Analysing and reducing the limitations of continuous-variable quantum cryptography and quantum networks

Kieran Neil Wilkinson

Doctor of Philosophy

University of York

Computer Science

July 2020

Dedicated to

Debbie and Neil

Abstract

Due to a recent influx of attention, the field of quantum information is rapidly progressing towards the point at which quantum technologies move from the laboratory to widespread community use. However, several difficulties must be overcome before this milestone can be achieved. Two such difficulties are addressed in this thesis. The first is the ever-growing security threat posed by quantum computers to existing cryptographic protocols and the second is the missing knowledge regarding the performance differences between quantum and classical communications over various existing network topologies. Continuous-variable (CV) quantum key distribution (QKD) poses a practical solution to the security risks implied by the advancement of quantum information theory, with the promise of provably secure communications. Unfortunately, the maximum range of many CV-QKD protocols is limited. Here, this limitation is addressed by the application of post-selection, firstly, to a scenario in which two parties communicate using terahertz frequency radiation in the atmosphere, and secondly, to measurement-device-independent QKD, in which two parties communicate through the medium of an untrusted relay. In both cases, the introduction of post-selection enables security over distances substantially exceeding those of equivalent existing protocols. The second difficulty is addressed by a comparison of the quantum and classical networking regimes of the butterfly network and a group of networks constructed with butterfly blocks. By computing the achievable classical rates and upper bounds for quantum communication, the performance difference between the two regimes is quantified, and a range of conditions is established under which classical networking outperforms its quantum counterpart. This allows for guidance to be provided on which network structures should be avoided when constructing a quantum internet.

Contents

List of Figures

Declaration

The work in this thesis is based on research carried out at the Department of Computer Science, University of York, United Kingdom during 2017-2020. No part of this thesis has been submitted elsewhere for any other degree or qualification and it is all my own work unless referenced to the contrary in the text.

Part of the work presented here has been published in the following journal articles in which I am the leading author:

- *Long-distance continuous-variable measurement-device-independent quantum key distribution with post-selection*, K. N. Wilkinson, P. Papanastasiou, C. Ottaviani, T. Gehring, and S. Pirandola, Physical Review Research **2**, 033424 (2020) [1].

- *Exploring the Limitations of Quantum Networking through Butterfly-Based Networks* K. N. Wilkinson, T. P. W. Cope, and S. Pirandola, Advanced Quantum Technologies **3**, 1900103 (2020) [2].

Acknowledgements

The complete list of those who have contributed to my journey up to and throughout this process is, unfortunately, too long to express here in just a few words. Instead, I will mention those who played the biggest part, while extending my gratitude to those unmentioned whom I hope are aware of their contributions. I will start by expressing the utmost gratitude for my supervisor, Prof. Stefano Pirandola not only for his belief in my ability as a researcher but for his unfaltering support throughout this journey. This gratitude must be extended to my friends and co-authors Dr. Panagiotis Papanastasiou and Dr. Carlo Ottaviani for their friendship and the numerous stimulating discussions we had throughout my time at the University of York, particularly through our various quandaries. On a similar note, many thanks go to my colleagues and friends Jason and Athena with whom I have shared this experience and many laughs along the way. Finally, thanks go to Prof. Samuel L. Braunstein who has provided me with many words of wisdom and reassurance for which I am most grateful. It has been a great privilege to work alongside all of you.

Above all, I must thank all of my friends and family, for without them I would certainly not be writing these words today. Special thanks go to my wonderful girlfriend, Georgia who has provided me with unwavering support in this process through its many peaks and troughs. A worthy shoutout goes to my grandad for his continuous encouragement throughout my academic career and commendable persistence with the question “how’s your thesis going?”, but my particular gratitude goes to my parents who have made it possible for me to be where I am today.

“It’s something unpredictable, but in the end it’s right”

Chapter 1

Introduction

1.1 The ancestry of quantum information theory

Upon the turn of the twentieth century, physicists had been lulled into a false sense of security by the apparent ability of Newtonian mechanics and electrodynamics to describe, with extraordinary accuracy, almost any observable phenomenon. The accuracy and elegance of the theory caused physicists to harbor a belief that no new major component was needed to form a complete description of reality. However, problems were on the horizon as advancements in experimental technology were leading to discoveries that fell outside of the descriptive boundaries of these theories. A crisis quickly emerged when classical electrodynamics predicted infinite energies within the black-body radiation spectrum. This infamous blunder was quickly coined the ‘ultraviolet catastrophe’. Thankfully, in times of crisis, paradigm-shifting ideas emerge, in this case, in the form of Max Planck’s revolutionary radiation law [3]. Planck described the energy of the black body as a composition of discrete packets named ‘quanta’. Though unbeknownst to Planck, this insight would light the fuse on the quantum era of physics, leading to a radically different description of reality.

