode squeezed vacuum (TMSV) states.
- We analyse, in detail, the building block of a CV QR, for TMSV input states and thermal-loss channels, followed by a QS.
- We extend the above to input thermal states, for which we calculate the output distribution function and show how far it can get from Gaussian distributions.

3.1 Linear quantum amplification

Optical amplifiers, or simply amplifiers, are well known in the context of classical optical communications. They allow to increase the amplitude of an input signal, $|\mathsf{Amp}|_{\text{in}}$. The amplitude value of the output of an amplifier, $|\mathsf{Amp}|_{\text{out}}$, is hence boosted by a real factor $g > 1$ defined as:

$$g := \frac{|\mathsf{Amp}|_{\text{out}}}{|\mathsf{Amp}|_{\text{in}}}, \tag{3.1}$$

which is called amplifier's gain. Alternatively, one may define $G = g^2$ to be the power gain of an amplifier. Amplifiers inevitably add noise to the signals that they amplify. However, in classical communications, the amount of the added noise may not be as important as in quantum systems. There are fundamental restrictions in amplifying quantum states of light. In this regard, we follow Caves and colleagues Caves [1982], Caves *et al.* [2012], Pandey *et al.* [2013], in order to classify quantum amplifiers.

The so-called canonical quantum amplifier, i.e., the one that obeys the canonical commutation relation in $[\hat{a}, \hat{a}^\dagger] = \mathbb{1}_\infty$, is called a phase-preserving linear amplifier. Its objective is to take an input bosonic mode, represented by $\hat{a}_{\text{in}}$, and amplify it to an output field, represented by $\hat{a}_{\text{out}}$, while leaving the phase intact; in fact, $\langle \hat{a}^\dagger_{\text{out}} \rangle = g \langle \hat{a}^\dagger_{\text{in}} \rangle$ is desired. Nevertheless, a *perfect linear amplifier* would perform this task while preserving the signal to noise ratio. One may think that, in the Heisenberg picture, the creation operator of the primary mode (and not just its expectation value) should follow $\hat{a}^\dagger_{\text{out}} = g \hat{a}^\dagger_{\text{in}}$. However, this does not respect commutation relation, for $[\hat{a}_{\text{out}}, \hat{a}^\dagger_{\text{out}}] = g^2 \mathbb{1}_\infty \neq \mathbb{1}_\infty$. Therefore, in order to resolve this problem, we may add the noise operator $\hat{J}$ to the output field operator, such that:

$$\hat{a}^\dagger_{\text{out}} = g \hat{a}^\dagger_{\text{in}} + \hat{J}, \tag{3.2}$$

which results in the following total output noise, normalized by g^2,

$$\frac{\mathsf{V}_{\text{out}}}{g^2} = \mathsf{V}_{\text{in}} + \frac{\mathsf{V}_J}{g^2} := \mathsf{V}_{\text{in}} + \mathsf{V}_{\text{add}}, \tag{3.3}$$

where V is the variance of the quadratures of its corresponding optical mode. If the amplifier is to respect commutation relation $[\hat{a}_{\text{out}}, \hat{a}^{\dagger}_{\text{out}}] = \mathbb{1}_{\infty}$, (3.2) would imply that $[\hat{J}, \hat{J}^{\dagger}] = (g^2 - 1)\mathbb{1}_{\infty}$; hence, an uncertainty principle for operator $\hat{J}$ asserts $\mathsf{V}_{\text{add}} \geq 1 - \frac{1}{g^2}$. Also, if we prefer to deal with an added-noise number that has the gain dependence removed, we consider $\mathsf{V}_{\text{add}}/(1 - \frac{1}{g^2}) \geq 1$. Thus, the minimum added noise, in excess of the input noise, is unity: the shot-noise unit.

It is discussed by Combes *et al.* [2016] that any phase-preserving amplifier on the input state $\hat{\rho}_A$ can be modelled via a device, whose input includes a state $\hat{\rho}_A$ and an ancillary state $\hat{\pi}_B$. Output of such a device, represented by quantum map $\mathcal{E}$, is shown to be $\mathcal{E}(s)\hat{\rho}_A \otimes \hat{\pi}_B \mathcal{E}^{\dagger}(s)$, with output amplified state $\text{tr}_B(\mathcal{E}(s)\hat{\rho}_A \otimes \hat{\pi}_B \mathcal{E}^{\dagger}(s))$. The amplification gain of the amplifier is quantified by the parameter s: $g = \cosh(s)$. In addition, the amount of output noise is computed:

$$\frac{\mathsf{V}_{\text{out}}}{g^2} = \mathsf{V}_{\text{in}} + \mu^2(1 - \frac{1}{g^2}), \tag{3.4}$$

where μ is the parameter that characterizes the ancilla state $\hat{\pi}_B$. In fact, it turns out that $\hat{\pi}_B$ is a thermal state with mean photon number $\bar{\mathsf{n}} = \mu^2 - 1$. By removing the gain dependence, we have $\mathsf{V}_{\text{add}}/(1 - \frac{1}{g^2}) \geq \mu^2$.

One can then classify phase-preserving amplifiers in four types, which correspond to various values of μ^2: (i) non-ideal linear amplifier, which is physical and corresponds to $\mu^2 > 1$; (ii) ideal linear amplifier, which is physical and corresponds to $\mu^2 = 1$; (iii) perfect linear amplifier, which is unphysical and corresponds to $\mu^2 = 1/2$; and (iv) immaculate linear amplifier, which is unphysical and corresponds to $\mu^2 = 0$. Note that a non-deterministic NLA may add no noise to input signals. We also remark that unphysicality is associated to the ancillary states $\hat{\pi}_B$ with negative mean photon numbers $\bar{\mathsf{n}} = \mu^2 - 1$. It means that such an amplification cannot be performed deterministically.

When $\mu^2 < 1$, it turns out that these devices work effectively only over a restricted region of phase space and with some less-than-unity success probability Menzies & Croke [2009]. In fact, the quantum limits for μ^2 devices are not characterized by the amount of added noise, but rather by three properties of the system Pandey *et al.* [2013]:

a) the operating region of phase space over which the amplifier can effectively amplify input states;

b) the fidelity to target coherent states; and

c) the success probability.

If the input region is taken to be the entire phase plane and the fidelity to the target state is one, i.e., an immaculate amplifier that works on the entire phase plane, the probability that such a device works is strictly zero Menzies & Croke [2009], Pandey *et al.* [2013]. Even should one restrict the input coherent states to a circle in phase space centred at the origin, while we demand unity fidelity to the amplified target state, one can show that the success probability is zero. For instance, for the optimal model of an NLA, when the input coherent states are restricted to the disk of complex amplitudes $|\alpha| < \sqrt{\bar{\mathsf{n}}_{\mathsf{c}}}/g$, where $\bar{\mathsf{n}}_{\mathsf{c}}$ is a cutoff, the fidelity of the amplifier output to $|g\alpha\rangle$ is unity, but the success probability scales as $P_{\mathsf{succ}}(\alpha, \bar{\mathsf{n}}_{\mathsf{c}}) \propto \frac{e^{-|\alpha|^2}}{g^{2\bar{\mathsf{n}}_{\mathsf{c}}}}$.

There are only a handful of realistic proposals to implement an NLA Ralph & Lund [2009], Barbieri *et al.* [2011], Eleftheriadou *et al.* [2013]. One important class of NLAs is proposed by Ralph & Lund [2009], whose operation is based on optical state truncation by using single-photon inputs Pegg *et al.* [1998] (the two-photon version of such an NLA is studied by Jeffers [2010]). Such truncation devices are widely known as quantum scissors (QSs) in the literature. The Ralph and Lund NLA (RL-NLA) is classified as an immaculate quantum amplifier Pandey *et al.* [2013]; it non-deterministically does noiseless linear amplification. Below, we will briefly review the structure of the RL-NLA.

3.2 Quantum-scissor based NLA

Ralph & Lund [2009] proposed a setup, shown in figure 3.1(a), to implement an NLA, which relies on the QS module in figure 3.1(b). An N-splitter (NS) first splits the input coherent state $|\beta\rangle$ into N weak coherent states $|\alpha\rangle$, where $\alpha = \beta/\sqrt{N}$. Next, each $|\alpha\rangle$ is individually amplified using a QS. At the core of a QS, there is a partial Bell-state measurement module, with a balanced beam splitter followed by two single-photon detectors, in the space spanned by number states $|0\rangle$ and $|1\rangle$. This Bell-state measurement module is driven by an asymmetric Bell state $|\psi\rangle = \sqrt{\mu}|1\rangle_{\hat{c}}|0\rangle_{\hat{b}_3} + \sqrt{1-\mu}|0\rangle_{\hat{c}}|1\rangle_{\hat{b}_3}$, generated by a single photon that goes through a beam splitter with transmittance μ; see figure 3.1(b). For an input state in the $|0\rangle$-$|1\rangle$ space, the QS could then offer an asymmetric teleportation

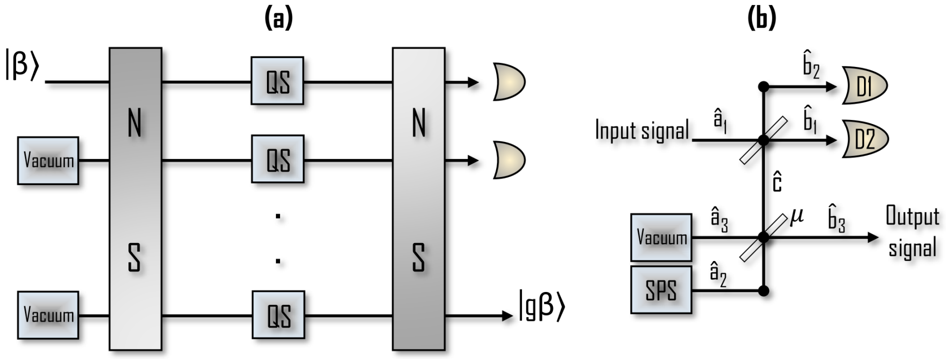

Figure 3.1: Schematic of the QS-based quantum amplifier. **(a)** Ralph and Lund NLA. **(b)** Structure of a quantum scissor.

functionality, whenever the Bell-state measurement operation is successful, i.e., when only one of D1 or D2 detector in figure 3.1(b) clicks. For instance, in the particular case of a weak coherent state input $|\alpha\rangle_{\hat{a}_1} \approx |0\rangle_{\hat{a}_1} + \alpha|1\rangle_{\hat{a}_1}$, with $|\alpha| \ll 1$, a single click could come from the single-photon component in the entangled state $|\psi\rangle$ and/or the input state. In that case, the output state, after renormalization, can be approximated by $|0\rangle_{\hat{b}_3} + \alpha g|1\rangle_{\hat{b}_3} \approx |\alpha g\rangle_{\hat{b}_3}$, for $|g\alpha| \ll 1$, where $g = \sqrt{(1-\mu)/\mu}$ represents the amplification gain of the QS, with μ being the main parameter in the heart of the QS module. Under these assumptions, the success probability for the QS operation is given by $P^{\text{RL}}_{\mathsf{succ}}(\alpha) \approx \mu + (1-\mu)|\alpha|^2$. Note that, in the above description, the essential assumption for a QS to possibly operate as an NLA is that $|\alpha| \ll 1$ and $|g\alpha| \ll 1$.

Upon successful operation in all QS modules, the second N-splitter is designed to congregate all the light into a single output port. The NLA is assumed successful in amplifying input state $|\beta\rangle$ providing that there are no clicks after the second N-splitter in other $N-1$ output ports. For $N \gg g|\alpha|$, RL-NLA does the following:

$$|\beta\rangle \longrightarrow \frac{e^{|\beta|^2(g^2-1)/2}}{(g^2+1)^{N/2}}|g\beta\rangle. \tag{3.5}$$

Success probability of the NLA is then given by $P_{\mathsf{succ}}(\beta) = e^{|\beta|^2(g^2-1)}/(g^2+1)^N$. In order to have a gain greater than unity, we must choose $\mu < 1/2$.

Although it is shown that RL-NLA can succeed in amplifying an input coherent state, it might face challenges in an actual realization, where an experimentalist has to consider practical issues. First, for a given N, the RL-NLA setup needs N single-photon states to be injected into the QSs. "On-demand" single-photon sources are then needed. Such a source can be supplied by quantum dots Ding *et al.* [2016]. In order to have a full analysis, one needs to provide a proper model for the single-photon source. Second, inefficiency of the detectors, when the detector does not click while there exists a photon, as well as the dark count in the detectors, when the detector clicks while there is no photon, should be taken into account and modelled. Third, in the main setup, it is assumed that the QS' inputs are truncated coherent states, in a superposition of $|0\rangle$ and $|1\rangle$ number states. This assumption is not generally true since the actual input states into the QSs are coherent states and, in principle, could even be arbitrary states. As a result, the probability of success would change. Finally, in order to have a more realistic model of the NLA, we need to model the N-splitters as well. The N-splitters can be built using typical 50/50 beam splitters, imperfection of which should also be considered.

Another point to remark is that the probability of success of RL-NLA is input-dependent and exponentially *increasing* with the input mean photon number $|\alpha|^2$. Nonetheless, this fact is restricted by the assumption $N \gg g|\alpha|$. Therefore, a trade-off holds here: for a fixed N, we cannot have large input power and large amplification gains at the same time.

While considering a QS-based CV-QKD system, we should take into account the following concerns. First, note that the output state of a QS is always in the space spanned by single-photon and vacuum states. By approximating the output state as a coherent state, we are introducing some errors, which can affect the security of the system. More precisely, the transition from a coherent state to a single-photon state is a non-Gaussian one, whose effect must be carefully considered in the security analysis. Secondly, for the purpose of CV-QKD, where, in principle, an arbitrary modulation variance may be required, which can result in large-amplitude coherent states, an approximation to the output state of the QSs/RL-NLA may not be satisfactory. In other words, in the GG02 protocol, the coherent states are chosen randomly via Gaussian distributions; hence, the input states to the QS may not necessarily satisfy the assumption $|\alpha| \ll 1$.

Therefore, in order to resolve the above issues, we present, in section 3.4, the *exact* output state and probability of success for not only an arbitrary coherent state, but also arbitrary TMSV and thermal states, at the input of a QS. Before that we discuss the use of NLAs in a repeater setup. It is also worth mentioning that one can implement a QS/NLA which truncates input states to first N Fock states Jeffers [2010], McMahon *et al.* [2014]. In this thesis, however, we limit ourselves to the single-photon truncation. In section 4.2, we will apply our findings to the key rate analysis of a QS-equipped CV-QKD system. For simplicity, we assume that the required single-photon source in the QS is ideal and on-demand. Single-photon detector efficiencies are also assumed to be unity. Our analysis can, nevertheless, be extended to account for the imperfections in the source and detectors.

3.3 Continuous-variable quantum repeaters

In quantum communication channels, existence of loss and noise imposes limitations on transferring quantum information. The input signal gets more and more attenuated as it goes to longer distances. Therefore, loss, along with noise in quantum channels, restrict the CV-QKD protocols to limited distances and low secret key rates. Similar to DV systems Briegel *et al.* [1998], one can then think of using quantum repeaters (QRs) for CV systems.

An immediate application of NLAs is to make use of them in the structure of QRs, which can outperform conventional bounds on quantum communication rates Pirandola *et al.* [2017], Pirandola [2019]. A CV version of QRs has recently been proposed by Dias & Ralph [2017], which relies on CV teleportation techniques and NLAs, with the ultimate goal of increasing the transmission distance. Our analysis in this dissertation will provide insights into the applicability of such proposals for CV QRs Dias & Ralph [2017], Furrer & Munro [2018], Seshadreesan *et al.* [2018] particularly for QKD purposes. This is achieved by studying the elementary repeater (error correction) link used in the repeater setups by Dias & Ralph [2017] and Seshadreesan *et al.* [2018].

The CV QR proposed by Dias and Ralph operates as follows. It contains a chain of $\mathcal{N}$ identical single-link modules, as its building block, as shown in figure 3.2. Each module contains a TMSV state, represented by V, a quantum channel with transmittance T, and an NLA with amplification gain g. The module is ready to operate, i.e., to get linked to the other blocks of the repeater network,

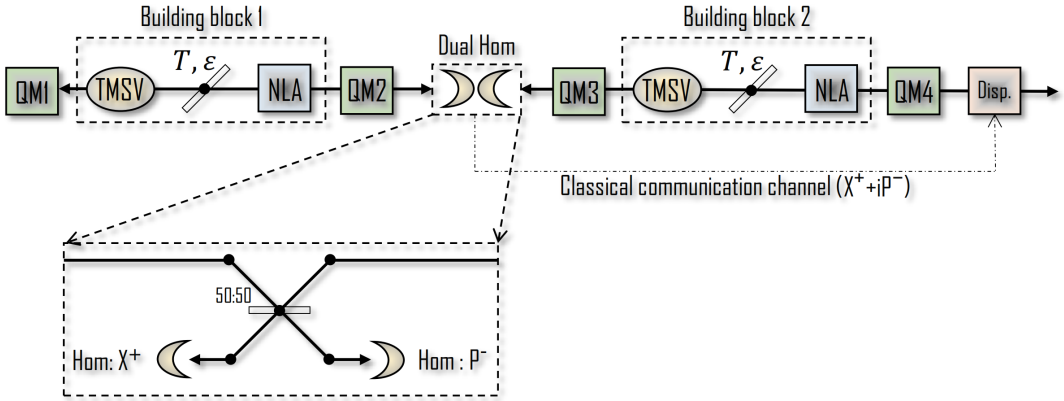

Figure 3.2: Schematic of a single-node CV quantum repeater setup. It consists of two building blocks. A Dual Hom box is used to connect neighbouring building blocks of the repeater network by coupling the signals at a balanced beam splitter followed by two homodyne detection modules, of which one measures X quadrature while the other measures P. At the Displacement box, based on information received from the Dual Hom module, $X^+ + iP^-$, proper adjustments are performed on the final state.

upon a successful NLA operation. If all $\mathcal{N}$ building-block links are ready, dual homodyne units—also known as CV Bell detection relays—are performed to connect neighbouring modules. Otherwise, the end-to-end states of each primary module should be stored in quantum memories (QMs), as shown in figure 3.2, and wait until successful NLA operation is announced for adjacent modules. The information obtained by dual homodyne units are then sent through a classical channel, where a proper displacement operation is applied (displacement operations can be done at each stage or they can be postponed for a global displacement at the end).

It is shown that the above QR setup can offer an effective channel transmittance of T for the repeater network, where the total transmittance for the no-repeater link would be $T^{\mathcal{N}}$. Assuming that high-efficacy QMs are available, the success probability of the QR scales polynomially with the single-link probability of success, $P^{(1)}_{\mathsf{succ}}$, as follows

$$P^{\mathrm{QR}}_{\mathsf{succ}} = (P^{(1)}_{\mathsf{succ}})^{\log_2(2\mathcal{N})}, \tag{3.6}$$

while it scales exponentially, $(P^{(1)}_{\mathsf{succ}})^{\mathcal{N}}$, for the no-QR case.

In the context of CV-QKD, the building block in figure 3.2 is previously studied with an ideal NLA Blandino *et al.* [2012]. It was shown that an NLA can indeed increase the secure distance of CV-QKD. However, there, the NLA was essentially considered as a "black-box", whose innermost structure is not known, except that it does $|\alpha\rangle \rightarrow |g\alpha\rangle$ without adding excess noise. They have also assumed the maximum success probability for such an ideal NLA, i.e., $1/g^2$. Thus, the use of realistic devices, such as QSs and/or QS-based NLAs, is one step towards a real-world implementation of such systems. When considering a QS as an NLA, previous studies have worked out some features of the system, such as output variance, for a *pure-loss* channel Dias & Ralph [2017], Seshadreesan *et al.* [2018]. However, they mostly rely on the very weak input assumption; hence, giving only an approximate output state and success probability for the QS-amplified primary building block. In addition, channel excess noise, which can get amplified via the NLA device, is assumed zero. One of the key objectives of this thesis is to account for an exact calculation of the QR building block, when a QS is in use, to offer a realistic study of the building-block operation. We simultaneously account for both loss and excess noise. As well, in the next chapters, we show the benefit of using a QS-assisted receiver in CV-QKD protocols.

We remark that one could use the heralded *quantum state comparison amplifier* proposed by Eleftheriadou *et al.* [2013] and experimentally demonstrated by Donaldson *et al.* [2015]. However, such an NLA can effectively amplify coherent states chosen from a finite set. While state comparison amplifier can be helpful for discrete-modulated CV-QKD protocols, where a finite set of coherent states is used, it might not be the case in a Gaussian-modulated scenario. In this thesis, we focus on the use of QSs, in both the Gaussian- and discrete-modulated CV-QKD protocols. The case of state comparison amplifiers remains open and is left for future work.

3.4 A comprehensive study of quantum scissors

In this section, we obtain the exact input-output relationship for a QS driven by a coherent state. At the same time, we first let the coherent state to travel through a thermal-loss channel. We use characteristic functions, described in section 2.1.1, to represent the involved states. Using such a formulation, we then analyse the QR building block in figure 3.2, which includes a QS driven by an arbitrary TMSV state through a thermal-loss channel with transmissivity T and excess noise ε.

3.4.1 Pre-measurement state for input coherent states

Consider figure 3.3, where we replace the NLA in the building block of figure 3.2 with a QS. We can use the well-known relationships for beam splitters Kok *et al.* [2007] to relate the four input modes to the four output modes; see figure 3.3. The dashed box Γ is a linear optics circuit, for which such input-output relationships can be obtained. In particular, considering the input modes represented by $\mathcal{A}^T = [\hat{a}_1\ \hat{a}_2\ \hat{a}_3\ \hat{a}_{\mathsf{n}}]$ and output modes $\mathcal{B}^T = [\hat{b}_1\ \hat{b}_2\ \hat{b}_3\ \hat{b}_{\mathsf{n}}]$, we find $\mathcal{B} = \Gamma\mathcal{A}$, where the transformation matrix

$$\Gamma = \begin{pmatrix} \sqrt{\frac{T}{2}} & \sqrt{\frac{\mu}{2}} & -\sqrt{\frac{1-\mu}{2}} & \sqrt{\frac{1-T}{2}} \\ -\sqrt{\frac{T}{2}} & \sqrt{\frac{\mu}{2}} & -\sqrt{\frac{1-\mu}{2}} & -\sqrt{\frac{1-T}{2}} \\ 0 & \sqrt{1-\mu} & \sqrt{\mu} & 0 \\ -\sqrt{1-T} & 0 & 0 & \sqrt{T} \end{pmatrix} \tag{3.7}$$

is a unitary matrix, i.e., $\Gamma^T = \Gamma^{-1}$. The output antinormally-ordered characteristic function can then be expressed in terms of the input one by

$$\begin{aligned} \chi_A^{\text{out}}(\xi_1, \xi_2, \xi_3, \xi_{\mathsf{n}}) =& \Big\langle \prod_{m=1}^{3} \hat{D}_A(\hat{b}_m, \xi_m)\hat{D}_A(\hat{b}_{\mathsf{n}}, \xi_{\mathsf{n}})\Big\rangle \\ =& \Big\langle \prod_{m=1}^{3} \hat{D}_A(\hat{a}_m, \lambda_m)\hat{D}_A(\hat{a}_{\mathsf{n}}, \lambda_{\mathsf{n}})\Big\rangle \\ =& \chi_A^{\text{in}}(\lambda_1, \lambda_2, \lambda_3, \lambda_{\mathsf{n}}), \end{aligned} \tag{3.8}$$

where $[\lambda_1\ \lambda_2\ \lambda_3\ \lambda_{\mathsf{n}}]^T = \Gamma^T[\xi_1\ \xi_2\ \xi_3\ \xi_{\mathsf{n}}]^T$. In above, we made use of the facts that $\hat{D}_A(s\hat{a}, \xi) = \hat{D}_A(\hat{a}, s\xi)$, where $s \in \mathbb{R}$, and $\langle\hat{D}_A(\hat{a}, \xi_1)\hat{D}_A(\hat{a}, \xi_2)\rangle = e^{\xi_1\xi_2^*}\langle\hat{D}_A(\hat{a}, \xi_1 + \xi_2)\rangle$.

Next, we consider the particular input state

$$\hat{\rho}_{\mathcal{A}} = |\alpha\rangle_{\hat{a}_1}\langle\alpha| \otimes |1\rangle_{\hat{a}_2}\langle 1| \otimes |0\rangle_{\hat{a}_3}\langle 0| \otimes \int d^2\beta f_\varepsilon(\beta)|\beta\rangle_{\hat{a}_{\mathsf{n}}}\langle\beta| \tag{3.9}$$

to the system, where $f_\varepsilon(\beta) = \frac{e^{-\frac{|\beta|^2}{\varepsilon/2}}}{\pi\varepsilon/2}$, with ε quantifying the noise level in $\hat{a}_{\mathsf{n}}$ port, represents a Gaussian thermal noise. Note that the part $|1\rangle_{\hat{a}_2}\langle 1| \otimes |0\rangle_{\hat{a}_3}\langle 0|$ is

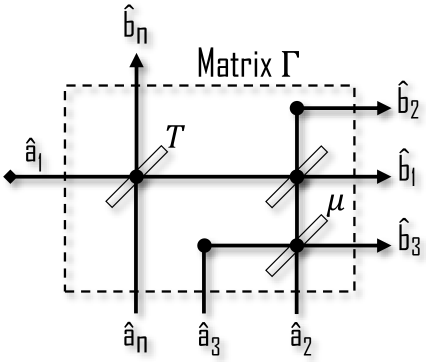

Figure 3.3: The quantum channel and the QS are considered as a combined system with input modes $\hat{a}_1 - \hat{a}_3$ and $\hat{a}_{\mathsf{n}}$ and four output modes $\hat{b}_1 - \hat{b}_3$ and $\hat{b}_{\mathsf{n}}$. The transformation matrix of the system is given by (3.7).

required as input for the QS operation. The input state in (3.9) corresponds to a Gaussian attack by Eve, which we later use in forthcoming sections. For the above set of input states, the output antinormally-ordered characteristic function can be found using (3.8) as follows

$$\begin{aligned}\chi_A^{\text{out}}(\xi_1, \xi_2, \xi_3, \xi_{\mathsf{n}}) =&\chi_A^{\text{in}}(\lambda_1, \lambda_2, \lambda_3, \lambda_{\mathsf{n}})\\ =&\text{tr}\Big[\hat{\rho}_A \hat{D}_A(\hat{a}_1, \lambda_1)\hat{D}_A(\hat{a}_2, \lambda_2)\hat{D}_A(\hat{a}_3, \lambda_3)\hat{D}_A(\hat{a}_{\mathsf{n}}, \lambda_{\mathsf{n}})\Big],\end{aligned} \tag{3.10}$$

which, by using the transformation matrix Γ, can be re-written in the following form

$$\begin{aligned}\chi_A^{\text{out}}(\xi_1, \xi_2, \xi_3, \xi_{\mathsf{n}}) =&e^{-\frac{T}{2}|\xi_1-\xi_2-\sqrt{2}\tau\xi_{\mathsf{n}}|^2} e^{\sqrt{2T}i\text{Im}[\bar{\alpha}(\xi_1-\xi_2-\sqrt{2}\tau\xi_{\mathsf{n}})]}\\ &\times e^{-\frac{1-T}{2}(1+\frac{\varepsilon}{2})|\xi_1-\xi_2+\frac{\sqrt{2}}{\tau}\xi_{\mathsf{n}}|^2} e^{-\frac{1-\mu}{2}|\xi_1+\xi_2-\frac{\sqrt{2}}{g}\xi_3|^2} e^{-\frac{\mu}{2}|\xi_1+\xi_2+\sqrt{2}g\xi_3|^2}\\ &\times \left(1 - \frac{\mu}{2}|\xi_1 + \xi_2 + \sqrt{2}g\xi_3|^2\right),\end{aligned} \tag{3.11}$$

where $g = \sqrt{(1-\mu)/\mu}$ and $\tau = \sqrt{(1-T)/T}$. Therefore, using (2.17), the joint state of the output modes is then given by

$$\begin{aligned}\hat{\rho}_{\mathbb{B}} = \int \frac{d^2\xi_1}{\pi} \int \frac{d^2\xi_2}{\pi} \int \frac{d^2\xi_3}{\pi} \int \frac{d^2\xi_{\mathsf{n}}}{\pi} \chi_A^{\text{out}}(\xi_1, \xi_2, \xi_3, \xi_{\mathsf{n}})\\ \hat{D}_N(\hat{b}_1, \xi_1)\hat{D}_N(\hat{b}_2, \xi_2)\hat{D}_N(\hat{b}_3, \xi_3)\hat{D}_N(\hat{b}_{\mathsf{n}}, \xi_{\mathsf{n}}).\end{aligned} \tag{3.12}$$

We can next trace out mode $\hat{b}_{\mathsf{n}}$ to obtain the joint state of the modes $\hat{b}_1 - \hat{b}_3$:

$$\hat{\rho}_{\text{out}} = \int \frac{d^2\xi_1}{\pi} \int \frac{d^2\xi_2}{\pi} \int \frac{d^2\xi_3}{\pi} \chi_A^{\text{out}}(\xi_1, \xi_2, \xi_3, 0) \hat{D}_N(\hat{b}_1, \xi_1) \hat{D}_N(\hat{b}_2, \xi_2) \hat{D}_N(\hat{b}_3, \xi_3), \tag{3.13}$$

where we made use of the identity $\text{tr}(\hat{D}_N(a, \xi)) = \pi\delta^2(\xi)$, and

$$\begin{aligned}\chi_A^{\text{out}}(\xi_1, \xi_2, \xi_3, 0) =& e^{-F_1|\xi_1-\xi_2|^2} e^{\sqrt{2T} i \text{Im}[\bar{\alpha}(\xi_1-\xi_2)]} e^{-\frac{\mu}{2}|\xi_1+\xi_2+\sqrt{2}g\xi_3|^2} e^{-\frac{1-\mu}{2}|\xi_1+\xi_2-\frac{\sqrt{2}}{g}\xi_3|^2} \\ & \times \Big(1 - \frac{\mu}{2}|\xi_1 + \xi_2 + \sqrt{2}g\xi_3|^2\Big),\end{aligned} \tag{3.14}$$

with $F_1 = \frac{1}{2} + \frac{1}{4}(1 - T)\varepsilon$. Note that $\varepsilon_{\mathsf{rec}} = (1 - T)\varepsilon$ is the amount of excess noise at the end of the quantum channel; thus, we have $F_1 = \frac{1}{2} + \frac{1}{4}T\varepsilon_{\mathsf{tm}}$, where $\varepsilon_{\mathsf{tm}} = \varepsilon_{\mathsf{rec}}/T$ is the equivalent amount of excess noise at the transmitter side.