Four years later, armed with Planck’s quantization idea, Einstein was able to formulate a quantized description of the photoelectric effect by hypothesizing that radiation itself is quantized and composed of *particles* of energy proportional to the frequency of the radiation [4]. This model of radiation appeared to be in direct contradiction to the widely accepted wave model that had been confirmed by the observation of an interference pattern in Young's double-slit experiment several years prior to Einstein's work. Light appeared to be behaving as a wave *and* a particle; an apparent paradox known as wave-particle duality. In his Ph.D. thesis, Louis de Broglie proposed that wave-particle duality was not a paradox but a physical phenomenon that was possessed not just by light but by all particles. His formulation associated with every particle a de Broglie wavelength simply computed as the ratio of the Planck constant to the particle's momentum.

The de Broglie formulation formed the foundation on which the first formalisms of the theory we now call quantum mechanics were developed. Inspired by the idea of formulating the wave mechanics behind de Broglie's 'matter waves', Erwin Schrödinger began searching for a three-dimensional wave equation that would describe the behavior of the electron in a hydrogen atom. His initial attempt to derive a relativistic equation fell short and he became discouraged. However, he decided to publish the non-relativistic version of his work, and with the help of Hermann Weyl, he was able to use his equation to predict the spectral lines of the hydrogen atom. Schrödinger interpreted the electron wave function emerging from his equation as a charge-density function that spreads throughout space. However, shortly after Schrödinger published his work, Max Born showed that the square of the absolute value of the wave function was proportional to the *probability density* associated with finding the electron at a given point in space. In general, Born's result implied that the wavefunction of a quantum system could reveal the probability distribution associated with the measurement outcome of that system. Born's results appeared to suggest the presence of an inherently random aspect to reality, a concept that shocked the world of physics that held the idea of determinism at its core. Schrödinger himself would later proclaim "I don't like it, and I'm sorry I ever had anything to do with it."

Born's discovery opened a Pandora's box of philosophical questions regarding the interpretation of the mathematics of quantum mechanics. The most widely accepted interpretation was proposed by Neils Bohr and Werner Heisenberg, known as the Copenhagen interpretation, in which a physical system exists in a superposition of states before measurement and, upon measurement, collapses into one possible state with probability determined by the Born rule. Importantly, this interpretation assumed quantum mechanics to be entirely probabilistic in nature. On the other side of the spectrum and entering the realms of science fiction, the Many-Worlds interpretation, proposed by Hugh Everett in 1957, suggests that every possible outcome of a measurement exists in its own ‘universe’ with unique space and time [5]. For each outcome, there is an observer who is only aware of the specific outcome that occurs in the space and time in which they reside.

One of the harshest critics of the probabilistic Copenhagen interpretation of quantum mechanics was Einstein who famously said “I, in any case, am convinced that He does not play dice with the universe”. Together with Boris Podolski and Nathan Rosen, he developed the EPR paradox thought experiment in an attempt to illuminate the conceptual difficulties of quantum mechanics and argue that it was an incomplete theory [6]. The experiment can be understood by considering two distant particles whose properties are interlinked in such a way that measurement of the state of one reveals that of the other. In this case, the particles are said to be *entangled*. The Copenhagen interpretation describes the state of the measured particle as uncertain until the moment the measurement is performed, thus the state of the other appears to be instantaneously certain. Einstein dubbed this concept ‘spooky action at a distance’, viewing it as a violation of the theory of relativity as knowing the state instantly implies faster-than-light communication between the particles. Bohr refuted the paradox, asserting that both particles should be described as a single quantum system rather than two individual entities. In this case, the measurement of one particle makes certain the state of the system as a whole and no communication is necessary.