3.4.2 Post-selected state for input coherent states

Following Ralph & Lund [2009], we consider a QS successful if only one detector of the QS, corresponding to modes $\hat{b}_1$ and $\hat{b}_2$ in figure 3.3, clicks. In order to model such measurements we use the following non-resolving measurement operator

$$\widehat{\mathsf{M}} = (\mathbb{1}_2 - |0\rangle_{\hat{b}_1}\langle 0|) \otimes |0\rangle_{\hat{b}_2}\langle 0|, \tag{3.15}$$

which corresponds to the case where photons are found in mode $\hat{b}_1$, but not in mode $\hat{b}_2$. The post-selected state, $\hat{\rho}_{\text{out}}^{\mathsf{PS}}$, is then given by Nielsen & Chuang [2000]:

$$\begin{aligned}\hat{\rho}_{\text{out}}^{\mathsf{PS}} =& \frac{\text{tr}_{\hat{b}_1\hat{b}_2}(\hat{\rho}_{\text{out}}\widehat{\mathsf{M}})}{\text{tr}(\hat{\rho}_{\text{out}}\widehat{\mathsf{M}})} \\ =& \frac{1}{P^{\mathsf{PS}}} \int \frac{d^2\xi_1}{\pi} \int \frac{d^2\xi_2}{\pi} \int \frac{d^2\xi_3}{\pi} \chi_A^{\text{out}}(\xi_1, \xi_2, \xi_3, 0)(\pi\delta^2(\xi_1) - 1)\hat{D}_N(\hat{b}_3, \xi_3),\end{aligned} \tag{3.16}$$

where $P^{\mathsf{PS}} = \text{tr}(\widehat{\mathsf{M}}\hat{\rho}_{\text{out}})$ is the corresponding (success) probability to measurement $\widehat{\mathsf{M}}$, which will be calculated in section 3.4.3.

Because the *truncated* post-measurement state lives in the qubit subspace spanned by number states $\{|0\rangle_{\hat{b}_3}, |1\rangle_{\hat{b}_3}\}$, the output state has the form

$$\hat{\rho}_{\text{out}}^{\mathsf{PS}}(\alpha) =\rho_{00}(\alpha)|0\rangle_{\hat{b}_3}\langle 0| + \rho_{01}(\alpha)|0\rangle_{\hat{b}_3}\langle 1| + \rho_{10}(\alpha)|1\rangle_{\hat{b}_3}\langle 0| + \rho_{11}(\alpha)|1\rangle_{\hat{b}_3}\langle 1|, \tag{3.17}$$

where $\rho_{jk}(\alpha) = {}_{\hat{b}_3}\langle j|\hat{\rho}^{\mathsf{PS}}_{\text{out}}(\alpha)|k\rangle_{\hat{b}_3}$, for $j, k = 0, 1$. We then obtain

$$\begin{cases} \rho_{00}(\alpha) = \frac{2[2F_1(2F_1+1)+T|\alpha|^2]}{(g^2+1)P^{\mathsf{PS}}(\alpha)(2F_1+1)^3} e^{-T\frac{|\alpha|^2}{2F_1+1}} \\ \rho_{01}(\alpha) = \frac{-2g\sqrt{T}\alpha}{(g^2+1)P^{\mathsf{PS}}(\alpha)(2F_1+1)^2} e^{-T\frac{|\alpha|^2}{2F_1+1}} = \rho^*_{10}(\alpha) \\ \rho_{11}(\alpha) = \frac{2g^2}{(g^2+1)P^{\mathsf{PS}}(\alpha)} \left(\frac{e^{-T\frac{|\alpha|^2}{2F_1+1}}}{2F_1+1} - \frac{e^{-T\frac{|\alpha|^2}{2F_1}}}{4F_1} \right). \end{cases} \tag{3.18}$$

We remark that in the case that no photon is found in mode $\hat{b}_1$ while a photon is observed in mode $\hat{b}_2$, the QS is still considered successful. After working out the post-selected output state, we find that the result has the same form as in (3.17), but we only need to replace α with $-\alpha$ in (3.18). In practice, in a QKD setup, Bob can negate its measurement results whenever this happens. One can also use a unitary operation to correct the output state so that we always end up with (3.17) as the post-selected state.

We also note that the post-measurement state is Hermitian and positive-semi-definite, as expected. Moreover, in the limit of $|g\alpha| \ll 1$, we can verify that the post-selected state of the single QS approaches the weak coherent state $|g\alpha\rangle$; hence, reducing to the results by Ralph & Lund [2009].

3.4.3 Probability of success

The probability of post-selection for measurement $\widehat{\mathsf{M}}$ and input $|\alpha\rangle$, $P^{\mathsf{PS}}(\alpha)$, is given by

$$\begin{aligned} P^{\mathsf{PS}}(\alpha) =& \text{tr}(\hat{\rho}_{\text{out}}\widehat{\mathsf{M}}) \\ =& \int \frac{d^2\xi_1}{\pi} \int \frac{d^2\xi_2}{\pi} \chi^{\text{out}}_A(\xi_1, \xi_2, 0, 0)(\pi\delta^2(\xi_1) - 1). \end{aligned} \tag{3.19}$$

By substituting (3.11) into the above expression, we obtain the exact QS probability of success

$$\begin{aligned} P_{\mathsf{succ}}(\alpha) =& 2P^{\mathsf{PS}}(\alpha) \\ =& \frac{4\Big(g^2(2F_1+1)^2 + 2F_1(2F_1+1) + T|\alpha|^2\Big)e^{-T\frac{|\alpha|^2}{2F_1+1}}}{(g^2+1)(2F_1+1)^3} - \frac{g^2 e^{-T\frac{|\alpha|^2}{2F_1}}}{(g^2+1)F_1}, \end{aligned} \tag{3.20}$$

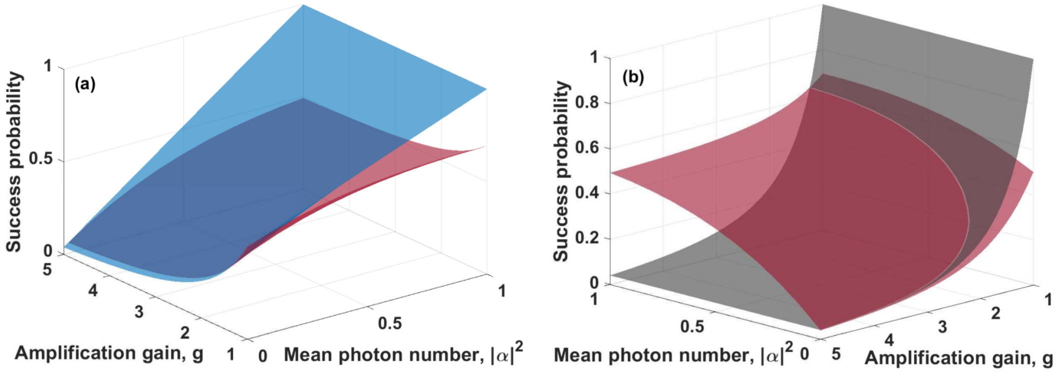

Figure 3.4: **(a)** The exact success probability of a single QS (lower red), P_{succ}, and that based on input intensity approximations (upper blue), $P_{\mathsf{succ}}^{\mathrm{RL}}$. **(b)** The exact success probability of a single QS (red), P_{succ}, and that of an ideal NLA (grey), upper bounded by $1/g^2$, versus average photon number and amplification gain. In all cases, $\varepsilon = 0$ and $T = 1$.

which is the total probability of success for the QS module, i.e., when either of D1 or D2 detector clicks. As expected, $P_{\mathsf{succ}}(\alpha)$ approaches, to first-order approximation, to $P_{\mathsf{succ}}^{\mathrm{RL}}(\alpha) = \mu + (1-\mu)|\alpha|^2 = (1+|g\alpha|^2)/(1+g^2)$, when $|\alpha| \ll 1$, at $\varepsilon = 0$ and $T = 1$. This approximation is, however, invalid even when we slightly deviate from the limiting condition on $|\alpha|$, as can be seen in figure 3.4(a). Here, we have plotted the exact probability of success, $P_{\mathsf{succ}}(\alpha)$, versus $|\alpha|^2$ and g, and compared it with the asymptotic value obtained by Ralph and Lund, $P_{\mathsf{succ}}^{\mathrm{RL}}(\alpha)$. It can be seen that the exact probability of success is always lower than the asymptotic value, and the difference is visible at all values of g. The success probability also increases with the decrease in g. For $|\alpha| \ll 1$, the success probability approaches its maximum possible value of $1/g^2$ Pandey *et al.* [2013]. But, again, as can be seen in figure 3.4(b), we quickly deviate from this ideal regime when $|\alpha|$ increases. This indicates that we cannot operate at maximum possible success probability for all possible inputs, as assumed in Blandino *et al.* [2012], if we use a QS as an NLA.

In figure 3.4(b), the maximum possible success probability, $1/g^2$, divides the plot into two regions. There is a region in which the success probability is above the maximum possible for an NLA. This implies that the QS operation should be very noisy in this region, hence breaking the assumption on the noise-free

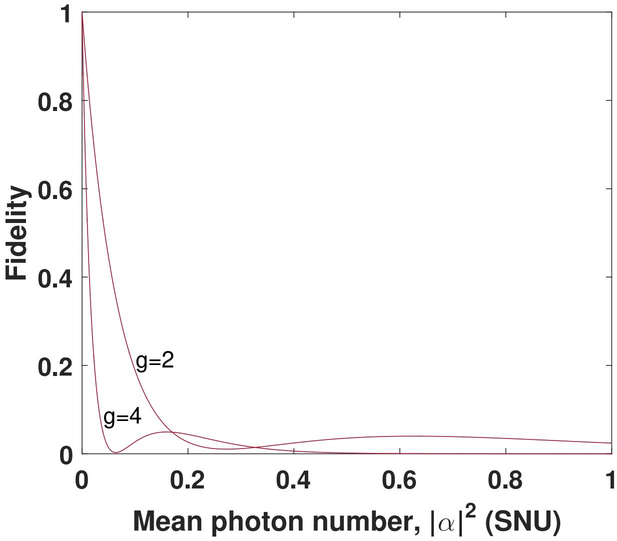

Figure 3.5: Fidelity of QS's output with the target amplified state $|g\alpha\rangle$ versus input intensity. In both cases, $\varepsilon = 0$ and $T = 1$.

operation of the NLA. If we want to work in the region that $P_{\mathsf{succ}}(\alpha) < 1/g^2$, we will then have to deal with limitations on the maximum gain that we can choose for the range of input states we may expect. This indicates a trade-off between the amount of noise that the QS may add to the signal versus its gain and success probability. We will later address this issue, in the context of CV-QKD, in our numerical results when we optimize the secret key generation rate over system parameters.

3.4.4 Fidelity of the amplified state

To gain more insight into the behaviour of QSs, we can look at other properties of them. For instance, a measure that can show how good a QS can be in amplifying an input coherent state, $|\alpha\rangle$, is the fidelity of the target amplified state, $|g\alpha\rangle$, which can be obtained, with what a QS is actually offering at its output, i.e., $\hat{\rho}_{\text{out}}^{\mathsf{PS}}(\alpha)$ given in (3.17). By definition Nielsen & Chuang [2000], the fidelity is calculated from

$$F(\alpha) = \langle g\alpha|\hat{\rho}_{\text{out}}^{\mathsf{PS}}(\alpha)|g\alpha\rangle. \tag{3.21}$$

We have plotted this quantity versus α for two fixed values of g in figure 3.5. As expected, it shows that a QS can amplify a relatively weak coherent state signal with a fidelity approaching unity. As the input intensity goes up, the QS is incapable of offering a fidelity close to one. In addition, figure 3.5 indicates that we should expect from a QS with a larger amplification gain to give low values of fidelity when compared with a low-gain QS. We also see that there is an overshoot on the curves. The reason probably is that the output state is a highly non-linear function of the input state's intensity, $|\alpha|^2$. We note that, as long as $P_{\mathsf{succ}}(\alpha)F(\alpha) < 1/g^2$, this behaviour is allowed by quantum mechanics; for more detail we refer to Pandey *et al.* [2013].

3.4.5 Non-Gaussian behaviour of quantum scissors

Before involving QSs in a CV-QKD system, it is necessary to better understand the nature of a quantum channel that includes a QS module. This is important because majority of results on the secret key rate of CV-QKD systems rely on Gaussian characteristics of the channel García-Patrón & Cerf [2006], Lodewyck *et al.* [2007]. This is not, however, the case for a QS-equipped channel as we see in this section.

In order to examine the non-Gaussian behaviour of the QS output, let us focus on the distribution of homodyne measurement results on quadrature $\hat{X}_B$. Let us also consider an input coherent state $|\alpha\rangle$, with $\alpha = X_A + iP_A$ as distributed by

$$f_{\mathcal{X}_A}(X_A) = \frac{e^{-\frac{X_A^2}{V_A/2}}}{\sqrt{\pi V_A/2}} \quad \text{and} \quad f_{\mathcal{P}_A}(P_A) = \frac{e^{-\frac{P_A^2}{V_A/2}}}{\sqrt{\pi V_A/2}}, \tag{3.22}$$

at the port $\hat{a}_1$, which results in a thermal state, characterized by variance V_A. After performing similar calculations, where in the input state given by (3.9) we replace the coherent state in mode $\hat{a}_1$ with a thermal state with variance V_A, the post-selected state will be given by

$$\hat{\sigma}_{\text{out}}^{\mathsf{PS}}(V_A) = \sigma_{00}(V_A)|0\rangle_{\hat{b}_3}\langle 0| + \sigma_{11}(V_A)|1\rangle_{\hat{b}_3}\langle 1|, \tag{3.23}$$

where

$$\begin{cases} \sigma_{00}(V_A) = \frac{8F_2}{(g^2+1)(2F_2+1)^2 P_{\mathsf{succ}}(V_A)} \\ \sigma_{11}(V_A) = \frac{4g^2}{(g^2+1)P_{\mathsf{succ}}(V_A)}\left(\frac{1}{2F_2+1} - \frac{1}{4F_2}\right), \end{cases} \tag{3.24}$$

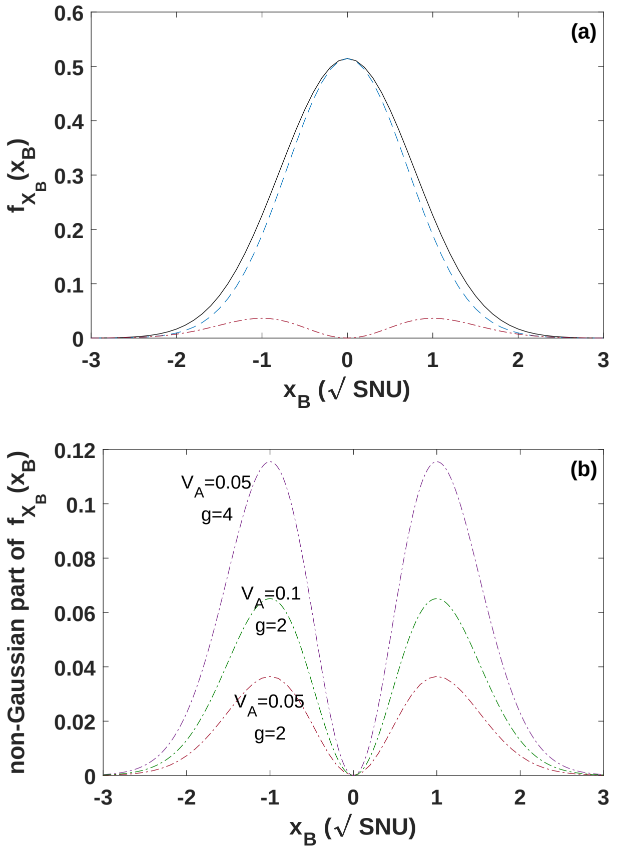

Figure 3.6: **(a)** The output distribution at the receiver side (solid black), which comprises Gaussian (dashed blue) and non-Gaussian (dot-dashed red) parts. Here, $V_A = 0.05$, $g = 2$, $\varepsilon = 0$, and $T = 1$. **(b)** The non-Gaussian part of the distribution for several different values of modulation variance and amplification gain.

with success probability given by

$$P_{\mathsf{succ}}(V_A) = \frac{4}{(g^2+1)}\Big(\frac{g^2(2F_2+1)+2F_2}{(2F_2+1)^2} - \frac{g^2}{4F_2}\Big). \tag{3.25}$$

Note that here parameter $F_2 = \frac{1}{2} + \frac{1}{4}T(V_A + \varepsilon_{\mathsf{tm}})$ is slightly different from F_1.

The probability distribution for obtaining a real number X_B after measuring $\hat{X}_B$, conditional on the success of the QS, is then given by

$$\begin{aligned} f_{X_B}(X_B) &= \mathrm{tr}(\hat{\sigma}^{\mathsf{PS}}_{\mathrm{out}}(V_A)|X_B\rangle\langle X_B|) \\ &= \Big(\sigma_{00}(V_A) + 2\sigma_{11}(V_A)X_B^2\Big)\frac{e^{-X_B^2}}{\sqrt{\pi}}, \end{aligned} \tag{3.26}$$

where $\hat{X}_B|X_B\rangle = X_B|X_B\rangle$.

The expression for $f_{\chi_B}(X_B)$ will then have two components: one is a Gaussian term in X_B proportional to $\sigma_{00}(V_A)$, and the other is a non-Gaussian term proportional to $\sigma_{11}(V_A)$. Figure 3.6(a) shows the contribution of each of these components in making $f_{\chi_B}(X_B)$ at $V_A = 0.05$ and $g = 2$. We notice that even for such a small modulation variance, which corresponds mostly to small values of $|\alpha|$, and a small amplification gain the non-Gaussian term is quite distinct. As can be seen in figure 3.6(b), higher amplification gains and higher values of modulation variance could even result in more deviation from a Gaussian state. This non-Gaussian behaviour would have ramifications on the key rate analysis of a QS-based system as we see in the next two chapters.

3.4.6 Pre-measurement state for input TMSV states

We use a similar approach to section 3.4.1 in using characteristic functions to find an input-output relationship when the QS is successful in figure 3.7, where now a TMSV state is at the input. As discussed in chapter 2, this analysis can ease calculation of Holevo information.

By using (2.16) and the transformation matrix Γ, we can write the full output antinormally-ordered characteristic function, including the mode $\hat{a}_0$, in terms of the input one, i.e., $\chi_A^{\text{out}}(\xi_0, \xi_1, \xi_2, \xi_3, \xi_\mathsf{n}) = \chi_A^{\text{in}}(\lambda_0, \lambda_1, \lambda_2, \lambda_3, \lambda_\mathsf{n})$, where we have

$$[\xi_0\ \xi_1\ \xi_2\ \xi_3\ \xi_\mathsf{n}] = \begin{pmatrix} 1 & 0 \\ 0 & \Gamma \end{pmatrix} [\lambda_0\ \lambda_1\ \lambda_2\ \lambda_3\ \lambda_\mathsf{n}]$$

and

$$\chi_A^{\text{in}}(\lambda_0, \lambda_1, \lambda_2, \lambda_3, \lambda_\mathsf{n}) = \chi_A^{\text{TMSV}}(\lambda_0, \lambda_1) \times \chi_A^{\text{in}}(\lambda_2, \lambda_3, \lambda_\mathsf{n}). \tag{3.27}$$

The function $\chi_A^{\text{TMSV}}(\lambda_0, \lambda_1)$ is the antinormally-ordered characteristic function of the TMSV state, given in (2.31) and described by a single parameter δ. The term $\chi_A^{\text{in}}(\lambda_2, \lambda_3, \lambda_\mathsf{n})$ is calculated for an input state $|1\rangle_{\hat{a}_2}\langle 1| \otimes |0\rangle_{\hat{a}_3}\langle 0| \otimes \int d^2\beta f_\varepsilon(\beta)|\beta\rangle_{\hat{a}_\mathsf{n}}\langle\beta|$, as seen in section 3.4.1.

Putting all this together, we then find the pre-measurement antinormally-

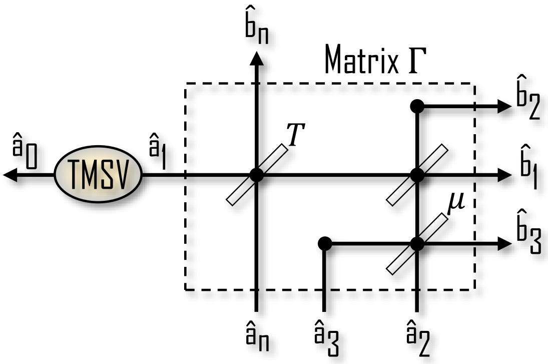

Figure 3.7: The quantum channel and the QS are considered as a combined system with input modes $\hat{a}_1 - \hat{a}_3$ and $\hat{a}_{\mathsf{n}}$ and four output modes $\hat{b}_1 - \hat{b}_3$ and $\hat{b}_{\mathsf{n}}$. The transformation matrix of the system is given by (3.7).

ordered characteristic function for modes $\hat{a}_0$, $\hat{b}_1 - \hat{b}_3$, and $\hat{b}_{\mathsf{n}}$, as follows:

$$\begin{aligned}\chi_A^{\text{out}}(\xi_0, \xi_1, \xi_2, \xi_3, \xi_{\mathsf{n}}) =& e^{-\delta^2|\xi_0|^2} e^{-\frac{\delta^2 T}{2}|\xi_1 - \xi_2 - \sqrt{2}\tau\xi_{\mathsf{n}}|^2} e^{-\delta\sqrt{2T(\delta^2-1)}\,\mathrm{Re}[\xi_0^*(\xi_1^* - \xi_2^*)]} \\ & \times e^{-\frac{1-T}{2}(1+\frac{\varepsilon}{2})|\xi_1 - \xi_2 + \frac{\sqrt{2}}{\tau}\xi_{\mathsf{n}}|^2} e^{-\frac{1-\mu}{2}|\xi_1 + \xi_2 - \frac{\sqrt{2}}{g}\xi_3|^2} e^{-\frac{\mu}{2}|\xi_1 + \xi_2 + \sqrt{2}g\xi_3|^2} \\ & \times \left(1 - \frac{\mu}{2}|\xi_1 + \xi_2 + \sqrt{2}g\xi_3|^2\right). \end{aligned} \tag{3.28}$$

Having obtained the output antinormally-ordered characteristic function (3.28), we use (2.17) to find the corresponding output state:

$$\begin{aligned}\hat{\rho}_{0123\mathsf{n}}^{\text{out}} = \int & \frac{d^2\xi_0}{\pi}\frac{d^2\xi_1}{\pi}\frac{d^2\xi_2}{\pi}\frac{d^2\xi_3}{\pi}\frac{d^2\xi_{\mathsf{n}}}{\pi}\chi_A^{\text{out}}(\xi_0, \xi_1, \xi_2, \xi_3, \xi_{\mathsf{n}}) \\ & \hat{D}_N(\hat{a}_0, \xi_0)\hat{D}_N(\hat{b}_1, \xi_1)\hat{D}_N(\hat{b}_2, \xi_2)\hat{D}_N(\hat{b}_3, \xi_3)\hat{D}_N(\hat{b}_{\mathsf{n}}, \xi_{\mathsf{n}}). \end{aligned} \tag{3.29}$$

In the following, we show how the shared state between Alice and Bob is found step-by-step. We first trace out mode $\hat{b}_{\mathsf{n}}$ to obtain

$$\begin{aligned}\hat{\rho}_{0123}^{\text{out}} = \int & \frac{d^2\xi_0}{\pi}\frac{d^2\xi_1}{\pi}\frac{d^2\xi_2}{\pi}\frac{d^2\xi_3}{\pi}\chi_A^{\text{out}}(\xi_0, \xi_1, \xi_2, \xi_3, 0) \\ & \hat{D}_N(\hat{a}_0, \xi_0)\hat{D}_N(\hat{b}_1, \xi_1)\hat{D}_N(\hat{b}_2, \xi_2)\hat{D}_N(\hat{b}_3, \xi_3). \end{aligned} \tag{3.30}$$

Next, by applying the QS measurements, given in (3.15), we find the post-selected state:

$$\hat{\rho}_{03}^{\mathsf{PS}} = \frac{\mathrm{tr}_{12}(\hat{\rho}_{0123}^{\text{out}}\widehat{\mathsf{M}})}{\mathrm{tr}(\hat{\rho}_{0123}^{\text{out}}\widehat{\mathsf{M}})} = \frac{\hat{\varrho}_{03}^{\mathsf{PS}}}{P_{\text{EB}}^{\mathsf{PS}}}, \tag{3.31}$$

where

$$\hat{\varrho}_{03}^{\mathsf{PS}} = \int \frac{d^2\xi_0}{\pi}\frac{d^2\xi_3}{\pi}\widetilde{\chi}_{\mathrm{A}}(\xi_0,\xi_3)\hat{D}_N(\hat{a}_0,\xi_0)\hat{D}_N(\hat{b}_3,\xi_3) \tag{3.32}$$

with

$$\widetilde{\chi}_{\mathrm{A}}(\xi_0,\xi_3) := \int \frac{d^2\xi_1}{\pi}\frac{d^2\xi_2}{\pi}\chi_A^{\mathrm{out}}(\xi_0,\xi_1,\xi_2,\xi_3,0)\Big(\pi\delta^2(\xi_1)-1\Big). \tag{3.33}$$

Also, $P_{\mathrm{EB}}^{\mathsf{PS}} = \overline{P}_{\mathsf{succ}}/2$ is the corresponding post-selection probability to measurement $\widehat{\mathsf{M}}$:

$$P_{\mathrm{EB}}^{\mathsf{PS}} = \widetilde{\chi}_{\mathrm{A}}(0,0) = \int \frac{d^2\xi_1}{\pi}\frac{d^2\xi_2}{\pi}\chi_A^{\mathrm{out}}(0,\xi_1,\xi_2,0,0)\Big(\pi\delta^2(\xi_1)-1\Big). \tag{3.34}$$

By using the bivariate state given in (3.31), we can now compute its statistical characteristics such as its corresponding covariance matrix (between modes $\hat{a}_0$ and $\hat{b}_3$ of the module given in figure 3.7), which we postpone to the next chapter when we present secret key rate analysis for the QS-equipped CV-QKD protocol. Also, in the EB scheme, we find the corresponding parameter δ in our TMSV state, which gives the same output statistics for the signal that goes to Bob, when Alice does a heterodyne measurement on her state. It turns out that to get an identical output state we should satisfy $\delta = \sqrt{(V+1)/2}$, where $V = V_A + 1$.

Furthermore, in the case of discrete modulation, where the TMSV state in figure 3.7 is replaced with the equivalent bipartite state to the quadrature-phase-shift-keying modulation, shown in figure 2.11, a similar route can be taken to work out the end-to-end state and its covariance matrix. This will fully be presented in chapter 5.

3.5 Summary

In this chapter, we reviewed the basic physics of quantum noiseless linear amplifiers (NLAs), which are intrinsically probabilistic. We also discussed how such amplifiers can be used in the design of a continuous-variable quantum repeater, whose probability of success scales polynomially with success probability of its building block. As a possible realization, we focused on a building block that has a quantum scissor (QS), as a non-deterministic NLA, at its core. We fully studied the module by working out its exact output as well as exact success probability for an arbitrary coherent state as its input. We, furthermore, extended our calculations to an arbitrary input two-mode squeezed vacuum state. In the next two chapters, we combine our knowledge of CV-QKD protocols and QS-based NLAs. We will study the use of a QS at the receiver side of the Gaussian modulated, in chapter 4, and discrete modulation, in chapter 5, CV-QKD protocols, and see if this would increase their secret key rates.

Chapter 4

Continuous-variable quantum key distribution with quantum scissors

In this chapter, we provide a realistic account of what a quantum scissor (QS) can offer within a CV-QKD setup. In particular, using an exact model for the QS setup, see chapter 3, we analyse the secret key rate of a Gaussian modulated protocol, whose receiver unit is equipped with a QS. One of the implications of our exact modelling for the QS is that we cannot directly apply standard key rate calculation techniques that rely on the Gaussianity of the output states. This will make the exact calculation of the key rate cumbersome. We manage this problem by using relevant bounds for certain components of the key rate. We investigate the extent to which the use of QSs can increase the security distance in CV-QKD systems.

One of our key incentives for carrying out the above analysis is to provide insights into the applicability of recent proposals for CV quantum repeaters (CV QRs) Dias & Ralph [2017], Furrer & Munro [2018], Seshadreesan *et al.* [2018] particularly for QKD operation. The QS-equipped CV-QKD link that we consider here contains the elementary repeater (error correction) link used in the repeater setup of Dias & Ralph [2017], and as such a poor performance for this basic building block could cast shadow on the usefulness of any larger quantum repeater setup that relies on such elementary links. In the repeater setup of Dias

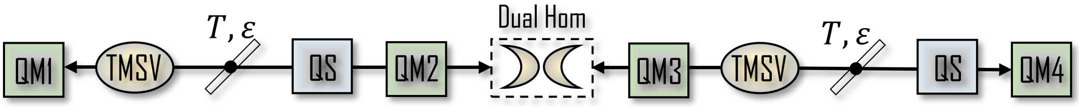

Figure 4.1: A two-leg quantum repeater module as proposed by Dias & Ralph [2017]. Each leg is composed of a TMSV source generating two-mode squeezed vacuum states, a quantum scissor (QS), and two quantum memory (QM) units. Beam splitters with transmissivity T characterize the loss in each leg, with excess noise represented by ε. Upon successful operation of the QS in each leg, the output of the QS and the TMSV source are stored in respective QMs. When both legs are ready, a joint dual homodyne (Dual Hom) measurement is performed on the quantum states stored in QM2 and QM3, which swaps entanglement to QM1 and QM4.

& Ralph [2017], CV teleportation is used to swap entanglement between already entangled links, in a set of quantum memories (QMs), represented by QM1-QM2 and QM3-QM4 in figure 4.1. Each of such links have been entangled by sending one half of a two-mode squeezed vacuum state, represented by TMSV boxes, through a thermal-loss channel. The received signal will then be amplified, in a probabilistic way, by the QS module, and will be stored in the corresponding QM. Note that, considering the non-deterministic behaviour of the QS, use of QM modules is necessary if we aim to achieve any rate enhancement from the CV QR setup. The dual homodyne module will then effectively perform entanglement swapping in the CV domain once both links have had successful QS operations.

We remark that the above repeater setup must use a *physical* noiseless linear amplifier (MLA) implementation, such as a QS, and not a virtual one, in order to offer any rate advantage. That is, the class of measurement-based NLA (MB-NLA) implementations Chrzanowski *et al.* [2014], Fiurášek & Cerf [2012], Walk *et al.* [2013], which rely on data post-selection, would not be suitable for such CV repeaters. Due to reliance of MB-NLAs on classical post-selection, the state of QM2 and QM4 must inevitably be measured before the entanglement swapping can be done. Even if we do not consider the applications of our considered setup in CV repeater settings, one must be cautious with typically poor success probability of MB-NLAs compared to that of physical NLAs Zhao *et al.* [2017]. This suggests that the use of physical NLAs in CV-QKD systems is still of interest, and, in fact, one may favour a physical realization of an NLA over its virtual post-measurement implementation due to restrictions on the MB-NLA Bernu *et al.* [2014]. Our study here would shed more light into the applicability of such physical realizations by offering an accurate analysis of the underlying system.

We would also like to point out that there are certain practical aspects that one should consider before using QSs in CV-QKD. One assumption that we make throughout this dissertation is that on-demand single-photon sources are available for our scheme. There are two practical issues, in this regard, that affect the performance of the QS-based system. The first is the rate at which single-photons are generated. The success rate of such sources directly affect the key rate achievable. Secondly, we should be cautious about the purity of the single-photon source output. Multiple-photon components, in particular, could be damaging to the performance of the QS. The good news is that the current available technology for quantum-dot sources has made a substantial progress to meet both above requirements. In particular, quantum dot sources with efficiencies over 80% and second-order coherence values < 0.004 have already been demonstrated Müller *et al.* [2014], Senellart *et al.* [2017]. Additionally, one issue is the reliance on single-photon detectors, which will make CV-QKD systems, in terms of requirements, as expensive as their discrete-variable counterparts. But, paying such prices may be unavoidable if one wants to have long-distance CV-QKD and/or CV repeaters.

In the following, we describe details of the proposed system. Next, we present the key rate analysis of the CV-QKD link with a single QS as part of its receiver. We then discuss the numerical results.

Our main contributions in this chapter

- We calculate exact mutual information for our QS-assisted CV-QKD system, by focusing on its prepare-and-measure (P&M) scheme.

- We find an upper bound for the Holevo information for our QS-assisted CV-QKD system, by focusing on its entanglement-based (EB) scheme.

- We provide a lower bound on the key rate of the QS-assisted CV-QKD system under Gaussian attacks.

- We show that secret key rate of the QS system can outperform the no-QS one at certain regimes of operation.

4.1 System description

In this section, we describe our proposed setup for the QS-amplified CV-QKD protocol.

4.1.1 Prepare-and-measure scheme: Preparing to calculate mutual information

We assume that Alice is connected to Bob via a quantum channel; see figure 4.2(a). The protocol runs along the same lines as proposed by Grosshans and Grangier in 2002 (GG02), as described in section 2.2. That is, in every round, Alice transmits a coherent state $|\alpha\rangle$ to Bob, where $\alpha = X_A + iP_A$, with $X_A, P_A \in \mathbb{R}$ being chosen randomly according to the following Gaussian probability density functions:

$$f_{\mathcal{X}_A}(X_A) = \frac{e^{-\frac{X_A^2}{V_A/2}}}{\sqrt{\pi V_A/2}} \quad \text{and} \quad f_{\mathcal{P}_A}(P_A) = \frac{e^{-\frac{P_A^2}{V_A/2}}}{\sqrt{\pi V_A/2}}, \tag{4.1}$$

where V_A is the modulation variance in the shot-noise units; therefore, the state that Alice prepares is a thermal state in the following form:

$$\hat{\rho}_{\mathsf{th}} = \int d^2\alpha \frac{e^{-\frac{|\alpha|^2}{V_A/2}}}{\pi V_A/2} |\alpha\rangle\langle\alpha|. \tag{4.2}$$

At the receiver, however, we equip Bob with a single QS before the homodyne module used in GG02. Upon a successful QS operation, Bob randomly chooses to measure $\hat{X}_B = \hat{a}_B + \hat{a}_B^\dagger$ or $\hat{P}_B = (\hat{a}_B - \hat{a}_B^\dagger)/i$, where $\hat{a}_B$ represents the annihilation operator for the output mode of the QS. During the sifting stage, Bob would then publicly declare his measurement choices as well as the rounds in which the QS has been successful. By using post-processing techniques, Alice and Bob extract a key from the subset of data for which the QS has been successful.

In chapter 3, for an arbitrary input state, we calculated the exact post-selected state and success probability for the QS-amplified channel. That will indeed help

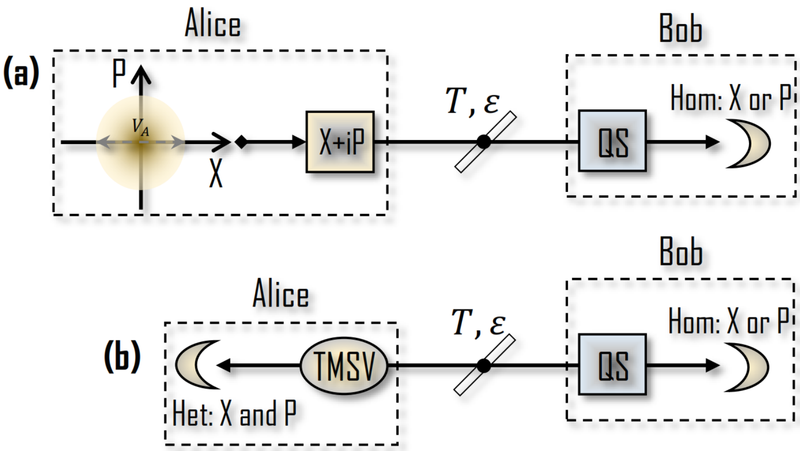

Figure 4.2: **(a)** Schematic view of P&M CV-QKD link with an additional quantum scissor at the receiver. **(b)** EB CV-QKD protocol equivalent to **(a)**. Hom and Het represent, respectively, the homodyne detection and heterodyne detection modules.

to compute the mutual information between Alice and Bob, as we will see shortly, in section 4.2.1.

4.1.2 Entanglement-based scheme: Preparing to calculate Holevo information

Alternatively, one can use the equivalent EB scheme of the protocol, shown in figure 4.2(b), where Alice's source is replaced with a TMSV source followed by a heterodyne detection on one of the two modes of the state. She sends the other mode to Bob through the quantum channel (in either P&M or EB case, we assume that Bob can reconstruct, in an error-free way, the phase reference for the local oscillator used in his homodyne detection). Note that the setup sketched in figure 4.2(b) is the same building block of the CV QR as in figure 3.2. We, thus, aim to work out the relevant calculations of the core module in the CV QR proposal by Dias & Ralph [2017]. In particular, for the Holevo information, following the results that we obtained in section 3.4.6, we work out the conditional covariance matrix (CM) between Alice and Bob, upon a successful QS operation; see section 4.2.2. The obtained CM is then used to calculate Holevo information. In this way, we will be able to analyse secret key rate of the proposed system.

4.1.3 Quantum channel

The trusted parties are assumed to use a thermal-loss channel with transmissivity T and an excess noise ε; see section 2.1.5. A potential model for such a channel is given by a beam splitter, with transmissivity T, that mixes Alice's signals and the eavesdropper's thermal state, given by the following expression:

$$\hat{\rho}_{\mathsf{th}} = \int d^2\beta \frac{e^{-\frac{|\beta|^2}{\varepsilon/2}}}{\pi\varepsilon/2} |\beta\rangle_{\hat{a}_{\mathsf{n}}} \langle\beta|, \tag{4.3}$$

where $\hat{a}_{\mathsf{n}}$ is the annihilation operator corresponding to the noise port. The equivalent excess noise at the input to the channel is then given by $\varepsilon_{\mathsf{tm}} = (1-T)\varepsilon/T$. In principle, the parties cannot tell what kind of channel they have without proper parameter estimation. The assumption of a thermal-loss channel corresponds to the case of a Gaussian attack, which may not be optimal for our non-Gaussian system. However, as long as the system does not deviate considerably from the Gaussian framework, the results obtained will provide us with a reasonable estimate of the potential key rate that can be obtained by a more rigorous analysis He *et al.* [2018]. We use the above model to calculate the relevant parameters of the CM when QSs are in use.

4.2 Secret key rate analysis

Here, we use the results in section 3.4 to determine the secret key rate of the GG02 protocol when Bob uses a single QS before his homodyne measurement. We find the secret key rate under Gaussian eavesdropping attacks Pirandola *et al.* [2008]. This corresponds to a thermal-loss channel with transmissivity T, modelled by a beam splitter, and an excess noise at the transmitter side $\varepsilon_{\mathsf{tm}}$; see section 2.1.5. Such an attack may not be the optimal one for our non-Gaussian channel. But, based on our analysis on non-Gaussianity behaviour of the QS, see figure 3.6, at the low-modulation-variance and low-amplification-gain regimes, the results obtained for this particular channel should not be far away from that obtained in an optimal attack He *et al.* [2018]. The secret key rate of CV-QKD protocols in the asymptotic limit of infinitely many signals is given by (2.37), which for clarity, we repeat here:

$$R_{\mathsf{RR}} = \beta I(\mathcal{X}_A : \mathcal{X}_B) - \chi_{BE}, \tag{4.4}$$

where here β is reconciliation efficiency.

In our proposed setup, since the QS operation is non-deterministic, the whole key rate formula should be multiplied by the *average* success probability of the QS, $\overline{P}_{\mathsf{succ}}$, where the averaging is performed over all possible inputs. Therefore, the secret key rate reads

$$R_{\mathsf{RR}} \geq \overline{P}_{\mathsf{succ}}(\beta I^{\star}(\mathcal{X}_A : \mathcal{X}_B) - \chi^{\star}_{BE}), \tag{4.5}$$

where '$\star$' indicates that the mutual and Holevo information terms are calculated for the post-selected data when the QS is successful. The measurement results corresponding to unsuccessful QS events will be discarded at the sifting stage.

The fact that we only use the post-selected data for key extraction implies that we have to account for the non-Gaussianity of the QS output states. Unfortunately, the non-Gaussian behaviour of the QS makes conventional methods for key rate calculation inapplicable. In order to take the non-Gaussian effects into account, we calculate the exact mutual information by directly using the conditional distribution of the QS output. Ideally one could also look for the exact calculation of the Holevo information term as well. But, this turns out to be extremely cumbersome. Instead, here, we find an upper bound for the Holevo information term by finding the CM of the output state from the total channel and then calculate the Holevo information for a Gaussian state with the same CM. The reason is that Gaussian collective attacks are proven to be optimal in the sense that they maximize the Holevo quantity García-Patrón & Cerf [2006] of a fixed CM for the output shared state. Given the generality of the results by García-Patrón & Cerf [2006], in a real experiment, once we obtain the CM terms from the measurement results, we can use the same methodology to obtain a lower bound on the key rate.

In the following, we provide more detail on how each of the terms in (4.5) can be calculated.

4.2.1 Mutual information

The mutual information between two random variables $\mathcal{X}_A$ and $\mathcal{X}_B$, corresponding to post-selected data on Alice's and Bob's sides, is the difference between the entropy function $H(\mathcal{X}_B)$ and the conditional entropy function $H(\mathcal{X}_B|\mathcal{X}_A)$ Cover & Thomas [2006]:

$$I^{\star}(\mathcal{X}_A : \mathcal{X}_B) = H(\mathcal{X}_B) - H(\mathcal{X}_B|\mathcal{X}_A), \tag{4.6}$$

where

$$H(\mathcal{X}_B) = -\int dX_B \; f_{\mathcal{X}_B}(X_B) \log_2 f_{\mathcal{X}_B}(X_B), \tag{4.7}$$

and

$$H(\mathcal{X}_B|\mathcal{X}_A) = -\int\int dX_A dX_B f(X_A, X_B) \log_2 f_{\mathcal{X}_B}(X_B|X_A), \tag{4.8}$$

with $f(X_A, X_B) = f_{\mathcal{X}_A}(X_A) f_{\mathcal{X}_B}(X_B|X_A)$ being the joint probability density function.

Here, $f_{\mathcal{X}_B}(X_B)$ can be obtained by using (3.26), while the conditional output distribution $f_{\mathcal{X}_B}(X_B|X_A)$ can be obtained as follows:

$$f_{\mathcal{X}_B}(X_B|X_A) = \mathrm{tr}(\hat{\omega}^{\mathrm{PS}}_{\mathrm{out}}(X_A)|X_B\rangle\langle X_B|), \tag{4.9}$$

where the conditional output state $\hat{\omega}^{\mathrm{PS}}_{\mathrm{out}}(X_A)$ is given by (A.1) in appendix A. In our study, we numerically carry out the above integrals for a given set of parameters.

4.2.2 Holevo information

In order to calculate the Holevo information term, $\chi^{\star}_{BE}$, we use the EB description of the protocol, where one part of a TMSV state travels through the quantum channel and is amplified by a QS, while the other is measured by Alice; see figure 3.7. In order to upper bound $\chi^{\star}_{BE}$, what we need is then the CM of Alice-Bob bipartite state. We derived the exact post-selected joint state in subsection 3.4.6, from which the CM parameters can be obtained. As shown in figure 3.7, we also account for the effect of the quantum channel loss and excess noise in our calculations.

Following the results in section 3.4.6, appendix B provides the detailed calculations of the corresponding CM parameters. It turns out that the CM of the shared bipartite state between Alice and Bob has the form

$$V_{AB} = \begin{pmatrix} V_x \mathbb{1}_2 & V_{xy}\sigma_{\mathsf{z}} \\ V_{xy}\sigma_{\mathsf{z}} & V_y \mathbb{1}_2 \end{pmatrix}, \tag{4.10}$$

where

$$\begin{aligned} V_x =& \frac{\delta^2}{(g^2+1)\overline{P}_{\mathsf{succ}}} \Bigg(\frac{8[\gamma^2 T + \big(2F_3 + 1 - \gamma^2 T\big)\big(g^2(2F_3+1) + 2F_3\big)]}{(2F_3+1)^3} \\ & - \frac{g^2(2F_3 - \gamma^2 T)}{F_3^2} \Bigg) - 1, \\ V_y =& \frac{4}{(g^2+1)\overline{P}_{\mathsf{succ}}} \Bigg(\frac{4[g^2(2F_3+1)+F_3]}{(2F_3+1)^2} - \frac{g^2}{F} \Bigg) - 1, \\ V_{xy} =& \frac{8\delta\gamma}{(g^2+1)\overline{P}_{\mathsf{succ}}(2F_3+1)^2} g\sqrt{T}, \end{aligned} \tag{4.11}$$

with $F_3 = \frac{1}{2} + \frac{1}{4}T(2(\delta^2 - 1) + \varepsilon_{\mathsf{tm}})$ and

$$\overline{P}_{\mathsf{succ}} = \frac{1}{g^2+1}\Big(4[(2F_3+1)g^2 + 2F_3]/(2F_3+1)^2 - g^2/F_3\Big). \tag{4.12}$$

It is interesting to make the following observation. If the TMSV state is assumed totally uncorrelated, which happens when its squeezing parameter goes to zero, both parts of the state are left with vacuum states. Thus, if the QS is successful, the output state of mode $\hat{b}_3$ should be a vacuum state as well. This means that the CM of the end-to-end state is the identity. We verify that in the case of having a totally uncorrelated TMSV state, corresponding to $\delta = 1$ and $\gamma = 0$ (see section 2.1.2), the CM will indeed result in the identity matrix; that is, we obtain $V_x = V_y = 1$ and $V_{xy} = 0$.

In addition, as a result of the statistical equivalence between EB and P&M schemes, where $\delta = \sqrt{(V+1)/2}$, with $V = V_A + 1$, we conclude that $F_3 = F_2$. Now that the CM is known, we can find an upper bound to the Holevo information by using (2.43).

4.3 Numerical results

In this section, we present numerical simulations of the secret key rate of the QS-amplified GG02 protocol and compare it with that of the conventional one.

We find the maximum value for the lower bound in (4.5) by optimizing, at each distance, the modulation variance, V_A, or, equivalently, the parameter δ in the EB scenario, as well as the QS parameter, μ, which specifies the QS amplification gain. We also account for the excess noise, as discussed in previous sections. We assume that the quantum channel between the sender and receiver is an optical fibre with loss factor α, whose transmittance is given by $T = 10^{-\alpha L/10}$, where L is the channel length and the loss factor is $\alpha = 0.2$ dB/km corresponding to standard low-loss telecom optical fibres. Also, we assume $\beta = 1$ and that ideal homodyne detection, with no electronic noise, is performed at the receiver.

We first highlight the importance of accounting for the non-Gaussian behaviour of the QS by comparing the difference between the exact value of the mutual information function $I^{\star}(\mathcal{X}_A : \mathcal{X}_B)$, given by (4.6), and that obtained by Gaussian approximation, i.e.,

$$I^{\mathrm{G}}(\mathcal{X}_A : \mathcal{X}_B) = \frac{1}{2} \log_2 \frac{V_x V_y}{V_x V_y - V_{xy}^2}. \tag{4.13}$$

Figure 4.3 shows both curves, versus distance, at no excess noise. It is clear that the Gaussian approximation would have overestimated the mutual information between Alice and Bob at all distances considered, and that could have resulted in wrong bounds for the key rate of QS-based systems.

Figure 4.4 shows the optimized secret key rates of both conventional (solid lines) and the QS-assisted (dashed lines) GG02 protocol versus distance, as well as that of the PLOB bound for a repeaterless thermal-loss channel (labelled TL-PLOB). This is the bound given in (23) of Pirandola *et al.* [2017] at an equivalent mean thermal photon number, $\bar{\mathsf{n}} = \varepsilon_{\mathsf{tm}} T/(2(1-T))$, to our receiver excess noise (here at $\varepsilon_{\mathsf{tm}} = 0.05$). There are several interesting observations that can be made in this figure. First, we note that in all considered cases, there exists a crossover distance at which the QS-assisted curves surpass their corresponding no-QS curves. At $\varepsilon_{\mathsf{tm}} = 0$, this happens at around 200 km. By increasing $\varepsilon_{\mathsf{tm}}$, the crossover distance would drop and reaches around 175 km at $\varepsilon_{\mathsf{tm}} = 0.05$. This proves the key objective of our study that, by using realistic NLAs, there would be certain regimes where NLA-based systems improve the performance and the distance at which secure keys can be exchanged.

It can be seen, in figure 4.4, that QS-equipped receivers may not support high key rates at short distances. In fact, except for the case of $\varepsilon_{\mathsf{tm}} = 0$, we may

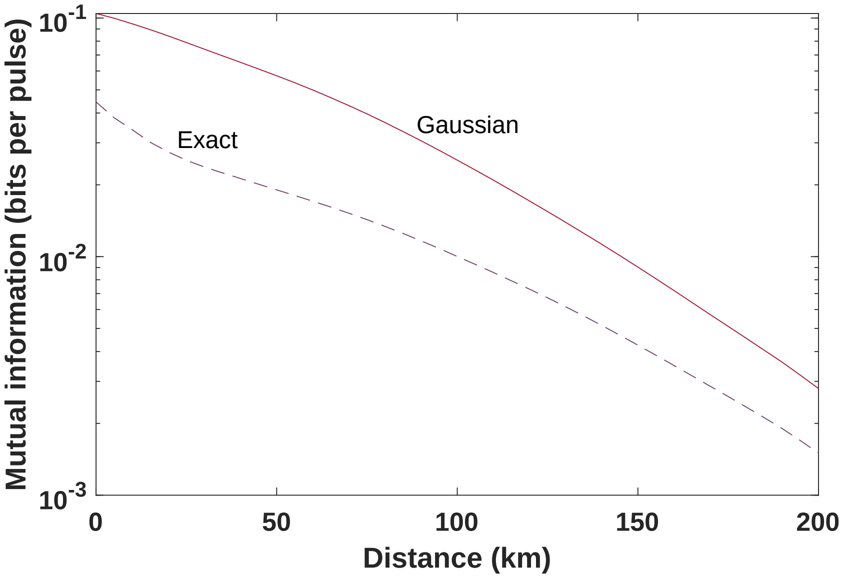

Figure 4.3: The exact mutual information function as compared to its Gaussian approximation versus distance at $\varepsilon = 0$. All other parameters have been optimized.

not be able to exchange any secret keys at very short distances for the QS-based system. Even for the no excess noise case, there are over two orders of magnitude difference between the no-QS and QS-based curves at $L = 0$. This is attributed to multiple factors. First, the trade-off between the choice of modulation variance and noise level in the system, would require us to use very small values of V_A at short distances, otherwise the QS will not operate at its low-noise regime. For instance, at $L = 0$, the optimum value of V_A for the QS-based system is 0.04. A no-QS system with such a low value of V_A also offers a low key rate of 2.83×10^{-2}, which is comparable to what we obtain for the QS-based system. Another factor is the success probability that at $L = 0$ is around 0.5, and it almost linearly goes down to around 0.15 at 200 km. One last factor is the fact that the QS is not entirely noise free. The additional noise by the QS would further decrease the rate at $L = 0$. In addition to this, if we have non-zero values of excess noise, a combination of the above effects plus the external noise drive the key rate to zero at very short distances. This is by itself not a practical dilemma, as, for a given channel length, one, in advance, can figure out whether to use a QS or not. But, this can affect the applicability of QS modules in a CV quantum repeater system.

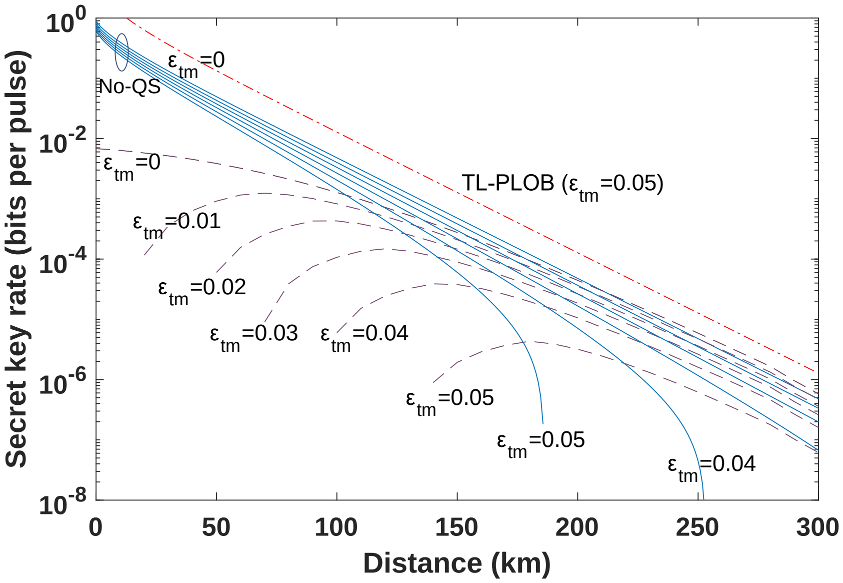

Figure 4.4: The optimized secret key rate for the QS-amplified CV-QKD protocol versus distance, as compared to the rate of conventional GG02, and the upper bound for a repeaterless thermal-loss channel (TL-PLOB) at a mean thermal photon number of $\varepsilon_{\text{rec}}/(2(1-T))$. The solid lines represent the no-QS case with top curve at $\varepsilon_{\text{tm}} = 0$, and the bottom one at $\varepsilon_{\text{tm}} = 0.05$, and the middle curves covering $\varepsilon_{\text{tm}} = 0.01 - 0.04$

.