The disagreement between Bohr and Einstein is one of the most famous in the history of physics. Bohr’s Copenhagen interpretation was gaining traction with mounting experimental evidence but physicists were still uncomfortable with its probabilistic implications. In 1964, John Bell devised the Bell inequalities, which quantify the point at which a theory of hidden variables cannot produce the same correlations observed between two entangled systems. The Bell inequalities (largely) settled the debate over the completeness of quantum mechanics when, eight years after Bell's paper, the first Bell test was carried out experimentally by Freedman and Clauser [7]. The result of this experiment and many more was a violation of the Bell inequality as predicted by the probabilistic quantum mechanical description of reality.

Despite the conceptually difficult and highly counter-intuitive nature of quantum mechanics, the field has seen unprecedented progress and continues to grow rapidly in modern physics. Moreover, the field has attracted interest from a range of other scientific disciplines including computer science and mathematics. This inter-disciplinary interest has led to the emergence of the field of quantum information theory (QIT) [8, 9], which aims to exploit the unique properties of quantum states for a wide range of information processing tasks. Its purpose is identical to that of classical information theory, but it differs vastly in nature. The emergence of QIT dates back to the 1980s when a quantum mechanical version of the Turing machine was proposed by Paul Benioff [10]. The main advantage of QIT is the emergence of quantum parallelism which makes it possible to manipulate large quantities of data at once [11]. This important characteristic allows the theory to provide solutions to many problems that are difficult and slow to solve using classical techniques. Some of the most well-known examples include the quantum discrete Fourier transform [12], Shor's algorithm for factorization of large numbers in polynomial time [13] and Grover's algorithm for searching [14]. Another important application pointed out by Richard Feynman and Yuri Manin is the ability of quantum computers to simulate certain physical entities that may be difficult or even impossible to simulate with modern-day computers [15]. Notwithstanding these important results, the research introduced in this thesis is placed within the branch of QIT which focuses on quantum communication between two or more parties over quantum channels. In this setting, quantum mechanics makes possible many non-trivial results such as quantum key distribution (QKD) and quantum networking that form the foundations on which the results presented here are obtained.

1.2 Thesis outline

Throughout this thesis, several original contributions to the field of quantum information theory will be introduced that are focused on illuminating and improving, where possible, the limitations of quantum communications across three different regimes. Firstly, a point-to-point scenario is considered in which two parties are connected by and communicate over an insecure quantum channel. This is followed by consideration of the more complex regime of assisted communication in which third-party relays are introduced into the communication line between the parties. Finally, the most general case is considered in which the points become two of many nodes communicating over any number of quantum channels in a quantum network.

In the consideration of direct and relay-assisted communications, the focus is directed at the capacity for secure communications using QKD. In particular, the goal is to address the current limitations of continuous-variable (CV) QKD in each setting, which mainly relates to the maximum range of the current state-of-the-art protocols. To counteract these limitations, two original CV-QKD protocols are introduced, one for each communication regime. In the consideration of quantum networks, the investigation follows a more fundamental path. The difficult questions posed by the intrinsic nature of quantum mechanics when considering the structure of future quantum networks are addressed. Specifically, the investigation seeks to identify and quantify the performances of network structures that are frequently and effectively used in classical networking, while being simultaneously detrimental to quantum networking. The following two sections provide an introduction to the fields of CV QKD and quantum networking in more detail and explain their role within the field of quantum information theory as a whole.

1.2.1 Quantum key distribution

With the promise of secure communications guaranteed by the laws of physics, quantum cryptography is an intriguing consequence of quantum theory of interest to a variety of disciplines. Quantum key distribution is the most advanced instance of quantum cryptography in which quantum mechanics plays a small but vital role in a wider cryptographic protocol of distributing a secret key between parties. Key distribution is a difficult open problem in private-key cryptography that QKD promises to solve by proving impossible an eavesdropper's task of successfully replicating a secret key in conjunction with keeping their presence undetectable. This impossibility emerges from the inherent uncertainty of quantum mechanics and the no-cloning theorem. If two communicating parties use QKD to share a secret key, they can subsequently apply a symmetric classical cryptographic protocol such as the unbreakable one-time pad algorithm, to completely guarantee security.

The race to develop quantum cryptography is fuelled by the threat posed to existing cryptographic protocols by the rapid advancement of quantum technologies, in particular, the development of many-qubit quantum computers. The application of Shor's algorithm on such machines has the potential to render insecure many existing cryptosystems based on factorization such as the Rivest-Shamir-Adleman (RSA) protocol [16]. As a solution to this problem, much effort has been directed at developing a class of so-called post-quantum classical cryptographic algorithms that are thought to be secure against quantum attacks. However, the security of such protocols is predicated on the computational ability (or lack thereof) of the attacker. Without knowledge of all possible quantum algorithms, or even future computing paradigms, security is not guaranteed. The security of QKD on the other hand is built on the fundamental nature of reality and it assumes the most general attack an eavesdropper may employ that is permitted under the laws of physics. As a result, it guarantees security, regardless of any attack incorporating unimaginably powerful technologies and algorithms that may be developed in the future.