Another observation in figure 4.4 is that, at long distances, the key rate for QS-based systems follows a parallel trend to that of the TL-PLOB curve. For instance, at $\varepsilon_{\text{tm}} = 0.05$, the key rate remains roughly one order of magnitude below the PLOB bound for long distances. We have numerically verified that, by optimizing system parameters, even for longer distances than shown on the graph, we can obtain positive key rates, albeit quiet low, for QS-assisted systems. The post-selection mechanism in the QS seems to be the key to obtaining positive key rates at long distances. At such distances, the channel loss naturally prepares low-intensity inputs to the QS, which allows us to use larger values of V_A, as shown in table 4.1. That would also enable us to use higher gains without necessarily increasing the QS noise. A higher-than unity gain for the post-selected states would then offer a better signal-to-noise ratio at long distances, which allows us to achieve positive secret key rates at longer distances than can otherwise be

Table 4.1: Optimized values for modulation variance and amplification gain at zero excess noise for the QS-based system.

Distance (km)	Optimized V_A	Optimized gain, g
0	0.05	1.00
100	0.8	1.36
200	3.5	2.38
300	11.5	4.36
400	12.5	14.1
500	13.5	100

achieved for a no-QS system.

Figure 4.4 also shows that our QS-amplified system cannot beat the existing upper bound for repeaterless systems Pirandola *et al.* [2017]. This agrees with the fact that any post-processing at the receiver side does not change the repeaterless nature of the link, even though a form of amplification is in use. But, it will be interesting to see if, based on the above results, we can assess the practicality of the proposed CV quantum repeater setups as proposed by Dias & Ralph [2017]. On the positive side, we can see that there exists a regime of operation where the slope of QS-based curves offer a square root advantage as needed in repeater systems. On the downside, however, this behaviour only appears in a limited range of distance, and only up to a maximum value of excess noise. In our simulations, we were not able to obtain any positive secret key rates at $\varepsilon_{\mathsf{tm}} = 0.06$, or higher. It seems that once the starting distance at which QS-based curves offer positive key rates lies above the maximum security distance for no-QS systems, it is no longer possible to get a positive key rate for QS-assisted systems. This may suggest that similar limitations might affect the suitability of CV repeater systems for QKD applications, which needs further investigation.

4.4 Summary

In this chapter, we studied the performance of the GG02 protocol where the received signal was amplified by a quantum scissor (QS). We showed that the QS would turn a Gaussian input state into a non-Gaussian one. That would make the conventional techniques to estimating the key rate not directly applicable to our case. We instead directly calculated the mutual information between Alice and Bob by working out the probability distribution function of the quadratures after the QS. Also, in order to calculate the leaked information to Eve, we obtained the exact covariance matrix of the bipartite state shared between sender and receiver labs in the particular case of a Gaussian attack. We then found the Holevo information corresponding to a Gaussian shared output state with the same covariance matrix, which gives an upper bound for the Holevo term in the case considered. We optimized the key rate over input modulation variance and amplification gain. Our results showed that, for a certain range of excess noise, the QS-enhanced system could reach longer distances than the no-QS system. Finally, note that while the original NLA proposal by Ralph and Lund relies on multiple QS modules, in our scheme, we find using one QS is optimal as it minimizes the noise while we can adjust the signal level by optimizing the modulation variance. This also agrees with the results reported in Seshadreesan *et al.* [2018], where they have shown that the reverse coherent information García-Patrón *et al.* [2009], Pirandola *et al.* [2009], as the figure of merit, is maximum when only one QS is used.

Chapter 5

Discrete-modulation continuous-variable quantum key distribution with quantum scissors

In chapter 4, we showed that quantum scissors (QSs), as non-deterministic amplifiers, can enhance the performance of Gaussian-modulated CV-QKD in noisy and long-distance regimes of operation. In this chapter, we extend this result to a *non-Gaussian* CV-QKD protocol with *discrete* modulation. We show that, by using a proper setting, the use of QSs in the receiver of such discrete-modulation protocols would allow us to achieve positive secret key rates at high loss and high excess noise regimes of operation, which would have been otherwise impossible. This also keeps the prospect of running discrete-modulation CV-QKD over CV quantum repeaters alive.

We consider all enabling factors within a single setup to study the rate-versus-distance behaviour for a discrete-modulation CV-QKD system, discussed in section 2.3, that uses QSs at its receiver. As pointed out, this is effectively the main building block in the CV quantum repeater setup proposed by Dias & Ralph [2017], which is now used for discrete-modulation CV-QKD. A realistic analysis of our setup could then be used to assess the practicality of the proposed repeater setups. It has already been shown that, by using an ideal non-deterministic noiseless linear amplifier (NLA) at the receiver's side, one can increase the maximum transmission distance and tolerable excess noise of the quadrature-phase-shift-keying (QPSK) protocol Xu *et al.* [2013]. However, a study that accounts for a realistic NLA, such as a QS, is missing. This is important, because one of the key incentives for using discrete-modulation CV-QKD is its similarity with existing coherent optical communications systems, which possibly makes its adoption and implementation more straightforward.

Our main contributions in this chapter

- We work out exact mutual information for our QPSK-modulated QS-assisted CV-QKD system, by focusing on its prepare-and-measure (P&M) scheme.
- We upper bound the Holevo information for our QPSK-modulated QS-assisted CV-QKD system, by focusing on its entanglement-based (EB) scheme.
- We provide a lower bound on the key rate of the QS-assisted CV-QKD system.
- We show that secret key rate of the QS system can beat the no-QS one at certain regimes of operation.

5.1 System description

In this section, we present our proposed P&M QS-amplified CV-QKD protocol with discrete modulation and its equivalent EB version. Both schemes are depicted in figure 5.1. Different components of the system are described below. In a conventional discrete modulation protocol, a particular finite constellation of coherent states is considered and used for encoding data. The QPSK modulation protocol was described in section 2.3, where its security proof was also discussed. Our QS-added protocol runs exactly the same as described there, except that Bob's receiver is now equipped with a QS. The trusted parties keep the detection results only if the QS operation is successful in the respective round; that is, only one of detectors D1 or D2, in figure 3.1(b), clicks. By doing reconciliation and privacy amplification, the parties can then obtain a common string of secret bits.

In order to calculate exact amount of mutual information, we use the P&M scheme of the protocol. We first, using our exact solution for the QS system with

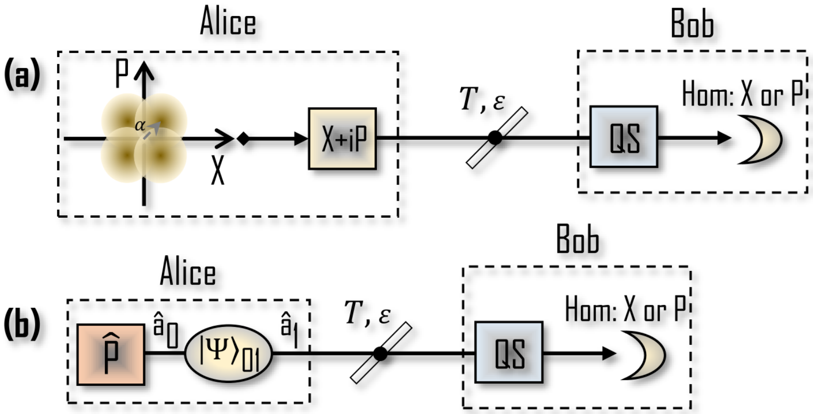

Figure 5.1: System description. **(a)** Schematic view of discrete-modulation CV-QKD protocol equipped with a QS as a part of its receiver. Here, the four yellow circles at the sender side represent the constellation of the four coherent states used at the encoder. The quantum channel is modelled by a beam splitter with transmissivity T and the excess noise represented by ε. **(b)** The EB CV-QKD protocol equivalent to **(a)**. $|\Psi\rangle_{01}$, QS, and $\widehat{\mathbf{P}}$ box, respectively, represent the bipartite entangled state in (2.48), a probabilistic QS as seen in figure 3.1(b), and the projective measurement module in $\{|\psi_k\rangle_0\}$ basis.

coherent state inputs, given in section 3.4, find the output state for the QPSK input; see section 5.2. Next, using such an output state, we work out the mutual information in section 5.3.

On the other hand, as earlier discussed, in order to calculate the Holevo information term, it is often easier to consider the equivalent EB scheme, which is shown in figure 5.1(b). In the EB version, instead of randomly choosing and sending single-mode coherent states, Alice measures one mode of a bipartite entangled state, and sends the other one to Bob. Note that in the Gaussian modulation case, the employed entangled state is a TMSV state, and Alice's measurement is a heterodyne detection. In the case of the QPSK protocol, it has been shown that one can start with a TMSV state, and apply a certain measurement to obtain the bipartite state $|\Psi\rangle_{01}$ in (2.48); see section 2.3 and Leverrier & Grangier [2011] for more detail.

In addition, we consider the same thermal-loss channel described in section 4.1.3.

5.2 Quantum-scissor assisted channel with discretely modulated inputs

We analysed QSs in detail in chapter 3. Here, we obtain the output state of the QS, upon successful operation, for an input QPSK state,

$$\hat{\rho} = \frac{1}{4}\sum_{k=0}^{3} |\alpha_k\rangle\langle\alpha_k|, \tag{5.1}$$

to the thermal-loss channel described in section 4.1 (note that $|\alpha_k\rangle = |\dot{\alpha}e^{(2k+1)i\pi/4}\rangle$, with $\dot{\alpha} \in \mathbb{R}^+$). In order to do so, we use the results reported in chapter 3. The output state of such a setup for an arbitrary coherent state, $|\alpha\rangle$, at the input has been derived in section 3.4, which, for clarity, we repeat the final results here:

$$\hat{\rho}^{\mathsf{PS}}_{\text{out}}(\alpha) = a(\alpha)|0\rangle_1\langle 0| + b(\alpha)|0\rangle_1\langle 1| + b^*(\alpha)|1\rangle_1\langle 0| + c(\alpha)|1\rangle_1\langle 1|, \tag{5.2}$$

where

$$\begin{cases} a(\alpha) = \frac{4[2F_1(2F_1+1)+T|\alpha|^2]}{(g^2+1)P_{\mathsf{succ}}(\alpha)(2F_1+1)^3} e^{-T\frac{|\alpha|^2}{2F_1+1}} \\ b(\alpha) = \frac{-4g\sqrt{T}\alpha}{(g^2+1)P_{\mathsf{succ}}(\alpha)(2F_1+1)^2} e^{-T\frac{|\alpha|^2}{2F_1+1}} \\ c(\alpha) = \frac{4g^2}{(g^2+1)P_{\mathsf{succ}}(\alpha)} \left(\frac{e^{-T\frac{|\alpha|^2}{2F_1+1}}}{2F_1+1} - \frac{e^{-T\frac{|\alpha|^2}{2F_1}}}{4F_1} \right), \end{cases} \tag{5.3}$$

with $F_1 = \frac{1}{2} + \frac{1}{4}(1-T)\varepsilon$ and

$$P_{\mathsf{succ}}(\alpha) = \frac{4\Big(g^2(2F_1+1)^2 + 2F_1(2F_1+1) + T|\alpha|^2\Big)e^{-T\frac{|\alpha|^2}{2F_1+1}}}{(g^2+1)(2F_1+1)^3} - \frac{g^2 e^{-T\frac{|\alpha|^2}{2F_1}}}{(g^2+1)F_1}. \tag{5.4}$$

In the case of QPSK modulation, the input state in (5.1) is an equi-probable mixture of four coherent states. Therefore, the output state is also a linear mixture of four states, i.e., $\hat{\rho}^{\mathsf{PS}}_{\text{out}}(\dot{\alpha}) = (1/4)\sum_{k=0}^{3} \hat{\rho}^{\mathsf{PS}}_{\text{out}}(\alpha_k)$, which can be simplified to the following state

$$\hat{\rho}^{\mathsf{PS}}_{\text{out}}(\dot{\alpha}) = a(\dot{\alpha})|0\rangle_1\langle 0| + c(\dot{\alpha})|1\rangle_1\langle 1|, \tag{5.5}$$

where $a(\dot{\alpha})$ and $c(\dot{\alpha})$ are given by (5.3).

Similar to the results obtained in section 3.4.5 for Gaussian distributed inputs, an interesting observation from (5.5) is that the output state of the QS is non-Gaussian. This is not just because we have used a non-Gaussian modulation, but even for a single coherent state at the input, as discussed in chapters 3 and 4, the output state is in the subspace spanned by $\{|0\rangle, |1\rangle\}$. There are two implications for this behaviour. First, the QS amplification cannot be noise free, as in an ideal NLA, but the amount of noise can vary based on the input signal and the amplification gain. Further, this non-Gaussianity can complicate the security analysis of the protocol. In our study, we manage this additional complexity by restricting the eavesdropper to collective Gaussian attacks Pirandola *et al.* [2008], as discussed in the previous chapter.

The non-Gaussianity of the channel manifests itself in the statistics that we can obtain from Bob's homodyne measurement. In particular, using similar techniques as in chapter 3 (equation (3.26)), the output probability distribution of $\hat{X}_B$ quadrature can be calculated as follows:

$$\begin{aligned} f_{\mathcal{X}_B}(X_B) &= \mathrm{tr}\Big(\hat{\rho}^{\mathsf{PS}}_{\mathrm{out}}(\dot{\alpha})|X_B\rangle\langle X_B|\Big) \\ &= \Big(a(\dot{\alpha}) + 2c(\dot{\alpha})X_B^2\Big)\frac{e^{-X_B^2}}{\sqrt{\pi}}, \end{aligned} \tag{5.6}$$

with $\hat{X}_B|X_B\rangle = X_B|X_B\rangle$. As can be seen in (5.6), similar to the Gaussian modulation case, the output probability distribution function is composed of a Gaussian and a non-Gaussian term. In the regime where $a(\dot{\alpha}) \gg c(\dot{\alpha})$, we are very close to a fully Gaussian system. For this to happen $\dot{\alpha}$ needs to be small. In the other extreme, when $c(\dot{\alpha}) \gg a(\dot{\alpha})$, we get a bimodal form for the output distribution, which is clearly non-Gaussian.

Similar to the calculation in appendix A, we can work out the conditional output probability distribution:

$$f_{\mathcal{X}_B}(X_B|X_{Ak}) = \mathrm{tr}[\hat{\rho}^{\mathsf{PS}}_{\mathrm{out,c}}(X_{Ak})|X_B\rangle\langle X_B|], \tag{5.7}$$

where

$$\hat{\rho}^{\mathsf{PS}}_{\mathrm{out,c}}(X_{Ak}) = a_{\mathrm{c}}(X_{Ak})|0\rangle_1\langle 0| + b_{\mathrm{c}}(X_{Ak})|0\rangle_1\langle 1| + b^*_{\mathrm{c}}(X_{Ak})|1\rangle_1\langle 0| + c_{\mathrm{c}}(X_{Ak})|1\rangle_1\langle 1| \tag{5.8}$$

is the QS output state conditioned on Alice sending a signal with X quadrature X_{Ak} *and* observing a click on D1. In this case,

$$\begin{cases} a_{\mathrm{c}}(X_{Ak}) = \frac{2\mu\left(4F_1(2F_1+1)+T(\dot{\alpha}^2+2X_{Ak}^2)\right)}{(2F_1+1)^3 P_c^{\mathsf{PS}}(X_{Ak})} e^{-\frac{T(\dot{\alpha}^2+2X_{Ak}^2)}{2(2F_1+1)}} \\ b_{\mathrm{c}}(X_{Ak}) = -\frac{2\sqrt{\mu(1-\mu)T}\,X_{Ak}}{(2F_1+1)^2 P_c^{\mathsf{PS}}(X_{Ak})} e^{-\frac{T(\dot{\alpha}^2+2X_{Ak}^2)}{2(2F_1+1)}} \\ c_{\mathrm{c}}(X_{Ak}) = 1 - a_{\mathrm{c}}(X_{Ak}) \end{cases} \tag{5.9}$$

and

$$\begin{aligned} P_c^{\mathsf{PS}}(X_{Ak}) =& \frac{2(2F_1+1)^2 - 2\mu(2F_1+1) + \mu T(\dot{\alpha}^2 + 2X_{Ak}^2)}{(2F_1+1)^3} e^{-\frac{T(\dot{\alpha}^2+2X_{Ak}^2)}{2(2F_1+1)}} \\ &- \frac{1-\mu}{2F_1} e^{-\frac{T(\dot{\alpha}^2+2X_{Ak}^2)}{4F_1}}. \end{aligned} \tag{5.10}$$

We will later use the above expressions in order to calculate the mutual information between the legitimate parties.

5.3 Secret key rate analysis

In this section, we present the key rate analysis for our QS-equipped CV-QKD system. We calculate the secret key generation rate for our system under the assumption that the eavesdropper is limited to Gaussian attacks. In this case, we can assume that the effective channel between the parties is a thermal-loss channel as we described in section 4.1. Note that the key rate obtained in this case is not necessarily an exact lower bound on the key rate because the optimal attack by an eavesdropper can be non-Gaussian. As it has been pointed out in He *et al.* [2018], however, the key rate obtained in our case is expected to be a close approximation to a true lower bound on the key rate.

In the asymptotic limit of many runs of the protocol, the secret key rate of a CV-QKD protocol under collective attacks is given by a similar equation to (4.5):

$$R_{\mathsf{RR}} \geq \overline{P}_{\mathsf{succ}}(\beta I^{\star}(\mathcal{X}_A : \mathcal{X}_B) - \chi_{BE}^{\star}), \tag{5.11}$$

In our protocol, the same as in the QS-amplified GG02 protocol, we discard data associated with the unsuccessful QS events and use only the post-selected data in order to produce a secret string of bits (we are using '$\star$' to emphasize this point). In the following, we first derive the exact value for mutual information $I^\star(\mathcal{X}_A : \mathcal{X}_B)$ and an upper bound for $\chi^\star_{BE}$ for the thermal-loss channel, upon successful QS events.

5.3.1 Mutual information

By definition, the mutual information of two random variables X_A and X_B is the difference between the entropy function $H(\mathcal{X}_B)$ and the conditional entropy $H(\mathcal{X}_B|\mathcal{X}_A)$:

$$I^\star(\mathcal{X}_A : \mathcal{X}_B) = H(\mathcal{X}_B) - H(\mathcal{X}_B|\mathcal{X}_A), \tag{5.12}$$

where

$$H(\mathcal{X}_B) = -\int dX_B \; f_{\mathcal{X}_B}(X_B) \log_2 f_{\mathcal{X}_B}(X_B) \tag{5.13}$$

and

$$H(\mathcal{X}_B|\mathcal{X}_A) = -\frac{1}{4}\sum_{k=0}^{3}\int dX_B \; f_{\mathcal{X}_B}(X_B|X_{Ak}) \log_2 f_{\mathcal{X}_B}(X_B|X_{Ak}). \tag{5.14}$$

Functions $f_{\mathcal{X}_B}(x_B)$ and $f_{\mathcal{X}_B}(X_B|X_{Ak})$ are given in (5.6) and (5.7), using which and the above equations, we numerically calculate the mutual information. We note that the input quadrature is a discrete random variable whereas the output is, in principle, continuous.

5.3.2 Holevo information

We upper bound the leaked information, $\chi^\star_{BE}$, by calculating the Holevo term for a Gaussian channel with the same covariance matrix (CM) as that of our system García-Patrón & Cerf [2006], Navascués *et al.* [2006]. In order to work out the corresponding CM, we first need to find the bipartite state between Alice's mode $\hat{a}_0$ and Bob's mode $\hat{b}_3$ for our QPSK setup in figure 5.2. This is akin to figure 3.7, except that the initial TMSV state is now replaced by the bipartite state in (2.48):

$$|\Psi\rangle_{01} = \frac{1}{2}\sum_{k=0}^{3} |\psi_k\rangle_0 |\alpha_k\rangle_1. \tag{5.15}$$

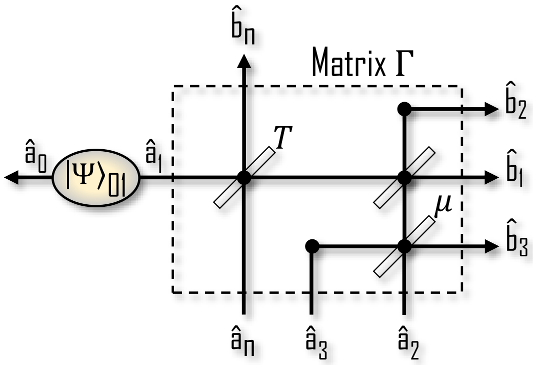

Figure 5.2: Entanglement-based version of the QS-amplified CV-QKD scheme. The noisy quantum channel and the QS are considered as a combined system, with input modes $\hat{a}_1 - \hat{a}_3$, and $\hat{a}_{\mathsf{n}}$, and output modes $\hat{b}_1 - \hat{b}_3$, and $\hat{b}_{\mathsf{n}}$. The initial state of modes represented by $\hat{a}_0 - \hat{a}_1$ is given by $|\Psi\rangle_{01}$. The initial state of the modes represented by operators $\hat{a}_2$, $\hat{a}_3$, and $\hat{a}_{\mathsf{n}}$ is, respectively, given by a single photon, a vacuum, and the thermal state in (4.3).

The quantum channel, QS operation, and the detection are the same as in the Gaussian-modulation study presented in chapter 4. In doing so, we let mode $\hat{a}_1$ of the above state to propagate through the thermal-loss channel, which couples Alice's signal to the thermal state given by (4.3):

$$\hat{\rho}_{\mathsf{th}} = \int d^2\beta \frac{e^{-\frac{|\beta|^2}{\varepsilon/2}}}{\pi\varepsilon/2} |\beta\rangle_{\hat{a}_{\mathsf{n}}}\langle\beta|, \tag{5.16}$$

and subsequently undergoes the QS operation.

Next, in order to calculate the joint state of modes $\hat{a}_0$ and $\hat{b}_3$, we follow the same procedure as in the previous chapter that relies on finding input-output characteristic functions for the module Γ, given in figure 5.2. Upon a successful QS operation, i.e., measurement $\widehat{\mathsf{M}} = (\mathbb{1}_2 - |0\rangle_{\hat{b}_1}\langle 0|) \otimes |0\rangle_{\hat{b}_2}\langle 0|$ in (3.15), we obtain

$$\hat{\rho}_{03} = \frac{1}{4P^{\mathsf{PS}}} \sum_{k=0}^{3}\sum_{l=0}^{3} |\psi_k\rangle_0\langle\psi_l| \otimes \hat{\Omega}_3^{kl}, \tag{5.17}$$

where

$$\hat{\Omega}_3^{kl} = \int \frac{d^2\xi_3}{\pi} \zeta_A^{kl}(\xi_3) \hat{D}_N(\hat{b}_3, \xi_3) \tag{5.18}$$

is the state that Bob measures. Here,

$$\zeta_A^{kl}(\xi_3) = \int \frac{d^2\xi_1}{\pi}\frac{d^2\xi_2}{\pi}\chi_A^{kl}(\xi_1, \xi_2, \xi_3) \tag{5.19}$$

where, for $|\alpha_k\rangle_1\langle\alpha_l|$ as the input state,

$$\begin{aligned}\chi_A^{kl}(\xi_1, \xi_2, \xi_3) =& e^{-F|\xi_1-\xi_2|^2} e^{\sqrt{\frac{T}{2}}[\alpha_l^*(\xi_1-\xi_2)-\alpha_k(\xi_1^*-\xi_2^*)]} \\ & \times e^{-\frac{\mu}{2}|\xi_1+\xi_2+\sqrt{2}g\xi_3|^2} e^{-\frac{1-\mu}{2}|\xi_1+\xi_2-\sqrt{2}/g\xi_3|^2} \\ & \times (\pi\delta^2(\xi_1) - 1)\Big(1 - \frac{\mu}{2}|\xi_1 + \xi_2 + \sqrt{2}g\xi_3|^2\Big) \end{aligned} \tag{5.20}$$

is the antinormally-ordered characteristic function of the output states in figure 5.2 after tracing over the noise mode $\hat{b}_{\mathsf{n}}$, which belongs to a potential eavesdropper. Also, success probability for measurement $\widehat{\mathsf{M}}$ is given by

$$\begin{aligned} P^{\mathsf{PS}} =& \frac{1}{4}\sum_{k=0}^{3}\int \frac{d^2\xi_1}{\pi}\frac{d^2\xi_2}{\pi}\chi_A^{kk}(\xi_1, \xi_2, 0) \\ =& \frac{1}{4}\sum_{k=0}^{3}\zeta_A^{kk}(0) \\ =& \zeta_A^{00}(0), \end{aligned} \tag{5.21}$$

where $\zeta_A^{kl}(0)$ is given by (C.2) in appendix C. This result exactly matches that of the P&M scheme, given in (5.4). We remark that the total success probability is given by $P_{\mathsf{succ}} = 2P^{\mathsf{PS}} = 2\zeta_A^{00}(0)$, which also accounts for the case of D2 clicking and D1 not clicking.

Finally, in order to find a lower bound on the secret key rate, we use the optimality of Gaussian collective attacks in the asymptotic limit for a given CM. Now that the bipartite state between Alice and Bob is known, and given by (5.17), we can work out the first and second order moments in the CM, which turns out to be in the standard symplectic form:

$$V_{AB} = \begin{pmatrix} V_x\mathbb{1}_2 & V_{xy}\sigma_{\mathsf{z}} \\ V_{xy}\sigma_{\mathsf{z}} & V_y\mathbb{1}_2 \end{pmatrix}. \tag{5.22}$$

We derive the closed form expression of the triplet (V_x, V_{xy}, V_y) in appendix C. Note that the obtained CM for vacuum state at the input, i.e., when $\dot{\alpha} = 0$, results in identity CM, i.e., $V_{AB} = \mathbb{1}_2 \otimes \mathbb{1}_2$, as one would expect. Having found the CM, one can then work out a bound on Holevo information using the set of equations given in section 2.2.3. But, before delving into the secret key rate analysis, we would like to make a comment on the CM and correlation shared between Alice and Bob.

Correlation factor

An important feature of the CM in (5.22) is its correlation parameter, which characterizes the amount of correlation between the parties's quadratures upon a successful QS operation. It is defined as $Z_4^{(\mathrm{QS})} = V_{xy}/\sqrt{T}$, where V_{xy} is given in (C.10). Figure 5.3 compares $Z_4^{(\mathrm{QS})}$ in our QS-based system with that of the no-QS setup, Z_4 Leverrier & Grangier [2011], and then compares both with that of the Gaussian modulation case without (Z_{G}) and with ($Z_{\mathrm{G}}^{(\mathrm{NLA})}$) an ideal NLA. In the case of Gaussian modulation without an NLA, instead of $|\Psi\rangle_{01}$, we start with a TMSV state given by $\sqrt{1-\lambda^2}\sum_{n=0}^{\infty}\lambda^n|n\rangle_0|n\rangle_1$, for which the corresponding CM is given by $\begin{pmatrix}(V_A+1)\mathbb{1}_2 & Z_{\mathrm{G}}\sigma_{\mathrm{z}} \\ Z_{\mathrm{G}}\sigma_{\mathrm{z}} & (V_A+1)\mathbb{1}_2\end{pmatrix}$, with $Z_{\mathrm{G}} = \sqrt{V_A^2 + 2V_A}$, where $V_A = 2\lambda^2/(1-\lambda^2)$ is its corresponding modulation variance. The parameter λ would ideally change to $g\lambda$ once one arm of the TMSV state goes through an ideal NLA with gain g Ralph & Lund [2009], Blandino *et al.* [2012]. The corresponding correlation term, $Z_{\mathrm{G}}^{(\mathrm{NLA})}$, can then be calculated by $Z_{\mathrm{G}}^{(\mathrm{NLA})} = \sqrt{(V_A')^2 + 2V_A'}$, where $V_A' = 2g^2\lambda^2/(1-g^2\lambda^2)$.

Figure 5.3 compares the above four correlation parameters as a function of V_A. In the case of the QPSK protocol, $V_A = 2\dot{\alpha}^2$. We can see that $Z_4^{(\mathrm{QS})}$, with $g = 2$, overtakes the two no-NLA curves at a V_A around 0.13. This suggests that the amount of correlation between Alice and Bob signals has been enhanced by the use of a QS. This may imply that higher key generation rates can be obtained in certain regimes of operation. One should, however, note that by increasing V_A, hence $\dot{\alpha}$, we may reduce the success probability of the QS system, and may make the amplified output noisy. Furthermore, by increasing $\dot{\alpha}$, Eve's Gaussian attack would be further away from her optimal attack. Hence, a trade-off involves here. We will discuss this point in our numerical results when we optimize the secret key rate over system parameters. One final interesting point in figure 5.3 is that the correlation term for the ideal NLA is always better than the QS system. This may suggest that the earlier analysis that rely on an ideal NLA may overestimate

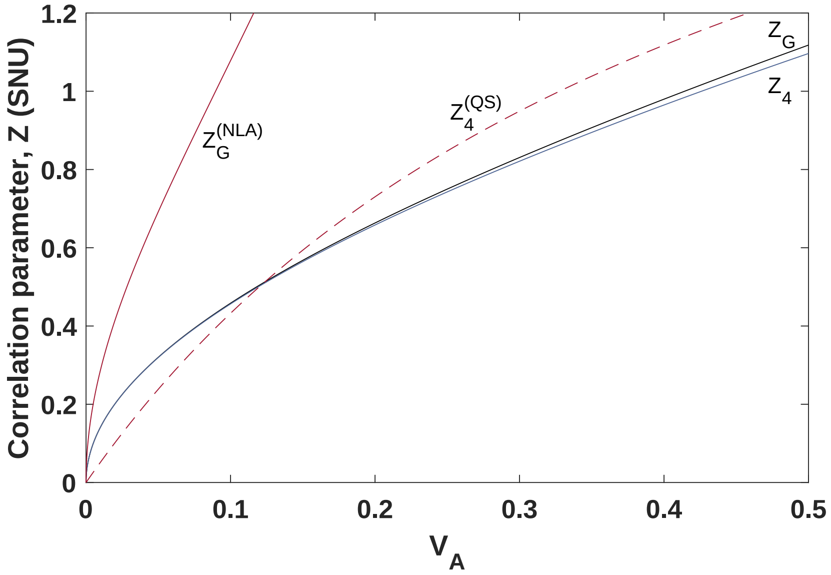

Figure 5.3: Correlation factor for the Gaussian modulation CM (solid black), the four coherent-state constellation without (solid blue) and with (dashed red) a QS with amplification gain $g = 2$. The solid red curve belongs to the TMSV state amplified via an ideal NLA ($g = 2$); see text for more information. Here, the channel is assumed loss-less and without any excess noise.

what can be achieved with a realistic NLA system.

5.4 Numerical results

In this section, we present some numerical results for the secret key rate of our QS-amplified QPSK CV-QKD system and compare it with that of the no-QS protocol, as well as its Gaussian modulated variants. To that end, we solve a dual optimization problem. We find the maximum value for the lower bound in (5.11) by optimizing over $\dot{\alpha}$, which specifies the modulation variance, and the QS parameter g, which specifies the QS amplification gain. In our numerical results, for a channel with length L, we assume that $T = 10^{-\alpha L/10}$, where $\alpha = 0.2$ dB/km is the loss factor for optical fibres. Also, we nominally assume a reconciliation efficiency equal to one and that Bob, upon successful QS events, uses an ideal homodyne detection, with no electronic noise and no loss, to measure the received

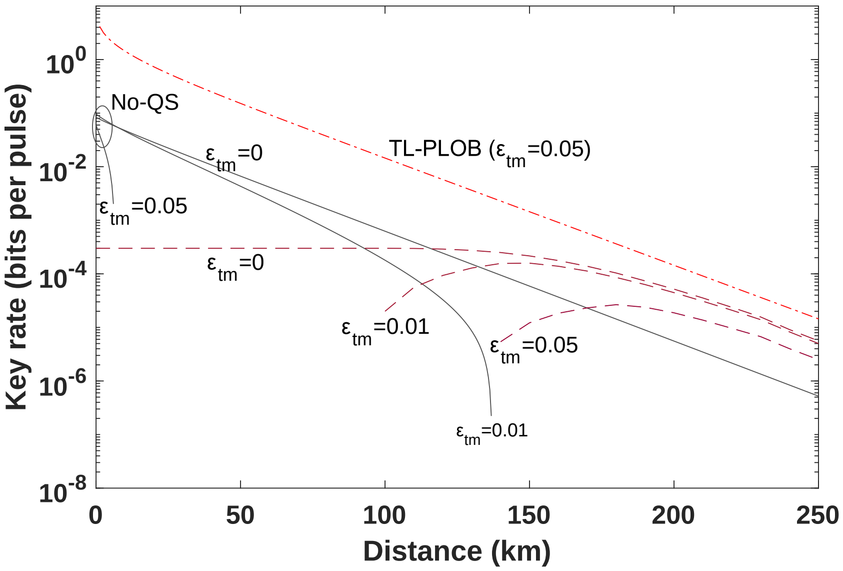

Figure 5.4: Numerical results of the optimized secret key rate for QS-equipped QPSK CV-QKD protocol versus distance (dashed lines), as compared to that of the protocol with no-QS (solid lines). The ultimate thermal-loss PLOB bound is shown at the top.

signals.

Figure 5.4 shows the optimized key rates for the no-QS and QS-equipped QPSK protocols versus distance. We observe that the behaviour of the different curves shown in figure 5.4 is very much akin to that of the Gaussian modulation QS-equipped CV-QKD presented in chapter 4. In particular, the QS-based systems are capable of beating their no-QS counterparts after a certain distance, and considerably increase the maximum security distance achievable by the underlying QKD protocol. The crossover distance at an input excess noise equal to zero and 0.01 SNU is, respectively, around 120 km and 110 km. In the case of $\varepsilon_{\rm tm} = 0.05$, the no-QS system has a very low reach, whereas, by using a QS, the system can now provide positive secret key rates at distances over 140 km. It can also be seen that the QS-based system offers either zero or very low secret key rates at short distances. This, as pointed out in chapter 4, can be because of the additional noise by the QS, especially, for large inputs, which requires us to use much lower values of $\dot{\alpha}$ that would be used in the no-QS system. This could make the signal component of the signal, at short distances, less than the excess noise part, hence resulting in no secure keys.

The opposite effect is seen at long distances where QS-based systems are offering a key rate parallel to the fundamental bounds for secret key generation rate for a thermal-loss channel (labelled by TL-PLOB). This is the bound given in (23) of Pirandola *et al.* [2017] at an equivalent mean thermal photon number, $\bar{\mathsf{n}} = \varepsilon_{\text{tm}}T/(2(1-T))$, to our receiver excess noise (here at $\varepsilon_{\text{tm}} = 0.05$). This extended security distance suggests that once the input to the QS is low enough, which is at long distances, the post-selection offered by the QS can improve the signal-to-noise ratio to a level that positive secret key rates are distillable. We have numerically verified that positive key rates are indeed achievable for $\varepsilon_{\text{tm}} < 0.09$ for the QS-based system.

The QS-equipped discrete modulation system seems to offer more resilience to excess noise and channel loss than its Gaussian modulation counterpart considered in chapter 4. For instance, the maximum tolerable excess noise in the latter case is around 0.06 SNU as compared to 0.09 SNU in the former case. The secret key rate obtained at a high excess noise value of 0.05 SNU is also higher for the discrete modulation versus Gaussian modulation case. This has been shown in figure 5.5, where the secret key rate for both systems, in the presence and absence of a QS, has been shown. This result is, however, counter-intuitive, and must be taken with caution. There is a fundamental difference between the Gaussian modulation and discrete modulation cases in that the latter is not a Gaussian one especially for large values of $\dot{\alpha}$. As shown in figure 5.6, the optimal value of $\dot{\alpha}$ is around 0.7 at $\varepsilon_{\text{tm}} = 0.05$. In our analysis, we have, however, assumed that Eve is restricted to a Gaussian attack, which will become less optimal as the input modulation deviates further from a Gaussian one. What our numerical results would then suggest is that for a Gaussian Eve, it is better to use a non-Gaussian modulation as this would make Eve's attack even less optimal.

If we want to obtain a more realistic account of what a non-restricted Eve could achieve in our system, we should then cap the choice of $\dot{\alpha}$ in our optimization to a value that preserves the Gaussianity of the input signal to some good extent. A suggested cap for $\dot{\alpha}$ is given by Ghorai *et al.* [2019] to be around 0.5. The lower curve in figure 5.5 shows the secret key rate under this constraint, while the corresponding optimal value of g is shown in figure 5.6. It is now clear that the rate obtained for the discrete modulation case, at $\beta = 1$, is lower than

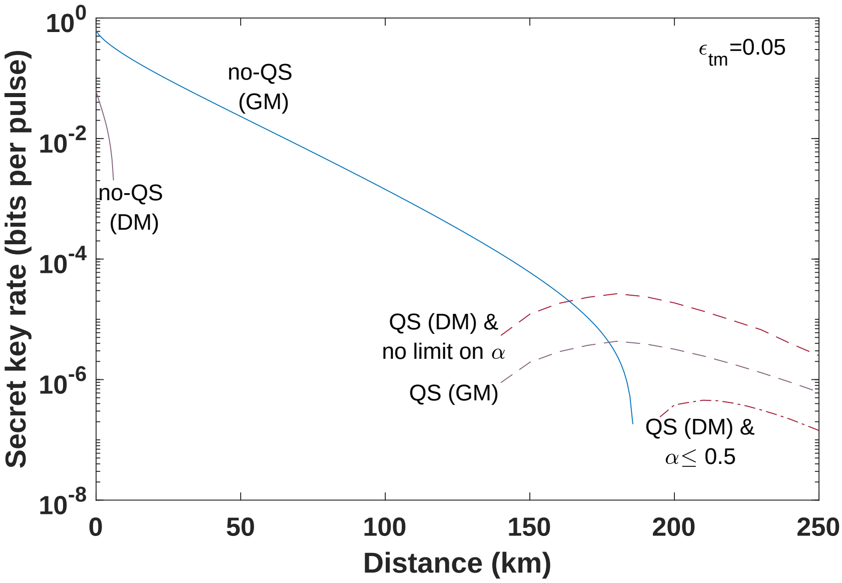

Figure 5.5: Numerical results of the optimized secret key rate for discrete modulation (DM) CV-QKD protocol versus distance, as compared to that of the Gaussian modulated (GM) GG02 protocol with and without a QS at $\varepsilon_{\text{tm}} = 0.05$. The lower curve represents the result of optimized key rate when α is capped at 0.5. The rates are obtained at $\beta = 1$.

that of the Gaussian modulation case. The no-QS Gaussian modulation system will, however, offer no positive key rate for $\beta < 0.98$, which implies that, if one considers the more efficient reconciliation techniques for discrete modulation systems, there would be regimes of operation where the discrete modulation system outperforms the Gaussian modulation case. Note that, as shown in figure 5.6, by capping $\dot{\alpha}$, larger values of gain are needed by the QS to achieve the optimal key rate.

In our optimization, in order to achieve the highest possible rates, we find that values of amplification gain as large as $g = 30$ are required; see figure 5.6. We note, however, that this might not be practically attainable. The reason is that a QS that can offer a large amount of amplification gain, e.g., $g = 30$, requires an imbalanced beam splitter, with $\mu = 1/(g^2 + 1) \approx 0.0011$, which is hard to make, if not impossible.

Finally, we would like to comment on the suitability of quantum scissors in

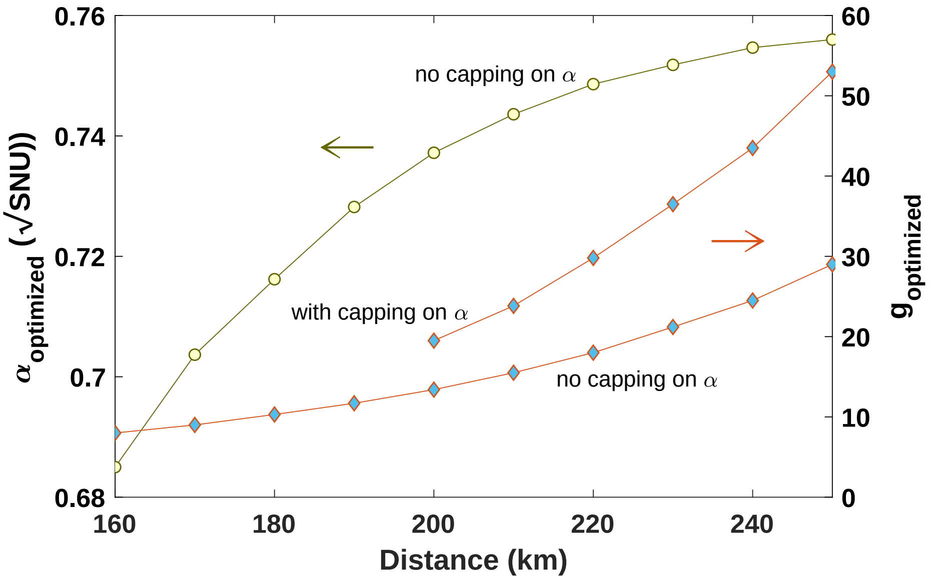

Figure 5.6: Optimized input amplitude (marked by circles) and optimized amplification gain (marked by diamonds) versus channel length at $\varepsilon_{\text{tm}} = 0.05$ with and without a cap (0.5, not shown on the graph) on $\dot{\alpha}$.

CV quantum repeaters (QRs). One of the objectives of calculating the key rate of a QS equipped CV-QKD system was the similarity of the setup to what was proposed, as the main building block, in recent proposals for CV QRs Dias & Ralph [2017], Seshadreesan *et al.* [2018]. Our intuition was that if a realistic QS could not offer any advantage over the no-QS one, then the prospect of a CV QR that relies on such QS devices would also be questionable. Our results suggest that there are regimes of operation that QS-based systems offer some advantage. We are, however, short of a convincing argument that such regimes of operation would be those in which repeater systems could operate as well. In fact, while our results keep the prospect of functioning CV QRs open, they also highlight the importance of considering all noise effects before jumping to any conclusions. Our analysis could then be used to further study the proposed repeater setups and assess how, in practice, they can perform.

5.5 Summary

In this chapter, we studied the performance of a CV-QKD system that used quadrature-phase-shift-keying modulation at the encoder and a certain optical state truncation device, i.e., a quantum scissor (QS), before its homodyne receiver. The objective was to find if and to what extent the use of QS, as a non-deterministic amplifier, could improve the rate behaviour of the system at long distances. We showed that, by optimizing the relevant system parameters, the QS-equipped system could tolerate more excess noise than the no-QS discrete-modulation system, and therefore could reach longer distances at positive values of excess noise. This effect was similar to that of a Gaussian-modulated CV-QKD system, as seen in the previous chapter, but in the discrete-modulation case we observed additional tolerance against excess noise if only Gaussian attacks are considered, or assume lower reconciliation efficiencies for the Gaussian modulation case, as is often the case. This enables us to extend the reach of CV-QKD systems provided that we supplement them with additional devices such as single-photon sources Senellart *et al.* [2017] and single-photon detectors Cahall *et al.* [2017]. This, at first, may sound counterproductive as it takes away some of the practical advantages of CV-QKD systems. But, one should note that these additional equipment are only needed at the receiver end of the link, which, in a practical setup, can represent a shared network node in a quantum network. Moreover, our analysis would specify the range of distances for which the use of a QS could be beneficial. Over shorter distances, one should still use a conventional system. Eventually, QRs are needed to reach arbitrarily long distances, for which the QS-based system studied here serves as a building block.

Chapter 6

Satellite-based continuous-variable quantum key distribution

In this chapter, with the ultimate goal of achieving a long-distance continuous-variable quantum key distribution (CV-QKD) system, we consider an alternative to setups assisted by noiseless linear amplifiers and/or quantum repeaters, that is, satellite-based CV-QKD. Satellite-based CV-QKD links can be part of a global solution to QKD networks Razavi [2018]. In the absence of practical quantum repeaters, fibre-based QKD links are limited to a distance of a few hundred kilometres Zhang *et al.* [2018b]. In contrast, free-space QKD relying on ground-to-satellite, satellite-to-ground, and/or satellite-to-satellite quantum communications links can potentially offer secure key exchange over thousands of kilometres Liao *et al.* [2017a, 2018]. That, however, comes at an additional price for launching and operating satellites, as well as with some restrictions on the achievable key rate and noise sensitivity. This chapter seeks solutions that can enhance the benefits reaped from investing in this technology by looking into relevant realistic threat models that would apply to satellite QKD. Continuous-variable QKD is not the obvious choice when it comes to space communications. The satellite-to-ground loss in typical settings that rely on low-Earth-orbit (LEO) satellites is often over 30 dB, at which CV-QKD systems have a poor performance. Here, we look at the specifics of a satellite link to come up with more realistic models for eavesdropping attacks, based on which new security analysis are developed. The results suggest that under this new restrictive regimes for Eve, CV-QKD can see a considerable boost in its performance, making it a viable potion for QKD in space.

Our main contributions in this chapter

- We model a satellite-to-ground QKD link, by assuming non-ideal links between (i) the sender and the eavesdropper; and (ii) the eavesdropper and the receiver. In this way, we limit Eve's access to Alice and/or Bob stations.
- Based on our model, we introduce several scenarios that we may need to deal with in practice.
- We find bounds on the secret key rate for majority of the scenarios, where we consider both Gaussian and non-Gaussian modulation protocols.
- We show that higher key rates can be achieved as compared to when unrestricted eavesdropping is possible.
- We observe that as Eve's access to the transmitted signal becomes less and less, we approach a classical limit that the legitimate parties can exchange secret keys up to the capacity of the channel connecting them.

6.1 Necessity of a realistic account for satellite-based CV-QKD

Satellite-based QKD has been considered in many theoretical Bonato *et al.* [2009], Moli-Sanchez *et al.* [2009], Meyer-Scott *et al.* [2011], Bourgoin *et al.* [2014], Boone *et al.* [2015], Bedington *et al.* [2017], Hosseinidehaj *et al.* [2019] and experimental Nauerth *et al.* [2013], Wang *et al.* [2013] , Bourgoin *et al.* [2015], Vallone *et al.* [2015] studies. The successful launch of the Chinese QKD satellite in 2017, and the experiments carried out since then Liao *et al.* [2017a,b, 2018], Ren *et al.* [2017], has nevertheless been a game changer in bringing the field into a new exciting development phase while a substantial global effort is directed at finding practical solutions to the wide-scale deployment of QKD systems.

Before the above development phase can be carried out, certain technological challenges must be addressed. For instance, a secure satellite-based QKD system must combat loss and noise effects in the link. Current experimental demonstrations suggest that a typical LEO satellite-to-ground link would suffer around 30-40 dB of loss for a modest-size receiver telescope Liao *et al.* [2017a], and with night operation only in order to minimize the noise. This would imply that DV-QKD protocols may be the most efficient option for distributing keys from satellites to terrestrial stations. Other options, such as CV-QKD, which is known to be more resilient to noise in low-loss regimes, or even entanglement-based or measurement-device-independent QKD, with a satellite as the middle node, are likely to be less practical or efficient. In the latter two cases, whilst we would not need to trust the satellite node, the total loss could exceed 80 dB (unless we use larger telescopes Günthner *et al.* [2017]), which makes these options possibly inefficient and/or expensive, if not infeasible.

We note, however, that the above limitations are partly because of the assumptions made in our security analysis, e.g., that the channel in its entirety is assumed to be under the control of a potential eavesdropper. Whether such an assumption is necessary/realistic in the satellite QKD scenario, which relies on line-of-sight links, needs to be scrutinized. Relaxing this assumption could open up new opportunities that have been discounted, but which, if proved to be viable, could offer additional options for implementation and commercial exploitation.

One of the distinctive features of a satellite link, as compared to a fibre link, is that it is a line-of-sight link; see figure 6.1. While it may not be possible, for a link of around 500 km of length in the LEO case, to fully monitor the channel between Alice and Bob, one can employ monitoring techniques, such as LIDAR, to detect objects of a certain minimum size along the path. In fact, the same system and the corresponding optics that are being used for tracking and acquisition purposes can also be used to detect unwanted objects along the beam. The minimum object size that LIDAR can detect grows with a power four of distance between the object and the LIDAR source. That said, our preliminary calculations suggest that for a 500-km-long satellite link, and for LIDAR used at both Alice and Bob stations, the largest undetected object within the beam width of our LIDAR sources is around a few centimetres wide; see appendix D[1]. This

[1] We credit the information presented in appendix D to Carlo Liorni at Institute für The-

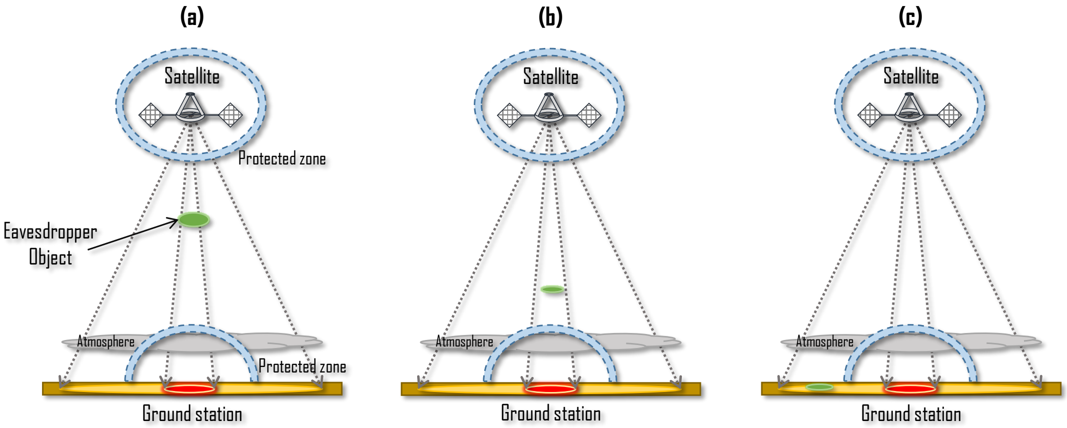

Figure 6.1: Schematic view of a satellite QKD link, where an eavesdropper can arrange an attack between the satellite and ground station. Due to the nature of such a link, the possibility of designing a powerful attack might be restricted. We refer to the explanatory text in section 6.2 to elaborate on scenarios **(a)**-**(c)**.

is important because for any effective eavesdropping activity, Eve requires (i) to somehow collect the signals transmitted by Alice, and/or (ii) to somehow be able to send her own signals towards Bob's receiver. In the satellite scenario, power collection requires telescopes of decent size, and manipulation of Bob's receiver might need powerful laser sources, especially if Eve's source is not fully aligned with Bob's telescope. This implies that the combination of limited size telescopes for Eve and a monitored/protected zone around Alice box could restrict Eve to only receiving a fraction of what Alice has sent. This would be the first departure point from a maximally powerful Eve. In the second case, where Eve cannot replace the channel between herself and Bob with an ideal channel, any resend/hacking attack by Eve will be affected by a lossy channel that the protection zone around receiver would enforce. This could also restrict Eve in implementing her attack scenario.

In the following, we study the security of satellite-based CV-QKD in several settings, where certain assumptions are made about the physical channel between the satellite and the ground station as well as capabilities of Eve in an attack. We classify, in section 6.2, different scenarios that reflect such limitations and model each class with generic models for which new security analyses can be developed.

oretische Physik III, Heinrich Heine Universität, Düsseldorf, Germany.

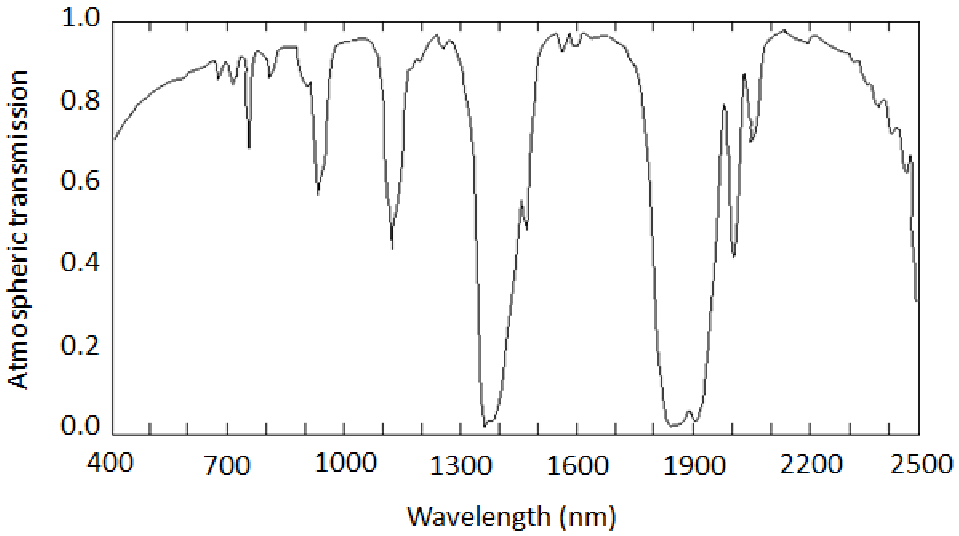

Figure 6.2: Atmospheric windows for space communications.

The rest of the chapter is then devoted to provide lower and/or upper bounds for several regions of interest where Eve's access to Alice's and/or Bob's sites is through lossy channels for CV-QKD protocols.

Atmospheric loss and light windows to/from space

In our everyday life, we see that *visible* light, in the range of wavelengths about 380-740 nm of the electromagnetic spectrum, passes through the Earth's atmosphere. This is why we can see the sun, moon, and stars, at least in a non-cloudy sky. However, not all the light in the electromagnetic spectrum can pass through the atmosphere; see figure 6.2. This is because some portion of the spectrum is absorbed by components of the atmosphere, such as water vapour, oxygen, and carbon dioxide molecules. The atmosphere is then said to be opaque for this class of wavelengths and transparent for, e.g., visible light. In fact, apart from visible light, there are only few other free-space optical communications windows of the electromagnetic spectrum that are open to space. This is a portion of the infrared spectrum band in the interval of roughly 750-2500 nm, as shown in figure 6.2. Indeed, when doing satellite QKD, the absorption band of the spectrum must be avoided.

6.2 Scenario classification for satellite CV-QKD

In this section, we model the restrictions imposed by our detection systems by lossy channels between Alice and Eve, and between Eve and Bob. In particular, we assume that a lossy channel with transmissivity η_{AE} connects Alice to Eve, and that Eve has no access to the signals lost on this channel. Similarly, we assume that every signal sent by Eve to Bob would go through a lossy channel with transmissivity η_{EB}, where neither Eve nor Bob has access to the lost signals on this channel. We investigate how these two restrictions affect the performance of a CV-QKD system run on such a link.