The seminal BB84 QKD protocol [17] and many subsequent protocols were based on systems with finite degrees of freedom, such as the polarisation of photons or ground/excited states of trapped ions, referred to as discrete variables. Several years later, the field of continuous-variable (CV) QKD was born [18, 19]. CV QKD aims to exploit systems with continuous degrees of freedom to guarantee security, the most obvious candidate being the quadrature amplitudes of the electromagnetic field. The key advantage of CV QKD over its discrete variable counterpart is the ease at which most state-of-the-art protocols can be implemented. Many quantum states of the electromagnetic field can be generated straightforwardly with linear optics and measurements can be performed with readily-available and low-cost homodyne detectors.

Since the inception of CV QKD, the field has seen substantial advancements in key areas such as protocol range, secret key rate, and ease of experimental implementation. In fact, CV QKD has been demonstrated to be capable of secret key rates close to the ultimate repeaterless (PLOB) bound [20]. Recently, CV QKD has been proposed as a viable candidate for secure communication at terahertz frequencies in the atmosphere [21] and as a means of inter-satellite communications [22]. Facilitation of communications in the terahertz band is an important topic of active research that is expected to experience rapid development in the near future due to the increasing demand for high-speed, short-distance wireless communications [23, 24]. The novel CV-QKD scheme for terahertz communication in the atmosphere offers the highly desirable feature of extremely high security at high rates for applications such as key cards and covert operations. Unfortunately, it is currently limited to particularly short distances on the scale of meters [21]. In Chap. 4, an alternative protocol is developed that exploits the technique of post-selection, first introduced for optical communications with optical states. By investigating the protocol under a variety of parameters, it is demonstrated that the limitations of CV QKD in this setting can be reduced by extending the maximum distance over which the legitimate parties can establish a secret key. As a result, the range of possible applications in this area is expanded.

QKD has been proven to be possible not only in the point-to-point regime but in the end-to-end regime in the form of measurement-device-independent (MDI) QKD, in which the parties communicate through the medium of an untrusted relay [25,26]. The seminal CV-MDI-QKD protocol was able to achieve very high secret key rates, especially in an asymmetric scenario (when the relay is positioned closer to one party than the other), however, in the symmetric configuration, communication is limited to relatively short distances, falling well short of DV protocols which, in some cases, can achieve secret key rates at distances exceeding the PLOB bound. In Chap. 5, an original post-selected CV-MDI protocol is introduced which is capable of extending the range of CV-MDI QKD. The protocol can bridge the gap between the CV and DV regimes while maintaining all of the advantages associated with CV QKD.

1.2.2 Quantum networking

The final part of this thesis involves a glance into the not-too-distant future in which quantum information and computation will have likely progressed to the level of adoption that requires significant infrastructure in order to connect quantum devices and create a widespread quantum internet [27, 28]. This kind of infrastructure will require further advancements in the field of quantum networking, in particular since it may be desirable to copy or replace existing classical network structures, it is important to establish any performance differences between classical and quantum networks of various topologies. A crucial element of this analysis is to take into consideration the unique properties of quantum mechanics that may cause the performance of certain quantum network topologies to deviate from that of their classical counterparts. In Chap. 6, this question is examined by consideration of the well-known butterfly network [29]. In the butterfly network, the duplicability of classical information may be exploited in order to transfer four bits of information using three channels. Here, it is formally show using the techniques of channel simulation that this exploit is not possible if the goal is to distribute quantum information. Furthermore, the analysis is extended to a group of larger networks constructed with butterfly blocks, and the differences between the achievable classical rates and an upper bound on the quantum rates for identity, erasure, and depolarizing channels are quantified. In doing so, guidance is provided on which network structures and conditions should be avoided in the construction of the quantum internet and within the wider field of quantum networking.

Chapter 2

Preliminaries

In this chapter, we will introduce the preliminary notions of quantum information theory required to instill in a reader unfamiliar with the theory, an understanding of the framework on which our research is built. In the first part of the chapter, we will focus on the pre-requisites of CV QKD which begins with a brief background of quantum optics with a particular focus on Gaussian states of light that frequently arise in our protocols. We also briefly introduce some of the fundamental principles of information theory in both classical and quantum regimes. In the later sections, we introduce the technique of teleportation stretching, which allows us to bound the rates of quantum channels and networks. These tools enable us to provide the necessary benchmarks for quantum networking that are utilized in Chap. 6.

Throughout this chapter, we assume that the reader is familiar with the fundamentals of quantum mechanics. For those seeking a more thorough understanding of the principles we outline here, the excellent books by Nielsen & Chuang [8] and Braunstein & Pati [9], and, of particular importance in the case of continuous-variable quantum information, the reviews by Braunstein et al. [19] and Weedbrook et al. [18] are recommended.

2.1 From classical to quantum optics

To begin our journey towards quantum optics, we will assume that the reader has a core understanding of the fundamental principles of classical electromagnetism.

As with most introductions to quantum optics, our starting point is with Maxwell's equations which form a succinct description of the field. We will demonstrate how Maxwell's equations lead to a description of electromagnetic radiation as a wave propagating through space and, using this framework, we will show how the transition to a quantum description of light is facilitated by the quantum harmonic oscillator and how this gives rise to a mathematical framework for quantum optics.

2.1.1 Classical electromagnetism in a flash

Let us now recap the Maxwell equations which govern the electric **E** and magnetic **B** fields. To streamline the mathematical description, we will choose our operating medium to be free space, in which there are no currents or charges. In this scenario, the Maxwell equations are as follows

$$\nabla \cdot \mathbf{E} = 0 \tag{2.1.1}$$

$$\nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t} \tag{2.1.2}$$

$$\nabla \cdot \mathbf{B} = 0 \tag{2.1.3}$$

$$\nabla \times \mathbf{B} = \mu_0 \epsilon_0 \frac{\partial \mathbf{E}}{\partial t}. \tag{2.1.4}$$

In only a few steps, we can arrive at Maxwell's crucial discovery of the wave nature of the electric and magnetic fields. Firstly, by taking the curl of both sides of Eq. (2.1.2) we obtain

$$\nabla \times (\nabla \times \mathbf{E}) = -\frac{\partial}{\partial t}(\nabla \times \mathbf{B}) \tag{2.1.5}$$

$$= -\mu_0 \epsilon_0 \frac{\partial^2 \mathbf{E}}{\partial t^2} \tag{2.1.6}$$

then, by applying vector identity $\nabla \times (\nabla \times \mathbf{E}) = \nabla(\nabla \cdot \mathbf{E}) - \nabla^2 \mathbf{E}$ and noting that the first term on the right hand side is zero due to Eq. (2.1.1), we arrive at the wave equation

$$\nabla^2 \mathbf{E} = \mu_0 \epsilon_0 \frac{\partial^2 \mathbf{E}}{\partial t^2}, \tag{2.1.7}$$

where it is easy to see that the wave speed is given by $c = (\mu_0 \epsilon_0)^{-1/2}$, the speed of light. This observation prompted Maxwell to proclaim “this coincidence is not merely numerical”.

In order to describe the behaviour of the electric and magnetic fields more easily, we introduce their scalar ϕ and vector $\mathbf{A}$ potentials, respectively, from which the Maxwell equations emerge. The Maxwell equations are satisfied if

$$\mathbf{B} = \nabla \times \mathbf{A} \qquad \text{and} \qquad \nabla\phi = -\mathbf{E} - \frac{\partial \mathbf{A}}{\partial t}. \tag{2.1.8}$$

Choosing the Coulomb gauge for which $\nabla \cdot \mathbf{A} = 0$, the electric field vector in Eq. (2.1.7) may be replaced by the vector potential. The general solution to this equation is a linear combination of a number of radiation modes with unique wavenumber $\mathbf{k}$, angular frequency $\omega_{\mathbf{k}}$ and polarization vector $\mathbf{e}_{\mathbf{k}\lambda}$,

$$\mathbf{A}(r,t) = \sum_{\mathbf{k}} \sum_{\lambda=1,2} \mathbf{e}_{\mathbf{k}\lambda} A_{\mathbf{k}\lambda}(\mathbf{r},t). \tag{2.1.9}$$

where the $A_{\mathbf{k}\lambda}(\mathbf{r},t)$ are general solutions to the wave equation which we may write for now as

$$A(\mathbf{r},t) = A_{\mathbf{k}\lambda}(t)\exp(i\mathbf{k}\cdot\mathbf{r}) + A^*_{\mathbf{k}\lambda}(t)\exp(-i\mathbf{k}\cdot\mathbf{r}). \tag{2.1.10}$$