There are different scenarios that one can consider with the above generic restrictions. One possible scenario, shown in figure 6.1(a), is when Eve's telescope is large enough to capture all signals that would end up on Bob's telescope, but too small to capture the entire signal sent by Alice. This case corresponds to $\eta_{AE} < 1$, but possibly with η_{EB} close to one. Another possibility is when Eve's telescope is assumed to be too small to capture the entire signal that would be received by Bob, in which case part of Alice's signal may reach Bob without Eve's intervention; see figure 6.1(b). Finally, another case is shown in figure 6.1(c), when Eve is simply a passive receiver of Alice's signal without sending anything to Bob.

All these cases, and more, can be captured in the diagram shown in figure 6.3. In this diagram, for a simulated/observed total channel transmissivity of η, we have introduced multiple regions and boundaries that could represent the above mentioned scenarios. For instance, region 1, R1, where $\eta_{AE}\eta_{EB} \geq \eta$, corresponds to the case in figure 6.1(a), whereas region 2, R2, for which $\eta_{AE}\eta_{EB} < \eta$, corresponds to the scenario in figure 6.1(b). Cases like that of figure 6.1(c) would correspond to boundary 4, B4, in figure 6.3. The uppermost-right case, with $\eta_{AE} = \eta_{EB} = 1$, represents the typical unrestricted Eve, whereas the lowermost-left case, with $\eta_{AE} = \eta_{EB} = 0$, is a rather benign eavesdropper.

Among the above scenarios, the worst case could correspond to the case where any signals received by Bob has gone through Eve's apparatus. In this case, Eve will have full control over a channel with transmissivity $\eta/(\eta_{AE}\eta_{EB}) < 1$, while Alice and Bob each can be thought of having extended encoder/decoder boxes. In this case, i.e., region R1, we might be able to modify existing security proofs

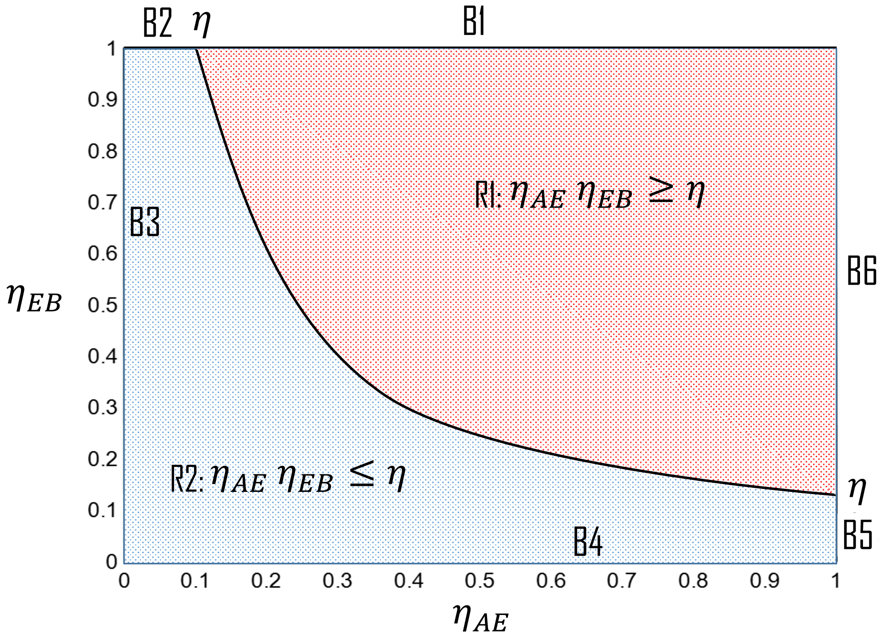

Figure 6.3: Different regions and boundaries of interest. R1 represents the region where $\eta \leq \eta_{AE}\eta_{EB}$. That is, there could be part of the channel with transmissivity $\eta/(\eta_{AE}\eta_{EB}) \leq 1$, which is fully under control of Eve. In R2, $\eta > \eta_{AE}\eta_{EB}$, which implies that there could be part of the signal that reaches Bob without going through Eve. B1–B6 represent boundaries of interest, where B1 and B2 are for the special case of $\eta_{EB} = 1$, in, respectively, regions R1 and R2. For B3, $\eta_{AE} = 0$, whereas in B4, $\eta_{EB} = 0$. Finally, B5 and B6 cover the case of $\eta_{AE} = 1$, in, respectively, regions R2 and R1. The graph is depicted at $\eta = 0.1$.

to obtain the secret key generation rates. Region R2 would then cover scenarios when $\eta > \eta_{AE}\eta_{EB}$. In this region, Eve should either introduce new signals to cover for the difference $\eta - \eta_{AE}\eta_{EB}$, which would be detected by Alice and Bob due to increase in the error rate, or let part of the signal gets to Bob uninterrupted. In the latter case, she can effectively apply her attack only on the part that she has received from Alice. We have also specified six boundaries, B1–B6, in figure 6.3, where each represent a particular case of interest.

Our calculations in appendix D suggest that by using LIDAR systems on both the satellite and ground station, with a reasonable power budget, we can find maximum values for η_{AE} and η_{EB} in the event that the eavesdropping object is undetectable by the LIDAR system. If a certain object is detected by the monitoring system, we can use its estimated size to bound η_{AE} and η_{EB}. It turns out that while, by using LIDAR, η_{AE} can be estimated to be only a few percent, η_{EB} could easily get close to 1. That implies that the most relevant scenarios could be those for which $\eta_{AE} < 1$ and $\eta_{EB} \approx 1$.

Here, our aim is to find bounds on key rate of relevant CV-QKD protocols with Gaussian and discrete modulations of coherent states, discussed in chapter 2, ideally in each region and boundary in figure 6.3, and, if possible, design and study new protocols that capitalize on Eve's imposed restrictions. In all cases, the satellite is assumed to have the QKD encoder and the terrestrial station would decode the received signals. In the following, we study the operation of CV-QKD protocols under such different scenarios.

6.3 Restricted Eve's access to encoder outputs

In this section, we study Gaussian- and discrete-modulated CV-QKD protocols, where Eve's access to the signals sent by Alice is restricted. We model this scenario via a beam splitter with transmissivity η_{AE}, as shown in figure 6.4(a). That is, the channel between Alice and Eve is no longer lossless. As earlier discussed, when Eve is restricted to receive only a fraction of the incoming light from Alice, we might expect to gain higher key rates. Therefore, in the reverse reconciliation case, the information that Alice and Bob can share could be higher than that of Eve and Bob.

Here, the implicit assumption is that in the optimal collective Gaussian attack, Eve only takes control over a channel with transmissivity $\eta/\eta_{AE} \leq 1$, where η is the total transmittance of the Alice-Bob link. As long as the channel is assumed Gaussian, the best Eve can do is to apply an entangling cloner Navascués & Acín [2005] to the part of the channel she has access to, i.e., the $A'B$ link in figure 6.5. In this way, Eve would attach herself to $A'B$, hiding behind the excess noise observed by Alice and Bob. In the entangling cloner, Eve would overlap the signal with one leg of her two-mode squeezed vacuum (TMSV) state, characterized by Z as its variance, sends one of the resultant outputs to Bob and stores the other in her quantum memories (QMs). The first problem that the restriction $\eta_{AE} < 1$ imposes on Eve is that she would now require more intense TMSV states, with larger Zs, to mimic the channel, in order to produce the same

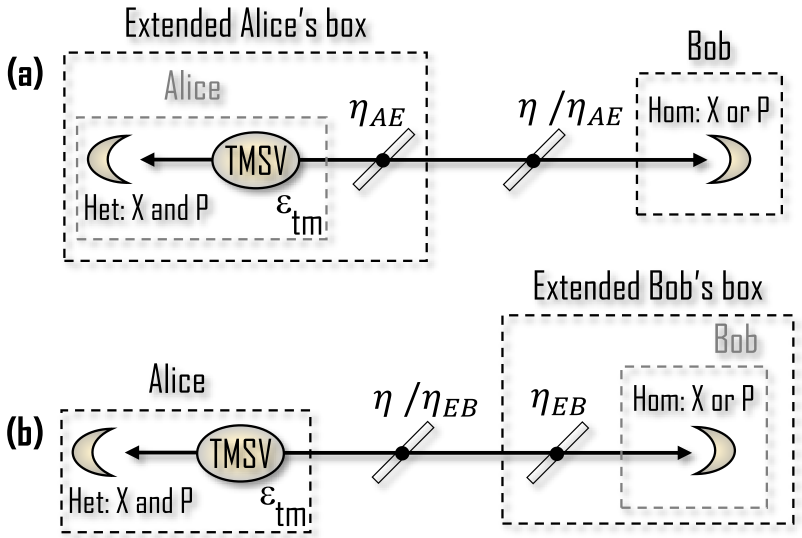

Figure 6.4: Schematic view of a realistic satellite-to-ground entanglement-based CV-QKD link, with Eve's limited access to the **(a)** encoder and **(b)** decoder modules. Alice's and Bob's modules each can be seen as an extended encoder/decoder boxes, see text for details. This model is valid only for $\eta/\eta_{AE}\eta_{EB} < 1$.

amount of excess noise as before. In fact, we show that at a fixed input excess noise, $\varepsilon_{\mathsf{tm}}$, and channel loss, η, we have

$$Z = 1 + \frac{\eta\varepsilon_{\mathsf{tm}}}{1 - \eta/\eta_{AE}}. \tag{6.1}$$

In addition, as discussed, Eve can simulate only the part of the channel she has control over. Input excess noise for this part of the channel, starting at point A' in figure 6.5, should be $\eta_{AE}\varepsilon_{\mathsf{tm}}$ to match the observed value of $\varepsilon_{\mathsf{tm}}$ at Alice's box. Also, given that the signal that leaves Alice box has been attenuated by η_{AE} before reaching point A', Eve can only manipulate a channel of transmissivity η/η_{AE}. Thus, in order to estimate the key rate for the limited Eve in figure 6.4(a), we would do the following transformation in the secret key rate recipe, given in chapter 2: $\eta \to \eta/\eta_{AE}$ and $\varepsilon_{\mathsf{tm}} \to \eta_{AE}\varepsilon_{\mathsf{tm}}$. Note that the obtained key rates are valid only when $\eta_{AE} \geq \eta$.

Some numerical results are plotted in figure 6.6 for the GG02 protocol. We assume modulation variance $V_A = 4$ SNU, reconciliation efficiency $\beta = 0.95$, efficiency of Bob's homodyning $\eta_{\mathsf{D}} = 0.6$, and electronic noise at his side $\nu_{\mathsf{elec}} =$

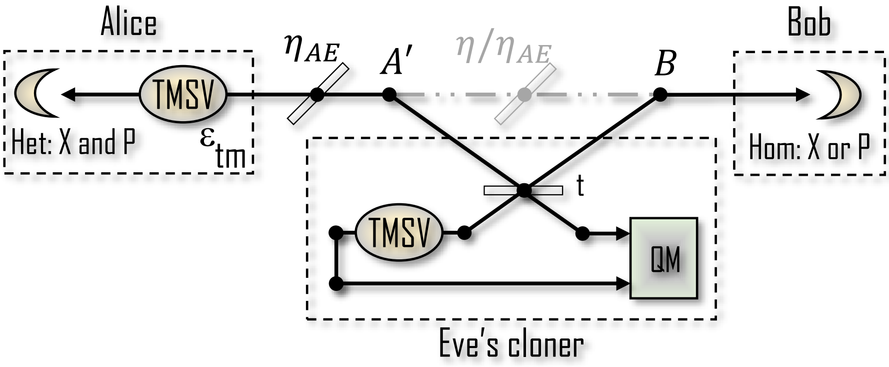

Figure 6.5: Quantum entangling cloner, using which Eve simulates the second part of the channel she has control over. Transmissivity of this part is given by η/η_{AE}, with excess noise $\eta_{AE}\varepsilon_{\text{tm}}$ at its input, A'.

0.01 SNU. In figure 6.6(a), we plot the key rate versus η for different values of η_{AE}. It is seen that the smaller fraction of Alice signals reach Eve's realm, i.e., the smaller η_{AE}, the larger key rates Alice and Bob can share. In other words, the lower η_{AE} is, the higher channel losses can be tolerated by our CV-QKD system. Figure 6.6(b) shows secret key rates versus η_{AE} for a total of 40 dB of channel loss, at several excess noise values. Note that, at $\varepsilon_{\text{tm}} = 0.1$ SNU, the parties cannot extract any key rate, unless Eve receives signals that have undergone nearly 0.4 or more loss. This indicates higher resilience to noise when η_{AE} restriction is imposed on Eve. We also mention that the results in figure 6.6(b) are not valid for $\eta_{AE} < 10^{-4}$, where our assumption $\eta/\eta_{AE} < 1$ is broken.

We have similarly found secret key rates for the discrete-modulated CV-QKD protocol Leverrier & Grangier [2009]. Our numerical results in figure 6.7 show similar trends of improvement in key rates when a non-ideal channel is connecting Alice to Eve. Comparing to the Gaussian-modulated GG02, in order to obtain any key rate advantage, Eve should be more restricted. This indicates that the advantage becomes clear for smaller values of η_{AE} (assuming other parameters unchanged). This is partly because of the security proof limitations of the discrete modulation protocol Leverrier & Grangier [2011]. Using more advanced transmitted techniques one may be able to get around this problem. Figure 6.7(b) shows key rate versus η_{AE} at a fixed 40 dB channel loss and several values of excess noise. We observe that at $\varepsilon_{\text{tm}} = 0.1$ SNU, we need $\eta_{AE} < 0.09$ to generate

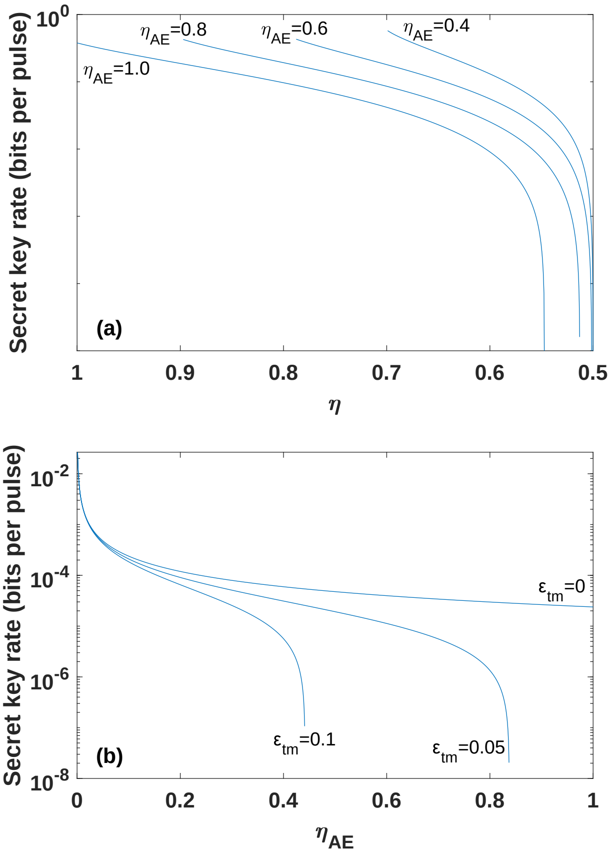

Figure 6.6: Gaussian-modulated GG02 protocol at $\eta_{EB} = 1$. **(a)** Key rates versus distance for different values of η_{AE} and 0.1 SNU excess noise. **(b)** The key rate versus η_{AE} for a fixed channel loss of 40 dB. The parameters $V_A = 4$ SNU, $\beta = 0.95$, $\eta_\mathsf{D} = 0.6$, and $\nu_\mathsf{elec} = 0.01$ SNU are used in the plots.

positive key rates. The rate rapidly grows below this threshold value. Here again, the results are valid only for $\eta_{AE} > 10^{-4}$.

6.4 Restricted Eve's access to decoder inputs

In this section, we study Gaussian- and discrete-modulated CV-QKD protocols, where Eve is restricted to transmit her own signals towards Bob's receiver. By considering a similar scenario, we model this case via a beam splitter with transmissivity η_{EB}, as shown in figure 6.4(b). In other words, we restrict Eve's power

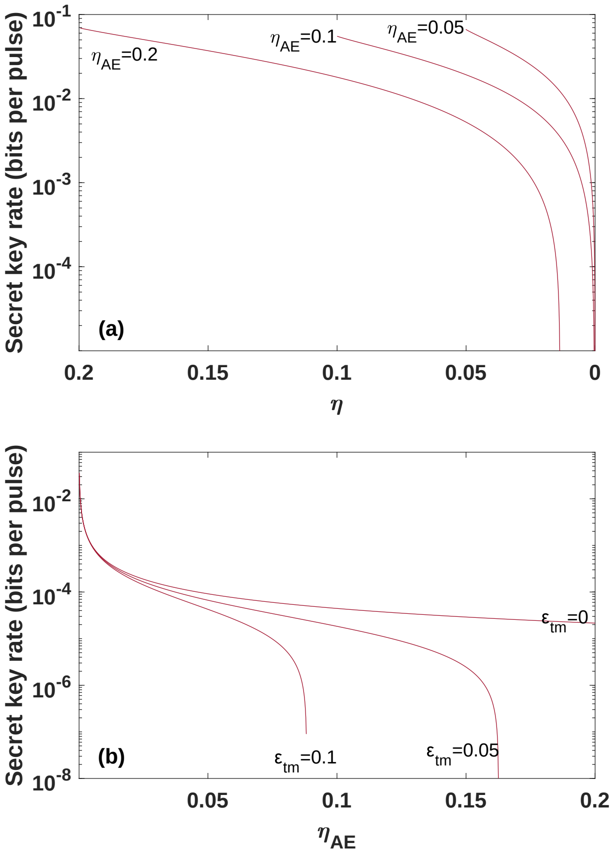

Figure 6.7: Discrete-modulated GG02 protocol at $\eta_{EB} = 1$. **(a)** Key rates for different values of η_{AE} and 0.1 SNU channel excess noise. **(b)** The key rate versus η_{AE} for a fixed channel loss of 40 dB. The parameters $\beta = 0.95$, $\eta_{\mathsf{D}} = 0.6$, and $\nu_{\mathsf{elec}} = 0.01$ SNU are used in the plots.

by considering a non-ideal channel between her and Bob (we assume that Eve has no access to the outputs of η_{EB}). Therefore, in a sense, we have an expanded Bob's box, so that the loss occurred by η_{EB} can be seen as part of an imperfect homodyne detection; hence, it can be assumed trusted. It is worth mentioning that it is shown that trusted noise at the receiver, as well as the transmitter side, can in fact improve the key rate of a CV-QKD protocol with reverse reconciliation Usenko & Filip [2016].

Here, we compute the secret key rate for the restricted Eve in figure 6.4(b). By giving a similar reasoning to that of section 6.3, we need to do $\eta \rightarrow \eta/\eta_{EB}$

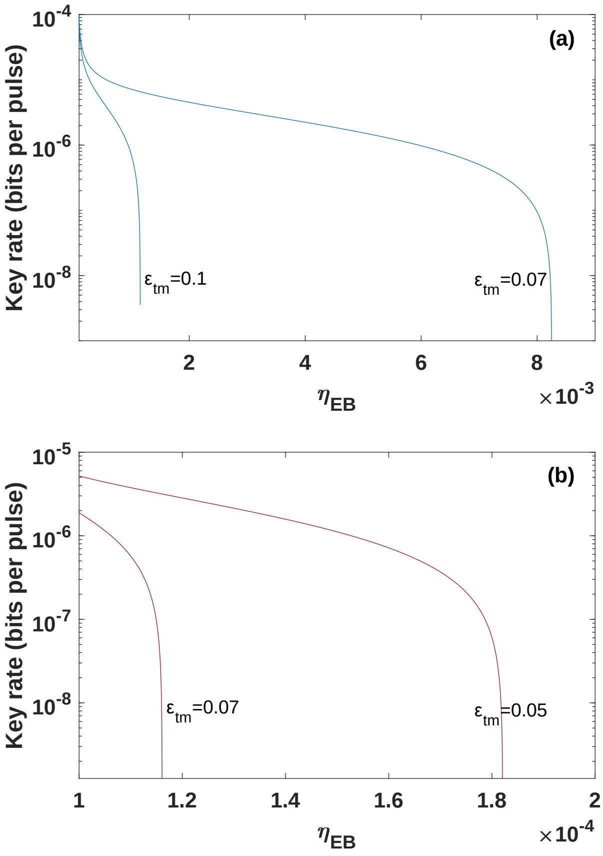

Figure 6.8: Satellite CV-QKD secret key rates with restricted Eve's access to decoder input versus η_{EB} for fixed channel loss of 40 dB for **(a)** Gaussian-modulated and **(b)** discrete-modulated protocols. The parameters $\beta = 0.95$, $\eta_{\mathsf{D}} = 0.6$, and $\nu_{\mathsf{elec}} = 0.01$ SNU and $\eta_{AE} = 1$ are used in the plots.

and $\eta_{\mathsf{D}} \to \eta_{EB}\eta_{\mathsf{D}}$, where detection noise is now assumed to be composed of two terms (note that $\varepsilon_{\mathsf{tm}}$ does not get modified since at the entrance of Eve's realm it has not changed).

Numerical results are plotted in figure 6.8 for both Gaussian- and discrete-modulated GG02 protocols, assuming a channel with 40 dB of loss. Here, as well, the outcomes are valid only for the values of η_{EB} where $\eta/\eta_{EB} \leq 1$ holds. In contrast to η_{AE}, in both cases, η_{EB} should take very small values (being on the order of the channel loss, 40 dB) in order to let the parties exchange secret bits. The reason is that in this case Eve has "full" access to Alice's signals; hence, she can apply a more powerful attack than that of η_{AE}-restricted.

6.5 Extending regimes of operation

So far, our analysis works only for $\eta < \eta_{AE}\eta_{EB}$, so that we can cover only the region R1 of the $\eta_{AE} - \eta_{EB}$ map in figure 6.3. Although the above analysis can cover a relatively vast area of operation in a real-world experiment, one can study some extreme cases, including the boundaries B2 and B3, in more detail. In these cases, $\eta_{AE} < \eta$, which means that the signals that Eve receives many not contain much information about Alice's signal. It may then make sense to use direct reconciliation (DR) to extract secret keys. According to (2.36),

$$R_{\mathsf{DR}} = \beta I(\mathcal{X}_A : \mathcal{X}_B) - \chi_{AE}. \tag{6.2}$$

The mutual information, $I(\mathcal{X}_A : \mathcal{X}_B)$, is an observable in an experiment. Hence we simulate its value by assuming that the channel between Alice and Bob is a pure-loss channel as shown in figure 6.9(a). $I(\mathcal{X}_A : \mathcal{X}_B)$ is then given by (2.46) for this channel that is assumed inaccessible to Eve. This channel is characterized by transmissivity η and excess noise $\varepsilon_{\mathsf{tm}}$.

For the Holevo information, χ_{AE}, we consider a channel characterized by transmissivity η_{AE}, shown in figure 6.9(b), and the same excess noise at Alice's side, $\varepsilon_{\mathsf{tm}}$. We then use the definition of Holevo information in the DR case:

$$\chi_{AE} = H_{\mathrm{vN}}(\hat{\rho}_E) - H_{\mathrm{vN}}(\hat{\rho}_{E|A}), \tag{6.3}$$

where $H_{\mathrm{vN}}(\hat{\rho}_E)$ is von Neumann entropy of Eve's state, which is a thermal state with variance $V_E = \eta_{AE}(V + \varepsilon_{\mathsf{tm}}) + (1 - \eta_{AE})$, and $H_{\mathrm{vN}}(\hat{\rho}_{E|A})$ is Eve's state conditional on Alice's measurement.

The term $H_{\mathrm{vN}}(\hat{\rho}_E)$ is a function of symplectic eigenvalues of $\hat{\rho}_E$; see sections 2.1 for more detail. We then use the fact that the only symplectic eigenvalue of a single-mode thermal state is indeed its variance, i.e., $\Lambda_1 = V_E$. Hence,

$$H_{\mathrm{vN}}(\hat{\rho}_E) = g(V_E), \tag{6.4}$$

where $g(x) = (\frac{x+1}{2})\log_2(\frac{x+1}{2}) - (\frac{x-1}{2})\log_2(\frac{x-1}{2})$.

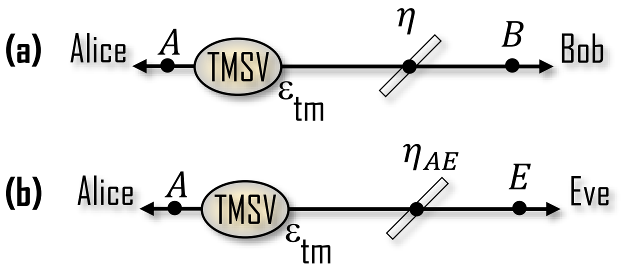

Figure 6.9: Schematic of the proposed model for the case where $\eta_{AE} < \eta$.

Similarly, the term $H_{\text{vN}}(\hat{\rho}_{E|A})$ is a function of conditional symplectic eigenvalues of $\hat{\rho}_E$. For that we need the eigenvalues of the conditional CM. Having that the covariance matrix of Alice-Eve link is as follows

$$V_{AE} = \begin{pmatrix} V\mathbb{1}_2 & \sqrt{\eta_{AE}(V^2-1)}\,\sigma_{\mathrm{z}} \\ \sqrt{\eta_{AE}(V^2-1)}\,\sigma_{\mathrm{z}} & V_E\mathbb{1}_2 \end{pmatrix}, \tag{6.5}$$

the conditional covariance matrix can be calculated from (2.42), whose eigenvalue is given by $\Lambda_{\text{cond}} = \sqrt{V_E - \frac{\eta_{AE}(V^2-1)}{V}}$.

Therefore, an upper bound on χ_{AE} can be calculated from the following

$$\chi_{AE} \leq g(\Lambda_1) - g(\Lambda cond). \tag{6.6}$$

Figure 6.10 shows the key rate versus η_{AE} for an Alice-Bob channel with fixed 40 dB loss. In the case where η_{AE} is strictly zero, i.e., Eve receives no signal at all, she can do no better than a random guesser. Theoretically speaking, she can apply her quantum entangling cloner in figure 6.5 on the small signal coming from Alice. But, what Eve does by influencing Bob's input/measurement outcomes would effectively translate to excess noise at Alice's side, where the key is decided. As such, Eve would still obtain no information about Alice's key, and the Alice-Bob channel reduces to a "classical" one, whose key rate is given by $R_{\text{DR}} = \beta I(\mathcal{X}_A : \mathcal{X}_B)$ (note that here we use direct reconciliation, where, for $\eta_{AE} = 0$, Eve obtains no information). It this case, the key rate in our simulated case of figure 6.9(a) goes to infinity at the asymptotic limit $V_A \to \infty$; however, the growing happens very slowly (e.g., for a variance as large as $V_A = 10^{20}$, the key rate is only about 25).

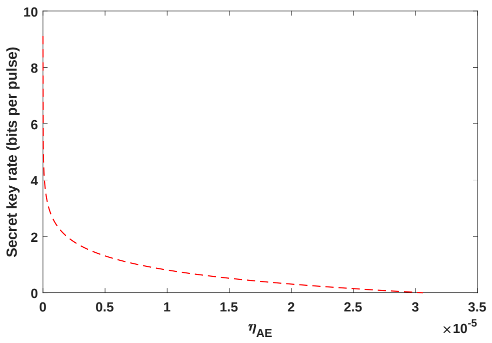

Figure 6.10: Key rate at boundaries B2 and B3 for the model in figure 6.9 for a fixed channel loss of 40 dB. The parameters $\varepsilon_{\mathsf{tm}} = 0.1$ SNU, $\beta = 0.95$, $\eta_{\mathsf{D}} = 0.6$, and $\nu_{\mathsf{elec}} = 0.01$ SNU are used in the plot.

6.6 Summary

In summary, we discussed a real-world threat model most relevant to satellite-based CV-QKD protocols. We relaxed the rather strong assumptions on the eavesdropper's unrestricted capabilities in receiving and re-transmitting QKD signals. Our analysis showed that this could in fact be the case for low-Earth-orbit satellites, which was recently exploited in the Chinese Misius QKD mission. Based on eavesdropper's restrictions in collecting and re-sending light, we classified several possible scenarios, for many of which we bounded secret key rates. We showed that, in all cases, restricting the eavesdropper's power can increase the key rate, as one would expect. Moreover, we highlighted that as Eve's access to the sent signals becomes less and less, we approach a classical limit that Alice and Bob can exchange secret keys up to the channel capacity connecting them.

Chapter 7

Conclusions and future work

Notwithstanding the immense impact of the communication technology on our lives since the mid-twentieth century, security of information is still a big challenge. In fact, powerful eavesdroppers can compromise the secrecy of data since most of the (classical) cryptographic methods rely on computational complexity, for which a security proof does not exist. Hence, in order to achieve absolute data security, we need a rather strong cryptographic scheme that can provide secure communication and/or secure key distribution.

During the last three decades, several communications and key distribution techniques, which relied on the fundamental quantum physics principals, have been proposed theoretically and examined experimentally. Such promising schemes offer unconditional security as a result of laws of quantum mechanics. Luckily, they can be implemented with the current optical technologies.

In general, quantum key distribution (QKD) schemes are classified into two main categories, namely, discrete-variable QKD (DV-QKD) and continuous-variable QKD (CV-QKD), both of which have been studied extensively. Although DV-QKD has its own advantages, CV-QKD schemes are more compatible with the current optical network equipment. However, they do not efficiently support secure communications over long distances. This restriction may be surpassed by using continuous-variable quantum repeaters (CV QRs). The integration of CV-QKD and CV QR protocols has not yet been well studied. In fact, the practicality of the implementation would be a great challenge due to the probabilistic nature of the noiseless linear amplifiers (NLAs), which may be needed at the heart of

CV QRs.

In this thesis, we studied the performance of a CV-QKD scheme running over the building-block of CV QR proposed by Dias & Ralph [2017].The secret key rate of a CV-QKD protocol, when an ideal NLA is used just before the receiver, is evaluated in Blandino *et al.* [2012]. The results indicated an increase in the secret key rates showing that, in principle, NLAs can be useful in CV-QKD. We, however, worked out the secret key rate for a realistic NLA device by replacing it with a quantum scissor (QS). We found the achievable bounds on key rate of the Gaussian-modulated (GG02) and a specific discrete-modulation (quadrature-phase-shift-keying) CV-QKD protocols, which are functions of both amplification gain and modulation variance of the sender's states. By optimizing over system parameters, we could enhance the secret key rates; hence, it turned out that the secure distance could, in principle, be increased via QSs.

Using QRs and NLAs is not the only way that could make a global QKD network viable. In fact, satellites that are equipped with QKD transmitters/receivers can also help. The second part of this thesis was devoted to satellite-based CV-QKD systems. Because of the nature of a satellite-to-ground and/or ground-to-satellite links, which can be monitored by means of RADAR or LIDAR systems, we were able to consider more realistic eavesdropping scenarios. That includes eavesdroppers who are restricted in collecting light and/or re-sending optical signals. By proposing proper models, we then showed that such limitations on the eavesdropper's power would increase the secret key rates of a satellite-to-ground CV-QKD protocol. In fact, we showed that one could benefit from CV-QKD in certain regimes that were not possible via direct strict security assumptions.

Future work: Quantum-repeater-based CV-QKD

The research conducted here can be further extended in several directions. Our study would, in particular, be highly relevant to analysing the performance of recently proposed continuous-variable quantum repeater systems in Dias & Ralph [2017], which rely on a similar building block as we studied in this work. In their proposal, dual homodyne detections are used to connect different blocks in the system. Considering the sensitivity to the excess noise in each leg of the system, it would be interesting to find out the regimes of operation in which a multi-hop CV repeater can be used for QKD purposes. One can compare the obtained key rates in this case with the already known benchmarks for the repeaterless links, i.e., the PLOB bound Pirandola *et al.* [2017], as well as multi-node repeater setups Pirandola [2019].

Another possible avenue for future work is to find better NLA schemes than QSs. In fact, an alternative to NLAs/QSs exists that works based on comparing the input coherent state with a known coherent state; hence, called quantum comparison amplifier Eleftheriadou *et al.* [2013], Donaldson *et al.* [2015]. Such a noiseless amplifier is non-deterministic; however, it does not need quantum resources, such as single photon sources. Especially, since a quantum comparison amplifier can only amplify states that are chosen from a pre-known finite set of coherent states, it can possibly be the better choice for a discrete-modulation protocol, where the number of transmitted coherent states is finite.

When it comes to studying QR-assisted CV-QKD, in particular, and QKD protocols, in general, one may face a cumbersome hierarchical structure of mathematical equations that are hard to solve exactly. In order to do a reliable key rate analysis, one possible research path that we suggest is to use numerical techniques Ghorai *et al.* [2019], Lin *et al.* [2019] to alleviate the analysis, which could have been otherwise impossible.

Future work: Satellite-based CV-QKD

Our theoretical model for satellite-based QKD, when the eavesdropper's capabilities are limited, could benefit from further investigation in several directions. As discussed in chapter 6, we did not cover all possible scenarios in a realistic satellite-based CV-QKD. For instance, region R2 in figure 6.3 can benefit from more detailed analysis to provide us with relevant lower/upper bounds on the key rate. Numerical techniques for rate analysis could also be tried and implemented. Also, for the wiretap channel, boundary B4, where Eve can (partially) collect light but she is unable to re-transmit signals, one can propose and study a more explicit model (some attempts have been made in Pan *et al.* [2019]). Such a model could result in a tighter bound on the key rate.

Another direction for this project would be to consider other restrictions that are realistic in the satellite setting. For instance, the current analysis assumes that Eve is capable of aligning her satellite with that of Alice, while being in a different orbit. This may not be technologically easy to achieve, which opens another avenue for investigation. In the end, the combination of physical layer security assumptions with that of QKD is a less explored territory, which could be expanded to all sorts of QKD protocols and implementations. This can produce a range of products with different pricing and performance and may prove crucial in the commercial success of QKD.

Appendix A

Conditional output state $\hat{\omega}_{\text{out}}^{\mathsf{PS}}(X_A)$

In order to find the conditional output state when Alice has used an X quadrature value of X_A, we start with the input state in (3.9), and take an average over P_A with the input Gaussian distribution of $f_{\mathcal{P}_A}(P_A) = e^{-\frac{P_A^2}{V_A/2}}/\sqrt{\pi V_A/2}$. As a result, the output characteristic function in (3.11) will also be averaged out and result in the following output state:

$$\hat{\omega}_{\text{out}}^{\mathsf{PS}}(X_A) = \omega_{00}(X_A)|0\rangle_{\hat{b}_3}\langle 0| + \omega_{01}(X_A)|0\rangle_{\hat{b}_3}\langle 1| + \omega_{10}(X_A)|1\rangle_{\hat{b}_3}\langle 0| + \omega_{11}(X_A)|1\rangle_{\hat{b}_3}\langle 1|, \tag{A.1}$$

where

$$\begin{cases} \omega_{00}(X_A) = \frac{\widetilde{\omega}_{00}(X_A)}{P_c^{\mathsf{PS}}(X_A)} \\ \omega_{01}(X_A) = \omega_{10}^*(X_A) = \frac{\widetilde{\omega}_{01}(X_A)}{P_c^{\mathsf{PS}}(X_A)} \\ \omega_{11}(X_A) = \frac{\widetilde{\omega}_{11}(X_A)}{P_c^{\mathsf{PS}}(X_A)}, \end{cases} \tag{A.2}$$

with

$$\begin{cases} \widetilde{\omega}_{00}(X_A) = \frac{8F_1(2F_1+1)^2+TV_A(8F_1^2+6F_1+1)+2T(TV_A+4F_1+2)X_A^2}{(g^2+1)(2F_1+1)^{5/2}(TV_A+4F_1+2)^{3/2}} \\ \qquad\qquad \times\sqrt{2}\, e^{-\frac{TX_A^2}{2F_1+1}} \\ \widetilde{\omega}_{01}(X_A) = -\frac{2g\sqrt{2T}X_A}{(g^2+1)(2F_1+1)^{3/2}\sqrt{TV_A+4F_1+2}} e^{-\frac{TX_A^2}{2F_1+1}} \\ \widetilde{\omega}_{11}(X_A) = \frac{g^2}{g^2+1}\left(\frac{2\sqrt{2}\, e^{-\frac{TX_A^2}{2F_1+1}}}{\sqrt{(2F_1+1)(TV_A+4F_1+2)}} - \frac{e^{-\frac{TX_A^2}{2F_1}}}{\sqrt{F_1(TV_A+4F_1)}}\right), \end{cases} \tag{A.3}$$

and $P_c^{\mathsf{PS}}(X_A) = \widetilde{\omega}_{00}(X_A) + \widetilde{\omega}_{11}(X_A)$.

Appendix B

Parameters of the covariance matrix elements (Gaussian modulation system)

We here work out the covariance matrix to the bipartite post-selected state $\hat{\rho}_{03}^{\mathsf{PS}}$ given in (3.31). In doing so, we need to work out the triplet (V_x, V_{xy}, V_y) of the corresponding covariance matrix as follows. By definition, assuming that $\hat{X}_0$ represents the X quadrature of mode $\hat{a}_0$, we have

$$V_x = \langle \hat{X}_0^2 \rangle_{\hat{\rho}_{03}} = \frac{\langle \hat{X}_0^2 \rangle_{\hat{\varrho}_{03}}}{P_{\mathrm{EB}}^{\mathsf{PS}}} = \frac{\mathrm{tr}(\hat{\varrho}_{03} \hat{X}_0^2)}{P_{\mathrm{EB}}^{\mathsf{PS}}}, \tag{B.1}$$

where

$$\begin{aligned} \mathrm{tr}(\hat{\varrho}_{03} \hat{X}_0^2) =& \int \frac{d^2\xi_0}{\pi} \frac{d^2\xi_3}{\pi} \widetilde{\chi}_A(\xi_0, \xi_3) \\ & \times \mathrm{tr}[\hat{X}_0^2 \hat{D}_N(\hat{a}_0, \xi_0)] \times \mathrm{tr}[\hat{D}_N(\hat{b}_3, \xi_3)] \\ =& \int \frac{d^2\xi_0}{\pi} \widetilde{\chi}_A(\xi_0, 0) \times \mathrm{tr}(\hat{D}_N(\hat{a}_0, \xi_0) \hat{X}_0^2), \end{aligned} \tag{B.2}$$

with $\widetilde{\chi}_A(\xi_0, \xi_3)$ given in (3.33).

Assuming that $\xi_0 = x + iy$, we can show that $\mathrm{tr}(\hat{D}_N(\hat{a}_0, \xi_0)\hat{X}_0^2) = \pi\delta^2(\xi_0) + 2\pi y \delta(x) \frac{d}{dy}\delta(y) - \pi\delta(x)\frac{d^2}{dy^2}\delta(y)$; thus,

$$\mathrm{tr}(\hat{\varrho}_{03} \hat{X}_0^2) = -\, \widetilde{\chi}_A(0,0) - \frac{d^2}{dy^2} \widetilde{\chi}_A(0, y, \xi_3 = 0)\Big|_{y=0}, \tag{B.3}$$

where we made use of the identity $\int dz f(z)\frac{d}{dz}\delta(z) = -\int dz \frac{d}{dz}f(z)\delta(z)$. Therefore,

$$V_x = -1 - \frac{\frac{d^2}{dy^2}\widetilde{\chi}_A(0, y, \xi_3 = 0)\Big|_{y=0}}{\widetilde{\chi}_A(0, 0)}. \tag{B.4}$$

In a similar way, assuming $\xi_0 = x + iy$ and $\xi_3 = u + iv$, we show that

$$V_y = \frac{\mathrm{tr}(\hat{\varrho}_{03}\hat{X}_3^2)}{\widetilde{\chi}_A(0, 0)} = -1 - \frac{\frac{d^2}{dv^2}\widetilde{\chi}_A(\xi_0 = 0, 0, v)\Big|_{v=0}}{\widetilde{\chi}_A(0, 0)} \tag{B.5}$$

and

$$V_{xy} = \frac{\mathrm{tr}(\hat{\varrho}_{03}\hat{X}_0\hat{X}_3)}{\widetilde{\chi}_A(0, 0)} = \frac{\frac{d}{dv}\left[\frac{d}{dy}\widetilde{\chi}_A(0, y, 0, v)\Big|_{y=0}\right]\Big|_{v=0}}{\widetilde{\chi}_A(0, 0)}. \tag{B.6}$$

Having the integrals in (3.33) taken, we are able to calculate the triplet (V_x, V_{xy}, V_y), thus, the covariance matrix. Using MAPLE, we obtain the closed form expressions as summarized in (4.11).

Appendix C

Parameters of the covariance matrix (non-Gaussian modulated system)

In this appendix, we calculate the triplet elements that quantifies the covariance matrix of our discrete modulation QS system, given in (5.22).

C.1 Variance at Alice's side (V_x)

By definition, and using the bipartite state in (5.17), we have:

$$V_x = \mathrm{tr}(\hat{\rho}_{03}\hat{X}_0^2) = \frac{1}{4P^{\mathsf{PS}}}\sum_{k=0}^{3}\sum_{l=0}^{3} G_{kl}H_{kl}, \tag{C.1}$$

where $\hat{X}_0 = \hat{a}_0 + \hat{a}_0^\dagger$, corresponding to mode $\hat{a}_0$, in figure 5.2, $G_{kl} := \mathrm{tr}(|\psi_k\rangle_0\langle\psi_l|\hat{X}_0^2)$ and $H_{kl} := \mathrm{tr}(\hat{\Omega}_3^{kl}) = \zeta_A^{kl}(0)$. We then find that:

$$\begin{aligned} H_{kl} &= \zeta_A^{kl}(0) = a_{kl}e^{-\frac{T\alpha_k\alpha_l^*}{2F+1}} - \frac{1-\mu}{2F}e^{-\frac{T\alpha_k\alpha_l^*}{2F}} \\ a_{kl} &= \frac{2}{(2F+1)^3}\Big((2F+1)^2 - \mu(2F+1) + \mu T\alpha_k\alpha_l^*\Big). \end{aligned} \tag{C.2}$$

One can then use the set of identities in (C.12) to work out the following expression:

$$\begin{aligned}V_x =&1+\frac{\dot{\alpha}^2}{\zeta_A^{00}(0)}\Big(\delta_1\Big[-A\sinh\Big(\frac{T\dot{\alpha}^2}{2F+1}\Big)+B\cosh\Big(\frac{T\dot{\alpha}^2}{2F+1}\Big)+C\sinh\Big(\frac{T\dot{\alpha}^2}{2F}\Big)\Big]\\&+\delta_2\Big[A\cosh\Big(\frac{T\dot{\alpha}^2}{2F+1}\Big)-B\sinh\Big(\frac{T\dot{\alpha}^2}{2F+1}\Big)-C\cosh\Big(\frac{T\dot{\alpha}^2}{2F}\Big)\Big]\\&+\delta_3\Big[-A\sin\Big(\frac{T\dot{\alpha}^2}{2F+1}\Big)+B\cos\Big(\frac{T\dot{\alpha}^2}{2F+1}\Big)+C\sin\Big(\frac{T\dot{\alpha}^2}{2F}\Big)\Big]/2\\&-\delta_4\Big[A\cos\Big(\frac{T\dot{\alpha}^2}{2F+1}\Big)+B\sin\Big(\frac{T\dot{\alpha}^2}{2F+1}\Big)-C\cos\Big(\frac{T\dot{\alpha}^2}{2F}\Big)\Big]/2\Big),\end{aligned}\tag{C.3}$$

where

$$\begin{aligned}&A=\frac{2}{(2F+1)^3}\Big((2F+1)^2-\mu(2F+1)\Big),\quad B=\frac{2\mu T\dot{\alpha}^2}{(2F+1)^3},\quad C=\frac{1-\mu}{2F}\\&\delta_1=\frac{\lambda_0}{\lambda_1}+\frac{\lambda_2}{\lambda_3},\quad \delta_2=\frac{\lambda_1}{\lambda_2}+\frac{\lambda_3}{\lambda_0},\quad \delta_3=\frac{\lambda_0}{\lambda_1}-\frac{\lambda_2}{\lambda_3},\quad \delta_4=\frac{\lambda_1}{\lambda_2}-\frac{\lambda_3}{\lambda_0}.\end{aligned}\tag{C.4}$$

Note that for $\dot{\alpha}=0$, $V_x=1$ is obtained.

C.2 Variance at Bob's side (V_y)

The variance at the receiver's side can be computed as follows:

$$V_y=\mathrm{tr}(\hat{\rho}_{03}\hat{X}_3^2)=\frac{1}{4P^{\mathsf{PS}}}\sum_{k=0}^{3}L_{kk},\tag{C.5}$$

where, assuming $\xi_3=z+it$,

$$\begin{aligned}L_{kk}=&\mathrm{tr}(\hat{\Omega}_3^{kk}\hat{X}_3^2)\\=&-\zeta_A^{kk}(0,0)-\frac{d^2}{dt^2}\zeta_A^{kk}(0,t)\Big|_{t=0}\\\frac{d^2}{dt^2}\zeta_A^{kk}(0,t)\Big|_{t=0}=&-b_ke^{-\frac{T|\alpha_k|^2}{2F+1}}+\frac{2(1-\mu)}{F}e^{-\frac{T|\alpha_k|^2}{2F}},\end{aligned}\tag{C.6}$$

with $\hat{X}_3=\widehat{b}_3+\widehat{b}_3^\dagger$ in figure 5.2 and $b_k=\frac{8}{(2F+1)^3}\Big((2F+1)^2-\mu(2F^2+3F+1)+\mu T|\alpha_k|^2\Big)$; hence,

$$\begin{aligned}V_y=&\frac{L_{00}}{\zeta_A^{00}(0)}\\=&\frac{1}{\zeta_A^{00}(0)}\Big(b_ke^{-\frac{T|\alpha_k|^2}{2F+1}}-\frac{2(1-\mu)}{F}e^{-\frac{T|\alpha_k|^2}{2F}}\Big)-1.\end{aligned}\tag{C.7}$$

Note that for $\dot{\alpha}=0$, $V_y=1$ is obtained.

C.3 Covariance between Alice and Bob (V_{xy})

By definition, the covariance between Alice and Bob is given by:

$$V_{xy}=\mathrm{tr}(\hat{\rho}_{03}\hat{X}_0\hat{X}_3)=\frac{1}{4P^{\mathsf{PS}}}\sum_{k=0}^{3}\sum_{l=0}^{3}N_{kl}S_{kl}, \tag{C.8}$$

where $N_{kl}:=\mathrm{tr}(|\psi_k\rangle_0\langle\psi_l|\hat{X}_0)$ is given in (C.12) and

$$\begin{aligned} S_{kl}=&\mathrm{tr}(\hat{\Omega}_3^{kl}\hat{X}_3)\\ =&-i\frac{d}{dt}\zeta_A^{kl}(0,t)\Big|_{t=0}\\ =&\frac{2\sqrt{\mu(1-\mu)T}\,(\alpha_k+\alpha_l^*)}{(2F+1)^2}e^{-\frac{T\alpha_k\alpha_l^*}{2F+1}}. \end{aligned} \tag{C.9}$$

One can then conclude that:

$$\begin{aligned} V_{xy}=&\frac{2\sqrt{\mu(1-\mu)T}\,\dot{\alpha}^2}{P^{\mathsf{PS}}(2F+1)^2}\Big[\omega_1\cosh\Big(\frac{T\dot{\alpha}^2}{2F+1}\Big)-\omega_2\sinh\Big(\frac{T\dot{\alpha}^2}{2F+1}\Big)\\ &+\omega_3\cos\Big(\frac{T\dot{\alpha}^2}{2F+1}\Big)-\omega_4\sin\Big(\frac{T\dot{\alpha}^2}{2F+1}\Big)\Big], \end{aligned} \tag{C.10}$$

where

$$\begin{aligned} \omega_1=&\sqrt{\frac{\lambda_0}{\lambda_1}}+\sqrt{\frac{\lambda_2}{\lambda_3}}, \quad \omega_2=\sqrt{\frac{\lambda_1}{\lambda_2}}+\sqrt{\frac{\lambda_3}{\lambda_0}},\\ \omega_3=&\sqrt{\frac{\lambda_0}{\lambda_1}}-\sqrt{\frac{\lambda_2}{\lambda_3}}, \quad \omega_4=\sqrt{\frac{\lambda_1}{\lambda_2}}-\sqrt{\frac{\lambda_3}{\lambda_0}}. \end{aligned} \tag{C.11}$$

It is seen that for $\dot{\alpha}=0$, $V_{xy}=0$ is obtained.

In the calculations of G_{kl} and N_{kl} we made use of the following identities:

$$\begin{aligned}
|\psi_0\rangle =& \frac{1}{2}\Big[|\phi_0\rangle + e^{i\pi/4}|\phi_1\rangle + e^{i\pi/2}|\phi_2\rangle + e^{3i\pi/4}|\phi_3\rangle\Big]\\
\hat{a}|\psi_0\rangle =& \frac{\dot{\alpha}}{2}\Big[e^{i\pi/4}\sqrt{\frac{\lambda_0}{\lambda_1}}|\phi_0\rangle + e^{i\pi/2}\sqrt{\frac{\lambda_1}{\lambda_2}}|\phi_1\rangle + e^{i3\pi/4}\sqrt{\frac{\lambda_2}{\lambda_3}}|\phi_2\rangle - \sqrt{\frac{\lambda_3}{\lambda_0}}|\phi_3\rangle\Big]\\
\hat{a}^2|\psi_0\rangle =& \frac{\dot{\alpha}^2}{2}\Big[e^{i\pi/2}\sqrt{\frac{\lambda_0}{\lambda_2}}|\phi_0\rangle + e^{i3\pi/4}\sqrt{\frac{\lambda_1}{\lambda_3}}|\phi_1\rangle - \sqrt{\frac{\lambda_2}{\lambda_0}}|\phi_2\rangle - e^{i\pi/4}\sqrt{\frac{\lambda_3}{\lambda_1}}|\phi_3\rangle\Big]\\
|\psi_1\rangle =& \frac{1}{2}\Big[|\phi_0\rangle + e^{i3\pi/4}|\phi_1\rangle + e^{i3\pi/2}|\phi_2\rangle + e^{i\pi/4}|\phi_3\rangle\Big]\\
\hat{a}|\psi_1\rangle =& \frac{\dot{\alpha}}{2}\Big[e^{i3\pi/4}\sqrt{\frac{\lambda_0}{\lambda_1}}|\phi_0\rangle + e^{i3\pi/2}\sqrt{\frac{\lambda_1}{\lambda_2}}|\phi_1\rangle + e^{i\pi/4}\sqrt{\frac{\lambda_2}{\lambda_3}}|\phi_2\rangle - \sqrt{\frac{\lambda_3}{\lambda_0}}|\phi_3\rangle\Big]\\
\hat{a}^2|\psi_1\rangle =& \frac{\dot{\alpha}^2}{2}\Big[e^{i3\pi/2}\sqrt{\frac{\lambda_0}{\lambda_2}}|\phi_0\rangle + e^{i\pi/4}\sqrt{\frac{\lambda_1}{\lambda_3}}|\phi_1\rangle - \sqrt{\frac{\lambda_2}{\lambda_0}}|\phi_2\rangle - e^{i3\pi/4}\sqrt{\frac{\lambda_3}{\lambda_1}}|\phi_3\rangle\Big]\\
|\psi_2\rangle =& \frac{1}{2}\Big[|\phi_0\rangle + e^{-i3\pi/4}|\phi_1\rangle + e^{i\pi/2}|\phi_2\rangle + e^{-i\pi/4}|\phi_3\rangle\Big]\\
\hat{a}|\psi_2\rangle =& \frac{\dot{\alpha}}{2}\Big[e^{-i3\pi/4}\sqrt{\frac{\lambda_0}{\lambda_1}}|\phi_0\rangle + e^{i\pi/2}\sqrt{\frac{\lambda_1}{\lambda_2}}|\phi_1\rangle + e^{i\pi/4}\sqrt{\frac{\lambda_2}{\lambda_3}}|\phi_2\rangle - \sqrt{\frac{\lambda_3}{\lambda_0}}|\phi_3\rangle\Big]\\
\hat{a}^2|\psi_2\rangle =& \frac{\dot{\alpha}^2}{2}\Big[e^{i\pi/2}\sqrt{\frac{\lambda_0}{\lambda_2}}|\phi_0\rangle + e^{-i\pi/4}\sqrt{\frac{\lambda_1}{\lambda_3}}|\phi_1\rangle - \sqrt{\frac{\lambda_2}{\lambda_0}}|\phi_2\rangle - e^{-i3\pi/4}\sqrt{\frac{\lambda_3}{\lambda_1}}|\phi_3\rangle\Big]\\
|\psi_3\rangle =& \frac{1}{2}\Big[|\phi_0\rangle + e^{-i\pi/4}|\phi_1\rangle + e^{i3\pi/2}|\phi_2\rangle + e^{-3i\pi/4}|\phi_3\rangle\Big]\\
\hat{a}|\psi_3\rangle =& \frac{\dot{\alpha}}{2}\Big[e^{-i\pi/4}\sqrt{\frac{\lambda_0}{\lambda_1}}|\phi_0\rangle + e^{i3\pi/2}\sqrt{\frac{\lambda_1}{\lambda_2}}|\phi_1\rangle + e^{-i3\pi/4}\sqrt{\frac{\lambda_2}{\lambda_3}}|\phi_2\rangle - \sqrt{\frac{\lambda_3}{\lambda_0}}|\phi_3\rangle\Big]\\
\hat{a}^2|\psi_3\rangle =& \frac{\dot{\alpha}^2}{2}\Big[e^{i3\pi/2}\sqrt{\frac{\lambda_0}{\lambda_2}}|\phi_0\rangle + e^{-i3\pi/4}\sqrt{\frac{\lambda_1}{\lambda_3}}|\phi_1\rangle - \sqrt{\frac{\lambda_2}{\lambda_0}}|\phi_2\rangle - e^{-i\pi/4}\sqrt{\frac{\lambda_3}{\lambda_1}}|\phi_3\rangle\Big].
\end{aligned} \tag{C.12}$$

Appendix D

Bounding Eve's accessibility to a satellite-to-ground link

In this appendix, we present calculations that lead to finding nominal values for parameters η_{AE} and η_{EB}, as discussed in chapter 6. We assume that the trusted parties are equipped with LIDAR technology for monitoring and detecting possible adversaries' objects.

We assume Alice is located on a Low Earth Orbit (LEO) satellite, travelling in a circular orbit at an altitude L above the ground. She is equipped with a telescope of aperture radius r_A. Bob, who is located at the terrestrial station, collects the incoming light from Alice using a telescope with radius r_B. For the Chinese satellite Micius, the values $r_A = 15$ cm, $r_B = 50$ cm, and $L = 500$ km are used. On the other hand, we assume that Eve, who is located at distance z from the satellite, is represented by a spacecraft equipped with two telescopes, both of radius r_E, of which one is pointed towards Alice and used for light collection, and one is pointed towards Bob for signal transmission.

By assuming that Alice's telescope transmits Gaussian beams, with initial width $W_0 = r_A$ and wavelength λ, we have that

$$\eta_{AE}(z) = 1 - \exp\Big(- 2\frac{r_E^2(z)}{W^2(z)}\Big), \tag{D.1}$$

where $W(z)$ is the beams' width at z. In above, we have also assumed that the signals impinge at the centre of Eve's collecting aperture, with radius $r_E(z)$, which is chosen by Eve based on her distance from the satellite station. Similarly,

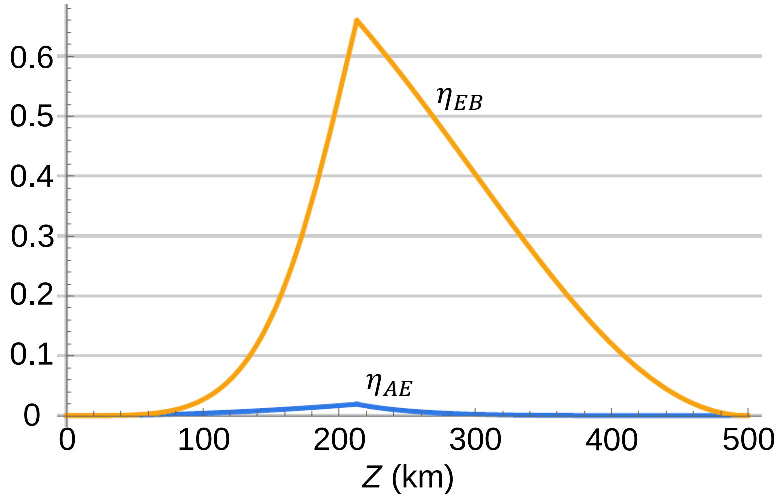

Figure D.1: Alice-to-Eve and Eve-to-Bob channel losses when a 4 Watt LIDAR system is used. Here, reflectivity of Eve's spacecraft is assumed 0.1.

we can show that

$$\eta_{EB}(z) = 1 - \exp\Big(-2\frac{r_B^2}{W_E^2(z)}\Big), \tag{D.2}$$

where $W_E(z)$ is beam width at Bob's side as re-transmitted by Eve and r_B is radius of the Bob's collecting aperture.

By making some assumptions on, e.g., the reflectivity of Eve's object, we can also find a maximum value for $r_E(z)$, under which Eve cannot be detected by a LIDAR and/or RADAR monitoring systems. The fact that Eve's spacecraft, i.e., telescope, size cannot be arbitrary large—while it remains undetected—would restrict her collecting and re-transmitting efficiencies, which are, respectively, represented by η_{AE} and η_{EB} in (D.1) and (D.2), respectively. Figure D.1 shows η_{AE} and η_{EB} as a function of z, when a LIDAR system is in use. The plots imply that, in a realistic regime of operation similar to the Chinese satellite Micius, η_{AE} can be on the order of a few percent, whereas η_{EB} can be close to one. As we show in chapter 6, this is the value of η_{AE} that matters most in improving the performance of CV-QKD systems under such restricted regimes.

References

Araki, H. & Lieb, E.H. (1970). Entropy Inequalities. *Commun. Math. Phys.*, **18**, 160–170.

Azuma, K. (2019). Journey Towards the Quantum Internet. *De Physicus*, pages: 52–54.

Barbieri, M., Ferreyrol, F., Blandino, R., Tualle-Brouri, R. & Grangier, P. (2011). Nondeterministic Noiseless Amplification of Optical Signals: A Review of Recent Experiments. *Laser Phys. Lett.*, **8**, 411.

Bedington, R., Arrazola, J.M. & Ling, A. (2017). Advances in Quantum Teleportation. *Nat. Commun.*, **3**, 30.

Bennett, C.H. & Brassard, G. (1984). Quantum Cryptography: Public Key Distribution and Coin Tossing. Presented in the IEEE International Conference on Computers Systems and Signal Processing.

Bennett, C.H. & Brassard, G. (2014). Quantum Cryptography: Public Key Distribution and Coin Tossing. *Theor. Comput. Sci.*, **560**, 7–11.

Bennett, C.H., Brassard, G., Crepeau, C. & Maurer, U.M. (1995). Generalized Privacy Amplification. *IEEE Transactions on Information Theory*, **41**, 1915–1923.

Bernu, J., Armstrong, S., Symul, T., Ralph, T.C. & Lam, P.K. (2014). Theoretical Analysis of an Ideal Noiseless Linear Amplifier for Einstein-Podolsky-Rosen Entanglement Distillation. *Journal of Physics B: Atomic, Molecular and Optical Physics*, **47**, 215503.

Blandino, R., Leverrier, A., Barbieri, M., Etesse, J., Grangier, P. & Tualle-Brouri, R. (2012). Improving the Maximum Transmission Distance of Continuous-Variable Quantum Key Distribution Using a Noiseless Amplifier. *Phys. Rev. A*, **86**, 012327.

Boaron, A., Boso, G., Rusca, D., Vulliez, C., Autebert, C., Caloz, M., Perrenoud, M., Gras, G., Bussières, F., Li, M.J., Nolan, D., Martin, A. & Zbinden, H. (2018). Secure Quantum Key Distribution over 421 km of Optical Fiber. *Phys. Rev. Lett.*, **121**, 190502.

Bonato, C., Tomaello, A., Deppo, V.D., Naletto, G. & Villoresi, P. (2009). Feasibility of Satellite Quantum Key Distribution. *New J. of Phys.*, **11**, 045017.

Boone, K., Bourgoin, J.P., Meyer-Scott, E., Heshami, K., Jennewein, T. & Simon, C. (2015). Entanglement over Global Distances via Quantum Repeaters with Satellite Links. *Phys. Rev. A*, **91**, 052325.

Bourgoin, J.P., Meyer-Scott, E., Higgins, B.L., Helou, B., Erven, C., Hubel, H., Kumar, B., Hudson, D., D'Souza, I., Girard, R., Laflamme, R. & Jennewein, T. (2014). Corrigendum: A Comprehensive Design and Performance Analysis of Low Earth Orbit Satellite Quantum Communication (2013 New J. Phys. 15 023006). *New J. of Phys.*, **16**, 069502.

Bourgoin, J.P., Gigov, N., Higgins, B.L., Yan, Z., Meyer-Scott, E., Khandani, A.K., Lütkenhaus, N. & Jennewein, T. (2015). Experimental Quantum Key Distribution with Simulated Ground-to-Satellite Photon Losses and Processing Limitations. *Phys. Rev. A*, **92**, 052339.

Braunstein, S.L. & Kimble, H.J. (1998). Teleportation of Continuous Quantum Variables. *Phys. Rev. Lett.*, **80**, 869–872.

Braunstein, S.L. & van Loock, P. (2005). Quantum Information with Continuous Variables. *Rev. Mod. Phys.*, **77**, 513–577.

Briegel, H.J., Dür, W., Cirac, J.I. & Zoller, P. (1998). Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication. *Phys. Rev. Lett.*, **81**, 5932–5935.

Cahall, C., Nicolich, K.L., Islam, N.T., Lafyatis, G.P., Miller, A.J., Gauthier, D.J. & Kim, J. (2017). Multi-Photon Detection Using a Conventional Superconducting Nanowire Single-Photon Detector. *Optica*, **4**, 1534–1535.

Caves, C.M. (1981). Quantum-Mechanical Noise in an Interferometer. *Phys. Rev. D*, **23**, 1693–1708.

Caves, C.M. (1982). Quantum Limits on Noise in Linear Amplifiers. *Phys. Rev. D*, **26**, 1817–1839.

Caves, C.M. & Schumaker, B.L. (1985). New Formalism for Two-Photon Quantum Optics. I. Quadrature Phases and Squeezed States. *Phys. Rev. A*, **31**, 3068–3092.

Caves, C.M., Combes, J., Jiang, Z. & Pandey, S. (2012). Quantum Limits on Phase-Preserving Linear Amplifiers. *Phys. Rev. A*, **86**, 063802.

Cerf, N.J., Lévy, M. & Assche, G.V. (2001). Quantum Distribution of Gaussian Keys Using Squeezed States. *Phys. Rev. A*, **63**, 052311.

Chrzanowski, H.M., Walk, N., Assad, S.M., Janousek, J., Hosseini, S., Ralph, T.C., Symul, T. & Lam, P.K. (2014). Measurement-Based Noiseless Linear Amplification for Quantum Communication. *Nat. Commun.*, **8**, 333–338.

Combes, J., Walk, N., Lund, A.P., Ralph, T.C. & Caves, C.M. (2016). Models of Reduced-Noise, Probabilistic Linear Amplifiers. *Phys. Rev. A*, **93**, 052310.

Cover, T.M. & Thomas, J.A. (2006). *Elements of Information Theory*. John Wiley & Sons, New Jersey, 2nd edn.

Dias, J. & Ralph, T.C. (2017). Quantum Repeaters Using Continuous-Variable Teleportation. *Phys. Rev. A*, **95**, 022312.

Ding, X., He, Y., Duan, Z.C., Gregersen, N., Chen, M.C., Unsleber, S., Maier, S., Schneider, C., Kamp, M., Höfling, S., Lu, C.Y. & Pan, J.W. (2016). On-Demand Single Photons with High Extraction Efficiency and Near-Unity Indistinguishability from a Resonantly Driven Quantum Dot in a Micropillar. *Phys. Rev. Lett.*, **116**, 020401.

Donaldson, R.J., Collins, R.J., Eleftheriadou, E., Barnett, S.M., Jeffers, J. & Buller, G.S. (2015). Experimental Implementation of a Quantum Optical State Comparison Amplifier. *Phys. Rev. Lett.*, **114**, 120505.

Eleftheriadou, E., Barnett, S.M. & Jeffers, J. (2013). Quantum Optical State Comparison Amplifier. *Phys. Rev. Lett.*, **111**, 213601.

Fiurášek, J. & Cerf, N.J. (2012). Gaussian Postselection and Virtual Noiseless Amplification in Continuous-Variable Quantum Key Distribution. *Phys. Rev. A*, **86**, 060302.

Furrer, F. & Munro, W.J. (2018). Repeaters for Continuous-Variable Quantum Communication. *Phys. Rev. A*, **98**, 032335.

García-Patrón, R. & Cerf, N.J. (2006). Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution. *Phys. Rev. Lett.*, **97**, 190503.

García-Patrón, R. & Cerf, N.J. (2009). Continuous-Variable Quantum Key Distribution Protocols over Noisy Channels. *Phys. Rev. Lett.*, **102**, 130501.

García-Patrón, R., Pirandola, S., Lloyd, S. & Shapiro, J.H. (2009). Reverse Coherent Information. *Phys. Rev. Lett.*, **102**, 210501.

Gerry, C. & Knight, P. (2005). *Introductory Quantum Optics*. Cambridge University Press, Cambridge, 1st edn.

Ghorai, S., Grangier, P., Diamanti, E. & Leverrier, A. (2019). Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation. *Phys. Rev. X*, **9**, 021059.

Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. (2002). Quantum Cryptography. *Rev. Mod. Phys.*, **74**, 145–195.

GLAUBER, R.J. (1963). Coherent and Incoherent States of the Radiation Field. *Phys. Rev.*, **131**, 2766–2788.

GROSSHANS, F. & CERF, N.J. (2004). Continuous-Variable Quantum Cryptography is Secure against Non-Gaussian Attacks. *Phys. Rev. Lett.*, **92**, 047905.

GROSSHANS, F. & GRANGIER, P. (2002). Continuous Variable Quantum Cryptography Using Coherent States. *Phys. Rev. Lett.*, **88**, 057902.

GROSSHANS, F., VAN ASSCHE, G., WENGER, J., BROURI, R., CERF, N.J. & GRANGIER, P. (2003). Quantum Key Distribution Using Gaussian-Modulated Coherent States. *Nature*, **421**, 238–241.

GÜNTHNER, K., KHAN, I., ELSER, D., STILLER, B., ÖMER BAYRAKTAR, MÜLLER, C.R., SAUCKE, K., TRÖNDLE, D., HEINE, F., SEEL, S., GREULICH, P., ZECH, H., GÜTLICH, B., PHILIPP-MAY, S., MARQUARDT, C. & LEUCHS, G. (2017). Quantum-Limited Measurements of Optical Signals from a Geostationary Satellite. *Optica*, **4**, 611–616.

HE, M., MALANEY, R. & GREEN, J. (2018). Quantum Communications via Satellite with Photon Subtraction. In *2018 IEEE Globecom Workshops (GC Wkshps)*, 1–6.

HOLEVO, A.S. (1973). Bounds for the Quantity of Information Transmitted by a Quantum Communication Channel. *Problems Inform. Transmission*, **9(3)**, 177–183.

HOSSEINIDEHAJ, N., BABAR, Z., MALANEY, R., NG, S.X. & HANZO, L. (2019). Satellite-Based Continuous-Variable Quantum Communications: State-of-the-Art and a Predictive Outlook. *IEEE Communications Surveys Tutorials*, **21**, 881–919.

HUANG, D., HUANG, P., LIN, D. & ZENG, G. (2016). Long-Distance Continuous-Variable Quantum Key Distribution by Controlling Excess Noise. *Sci. Rep.*, **6**, 19201.

HUSIMI, K. (1940). Some Formal Properties of the Density Matrix. *Proc. Phys. Math. Soc. Japan*, **22**, 264–314.

JEFFERS, J. (2010). Nondeterministic Amplifier for Two-Photon Superpositions. *Phys. Rev. A*, **82**, 063828.

JOUGUET, P., KUNZ-JACQUES, S. & LEVERRIER, A. (2011). Long-Distance Continuous-Variable Quantum Key Distribution with a Gaussian Modulation. *Phys. Rev. A*, **84**, 062317.

JOUGUET, P., KUNZ-JACQUES, S., DIAMANTI, E. & LEVERRIER, A. (2012). Analysis of Imperfections in Practical Continuous-Variable Quantum Key Distribution. *Phys. Rev. A*, **86**, 032309.

JOUGUET, P., KUNZ-JACQUES, S., LEVERRIER, A., GRANGIER, P. & DIAMANTI, E. (2013). Experimental Demonstration of Long-Distance Continuous-Variable Quantum Key Distribution. *Nat. Photon.*, **7**, 378–381.

KIMBLE, H.J. (2008). The Quantum Internet. *Nature*, **453**, 1023–1030.

KOK, P., MUNRO, W.J., NEMOTO, K., RALPH, T.C., DOWLING, J.P. & MILBURN, G.J. (2007). Linear Optical Quantum Computing with Photonic Qubits. *Rev. Mod. Phys.*, **79**, 135–174.

KRAUS, B., GISIN, N. & RENNER, R. (2005). Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Phys. Rev. Lett.*, **95**, 080501.

KUMAR, R., QIN, H. & ALLÉAUME, R. (2015). Coexistence of Continuous Variable QKD with Intense DWDM Classical Channels. *New J. of Phys.*, **17**, 043027.

KUNZ-JACQUES, S. & JOUGUET, P. (2015). Robust Shot-Noise Measurement for Continuous-Variable Quantum Key Distribution. *Phys. Rev. A*, **91**, 022307.

LEONHARDT, U. (1997). *Measuring the Quantum State of Light*. Cambridge University Press, Cambridge.

LEVERRIER, A. & GRANGIER, P. (2009). Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation. *Phys. Rev. Lett.*, **102**, 180504.

Leverrier, A. & Grangier, P. (2011). Continuous-Variable Quantum-Key-Distribution Protocols with a Non-Gaussian Modulation. *Phys. Rev. A*, **83**, 042312.

Liao, S.K., Cai, W.Q., Liu, W.Y., Zhang, L., Li, Y., Ren, J.G., Yin, J., Shen, Q., Cao, Y., Li, Z.P., Li, F.Z., Chen, X.W., Sun, L.H., Jia, J.J., Wu, J.C., Jiang, X.J., Wang, J.F., Huang, Y.M., Wang, Q., Zhou, Y.L., Deng, L., Xi, T., Ma, L., Hu, T., Zhang, Q., Chen, Y.A., Liu, N.L., Wang, X.B., Zhu, Z.C., Lu, C.Y., Shu, R., Peng, C.Z., Wang, J.Y. & Pan, J.W. (2017a). Satellite-to-Ground Quantum Key Distribution. *Nature*, **549**, 43.

Liao, S.K., Yong, H.L., Liu, C., Shentu, G.L., Li, D.D., Lin, J., Dai, H., Zhao, S.Q., Li, B., Guan, J.Y., Chen, W., Gong, Y.H., Li, Y., Lin, Z.H., Pan, G.S., Pelc, J.S., Fejer, M.M., Zhang, W.Z., Liu, W.Y., Yin, J., Ren, J.G., Wang, X.B., Zhang, Q., Peng, C.Z. & Pan, J.W. (2017b). Long-Distance Free-Space Quantum Key Distribution in Daylight towards Inter-Satellite Communication. *Nat. Photon.*, **311**, 509.

Liao, S.K., Cai, W.Q., Handsteiner, J., Liu, B., Yin, J., Zhang, L., Rauch, D., Fink, M., Ren, J.G., Liu, W.Y., Li, Y., Shen, Q., Cao, Y., Li, F.Z., Wang, J.F., Huang, Y.M., Deng, L., Xi, T., Ma, L., Hu, T., Li, L., Liu, N.L., Koidl, F., Wang, P., Chen, Y.A., Wang, X.B., Steindorfer, M., Kirchner, G., Lu, C.Y., Shu, R., Ursin, R., Scheidl, T., Peng, C.Z., Wang, J.Y., Zeilinger, A. & Pan, J.W. (2018). Satellite-Relayed Intercontinental Quantum Network. *Phys. Rev. Lett.*, **120**, 030501.

Lin, J., Upadhyaya, T. & Lütkenhaus, N. (2019). Asymptotic Security Analysis of Discrete-Modulated Continuous-Variable Quantum Key Distribution. *arXiv:1905.10896*.

Lodewyck, J., Bloch, M., García-Patrón, R., Fossier, S., Karpov, E., Diamanti, E., Debuisschert, T., Cerf, N.J., Tualle-Brouri, R., McLaughlin, S.W. & Grangier, P. (2007). Quantum Key Distribution over 25 km with an All-Fiber Continuous-Variable System. *Phys. Rev. A*, **76**, 042305.

Maurer, U.M. (1993). Secret Key Agreement by Public Discussion from Common Information. *IEEE Transactions on Information Theory*, **39**, 733–742.

McMahon, N.A., Lund, A.P. & Ralph, T.C. (2014). Optimal Architecture for a Nondeterministic Noiseless Linear Amplifier. *Phys. Rev. A*, **89**, 023846.

Menzies, D. & Croke, S. (2009). Noiseless Linear Amplification via Weak Measurements. *arXiv:0903.4181*.

Meyer-Scott, E., Yan, Z., MacDonald, A., Bourgoin, J.P., Hübel, H. & Jennewein, T. (2011). How to Implement Decoy-State Quantum Key Distribution for a Satellite Uplink with 50-dB Channel Loss. *Phys. Rev. A*, **84**, 062326.

Moli-Sanchez, L., Rodriguez-Alonso, A. & Seco-Granados, G. (2009). Performance Analysis of Quantum Cryptography Protocols in Optical Earth-Satellite and Intersatellite Links. *IEEE Journal on Selected Areas in Communications*, **27**, 1582–1590.

Müller, M., Bounouar, S., Jöns, K.D., Glässl, M. & Michler, P. (2014). On-Demand Generation of Indistinguishable Polarization-Entangled Photon Pairs. *Nat. Photon.*, **8**, 224–228.

Nauerth, S., Moll, F., Rau, M., Fuchs, C., Horwath, J., Frick, S. & Weinfurter, H. (2013). Air-to-Ground Quantum Communication. *Nat. Photon.*, **7**, 382.

Navascués, M. & Acín, A. (2005). Security Bounds for Continuous Variables Quantum Key Distribution. *Phys. Rev. Lett.*, **94**, 020505.

Navascués, M., Grosshans, F. & Acín, A. (2006). Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography. *Phys. Rev. Lett.*, **97**, 190502.

Nielsen, M.A. & Chuang, I.L. (2000). *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge.

Pan, Z., Seshadreesan, K.P., Clark, W., Adcock, M.R., Djordjevic, I.B., Shapiro, J.H. & Guha, S. (2019). Secret Key Distillation across a Quantum Wiretap Channel under Restricted Eavesdropping. *arXiv:1903.03136*.

Pandey, S., Jiang, Z., Combes, J. & Caves, C.M. (2013). Quantum Limits on Probabilistic Amplifiers. *Phys. Rev. A*, **88**, 033852.

Pegg, D.T., Phillips, L.S. & Barnett, S.M. (1998). Optical State Truncation by Projection Synthesis. *Phys. Rev. Lett.*, **81**, 1604–1606.

Pirandola, S. (2019). End-to-End Capacities of a Quantum Communication Network. *Commun. Phys.*, **2**, 51.

Pirandola, S., Braunstein, S.L. & Lloyd, S. (2008). Characterization of Collective Gaussian Attacks and Security of Coherent-State Quantum Cryptography. *Phys. Rev. Lett.*, **101**, 200504.

Pirandola, S., García-Patrón, R., Braunstein, S.L. & Lloyd, S. (2009). Direct and Reverse Secret-Key Capacities of a Quantum Channel. *Phys. Rev. Lett.*, **102**, 050503.

Pirandola, S., Eisert, J., Weedbrook, C., Furusawa, A. & Braunstein, S.L. (2015a). Advances in Quantum Teleportation. *Nat. Photon.*, **9**, 641–652.

Pirandola, S., Ottaviani, C., Spedalieri, G., Weedbrook, C., Braunstein, S.L., Lloyd, S., Gehring, T., Jacobsen, C.S. & Andersen, U.L. (2015b). High-Rate Measurement-Device-Independent Quantum Cryptography. *Nat. Photon.*, **9**, 397–402.

Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. (2017). Fundamental Limits of Repeaterless Quantum Communications. *Nat. Commun.*, **8**, 15043.

Qin, H., Kumar, R., Makarov, V. & Alléaume, R. (2018). Homodyne-Detector-Blinding Attack in Continuous-Variable Quantum Key Distribution. *Phys. Rev. A*, **98**, 012312.

Ralph, T.C. (1999). Continuous Variable Quantum Cryptography. *Phys. Rev. A*, **61**, 010303.

Ralph, T.C. & Lund, A.P. (2009). Nondeterministic Noiseless Linear Amplification of Quantum Systems. *AIP Conference Proceedings*, **1110**, 155–160.

Razavi, M. (2006). *Long-Distance Quantum Communication with Neutral Atoms*. Ph.D. thesis.

Razavi, M. (2018). *An Introduction to Quantum Communications Networks*. 2053-2571, Morgan & Claypool Publishers.

Ren, J.G., Xu, P., Yong, H.L., Zhang, L., Liao, S.K., Yin, J., Liu, W.Y., Cai, W.Q., Yang, M., Li, L., Yang, K.X., Han, X., Yao, Y.Q., Li, J., Wu, H.Y., Wan, S., Liu, L., Liu, D.Q., Kuang, Y.W., He, Z.P., Shang, P., Guo, C., Zheng, R.H., Tian, K., Zhu, Z.C., Liu, N.L., Lu, C.Y., Shu, R., Chen, Y.A., Peng, C.Z., Wang, J.Y. & Pan, J.W. (2017). Ground-to-Satellite Quantum Teleportation. *Nature*, **549**, 70.

Renner, R. (2005). *Security of Quantum Key Distribution*. Ph.D. thesis.

Renner, R. & Cirac, J.I. (2009). de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography. *Phys. Rev. Lett.*, **102**, 110504.

Senellart, P., Solomon, G. & White, A. (2017). High-Performance Semiconductor Quantum-Dot Single-Photon Sources. *Nature Nanotech.*, **12**, 1026–1039.

Seshadreesan, K.P., Krovi, H. & Guha, S. (2018). A Continuous-Variable Quantum Repeater with Quantum Scissors. *arXiv:1811.12393*.

Shannon, C.E. (1949). Communication Theory of Secrecy Systems. *The Bell System Technical Journal*, **28**, 656–715.

Simon, R., Mukunda, N. & Dutta, B. (1994). Quantum-Noise Matrix for Multimode Systems: U(n) Invariance, Squeezing, and Normal Forms. *Phys. Rev. A*, **49**, 1567–1583.

Singh, S. (2002). *The Code Book: The Secret History of Codes and Code-Breaking*. Fourth Estate, New York.

Stoler, D. (1970). Equivalence Classes of Minimum Uncertainty Packets. *Phys. Rev. D*, **1**, 3217–3219.

Sudarshan, E.C.G. (1963). Equivalence of Semiclassical and Quantum Mechanical Descriptions of Statistical Light Beams. *Phys. Rev. Lett.*, **10**, 277–279.

Usenko, V.C. & Filip, R. (2016). Trusted Noise in Continuous-Variable Quantum Key Distribution: A Threat and a Defense. *Entropy*, **18**, 20.

Vallone, G., Bacco, D., Dequal, D., Gaiarin, S., Luceri, V., Bianco, G. & Villoresi, P. (2015). Experimental Satellite Quantum Communications. *Phys. Rev. Lett.*, **115**, 040502.

Villar, A.S., Cruz, L.S., Cassemiro, K.N., Martinelli, M. & Nussenzveig, P. (2005). Generation of Bright Two-Color Continuous Variable Entanglement. *Phys. Rev. Lett.*, **95**, 243603.

Walk, N., Ralph, T.C., Symul, T. & Lam, P.K. (2013). Security of Continuous-Variable Quantum Cryptography with Gaussian Postselection. *Phys. Rev. A*, **87**, 020303.

Walker, N.G. & Carroll, J.E. (1984). Simultaneous Phase and Amplitude Measurements on Optical Signals Using a Multiport Junction. *Electron. Lett.*, **20**, 981–983.

Walls, D.F. & Milburn, G.J. (2008). *Quantum Optics*. Springer, Berlin, 2nd edn.

Wang, J.Y., Yang, B., Liao, S.K., Zhang, L., Shen, Q., Hu, X.F., Wu, J.C., Yang, S.J., Jiang, H., Tang, Y.L., Zhong, B., Liang, H., Liu, W.Y., Hu, Y.H., Huang, Y.M., Qi, B., Ren, J.G., Pan, G.S., Yin, J., Jia, J.J., Chen, Y.A., Chen, K., Peng, C.Z. & Pan, J.W. (2013). Direct and Full-Scale Experimental Verifications Towards Ground-Satellite Quantum Key Distribution. *Nat. Photon.*, **7**, 387.

Weedbrook, C., Lance, A.M., Bowen, W.P., Symul, T., Ralph, T.C. & Lam, P.K. (2004). Quantum Cryptography without Switching. *Phys. Rev. Lett.*, **93**, 170504.

Weedbrook, C., Pirandola, S., García-Patrón, R., Cerf, N.J., Ralph, T.C., Shapiro, J.H. & Lloyd, S. (2012). Gaussian Quantum Information. *Rev. Mod. Phys.*, **84**, 621–669.

Xu, B., Tang, C., Chen, H., Zhang, W. & Zhu, F. (2013). Improving the Maximum Transmission Distance of Four-State Continuous-Variable Quantum Key Distribution by Using a Noiseless Linear Amplifier. *Phys. Rev. A*, **87**, 062311.

Zhang, H., Mao, Y., Huang, D., Guo, Y., Wu, X. & Zhang, L. (2018a). Finite-Size Analysis of Eight-State Continuous-Variable Quantum Key Distribution with the Linear Optics Cloning Machine. *Chinese Physics B*, **27**, 090307.

Zhang, Q., Xu, F., Chen, Y.A., Peng, C.Z. & Pan, J.W. (2018b). Large Scale Quantum Key Distribution: Challenges and Solutions [Invited]. *Opt. Express*, **26**, 24260–24273.

Zhao, J., Haw, J.Y., Symul, T., Lam, P.K. & Assad, S.M. (2017). Characterization of a Measurement-Based Noiseless Linear Amplifier and its Applications. *Phys. Rev. A*, **96**, 012319.

Zhou, H., Zeng, P., Razavi, M. & Ma, X. (2018). Randomness Quantification of Coherent Detection. *Phys. Rev. A*, **98**, 042321.