Substituting the general solutions back into the wave equation, we find that the time-dependent coefficients $A_{\mathbf{k}\lambda}(t)$ satisfy the harmonic oscillator equation

$$\frac{\partial^2}{\partial t^2} A_{\mathbf{k}\lambda}(t) = -\omega_k^2 A_{\mathbf{k}\lambda}(t) \tag{2.1.11}$$

with $\omega_k = ck$. This allows us to state the complete form of the general solutions

$$A_{\mathbf{k}\lambda}(\mathbf{r},t) = A_{\mathbf{k}\lambda} e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} + A^*_{\mathbf{k}\lambda} e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)}. \tag{2.1.12}$$

The electric and magnetic fields are then readily expressed as

$$\mathbf{E}(\mathbf{r},t) = \sum_{\mathbf{k}} \sum_{\lambda=1,2} \mathbf{e}_{\mathbf{k}\lambda} E_{\mathbf{k}\lambda}(\mathbf{r},t) \tag{2.1.13}$$

$$\text{and} \quad \mathbf{B}(\mathbf{r},t) = \sum_{\mathbf{k}} \sum_{\lambda=1,2} \frac{\mathbf{k} \times \mathbf{e}_{\mathbf{k},\lambda}}{k} B_{\mathbf{k},\lambda}(\mathbf{r},t), \tag{2.1.14}$$

where the single-mode components are given by

$$E_{\mathbf{k}\lambda}(\mathbf{r},t) = i\omega_\kappa \left[A_{\mathbf{k}\lambda} e^{i(\mathbf{k}\mathbf{r}-\omega_k t)} - A^*_{\mathbf{k}\lambda} e^{-i(\mathbf{k}\mathbf{r}-\omega_k t)}\right] \tag{2.1.15}$$

$$\text{and} \quad B_{\mathbf{k}\lambda}(\mathbf{r},t) = ik\left[A_{\mathbf{k}\lambda} e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} - A^*_{\mathbf{k}\lambda} e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)}\right]. \tag{2.1.16}$$

2.1.2 The quantum harmonic oscillator

"The further away from home you are, the more you want to come back"

(Gary Marchant)

In order to adapt our discussion of classical electromagnetism for the quantum regime, we start with a brief discussion of the one-dimensional quantum harmonic oscillator. Let us consider a particle of mass m confined to a one-dimensional potential $U(x) = \omega^2 x^2/2$. The Hamiltonian of such a system consists of the sum of this potential and the kinetic energy of the particle,

$$\hat{H} = \frac{\hat{p}^2}{2m} + \frac{1}{2} m\omega^2 \hat{q}^2, \tag{2.1.17}$$

where $\hat{q}$ and $\hat{p}$ are the position and momentum operators, respectively, satisfying the canonical commutation relation $[\hat{q}, \hat{p}] = i\hbar$. Rather than proceeding to solve the Schrödinger equation with the Hamiltonian in this form, it is convenient to introduce the operator $\hat{a}$ and its hermitian conjugate $\hat{a}^\dagger$, defined as

$$\hat{a} = \frac{1}{\sqrt{2m\hbar\omega}} \left(m\omega\hat{q} + i\hat{p}\right) \tag{2.1.18}$$

$$\hat{a}^\dagger = \frac{1}{\sqrt{2m\hbar\omega}} \left(m\omega\hat{q} - i\hat{p}\right), \tag{2.1.19}$$

so that, conversely, the position and momentum operators may be written as

$$\hat{q} = \sqrt{\frac{\hbar}{2m\omega}} \left(\hat{a} + \hat{a}^\dagger\right) \tag{2.1.20}$$

$$\hat{p} = -i\sqrt{\frac{m\hbar\omega}{2}} \left(\hat{a} - \hat{a}^\dagger\right). \tag{2.1.21}$$

The operators $\hat{a}$ and $\hat{a}^\dagger$ are known as the creation and annihilation operators, respectively for reasons that will become clear as we proceed. It is straightforward to prove their commutation relations $\left[\hat{a}, \hat{a}^\dagger\right] = 1$ and $[\hat{a}, \hat{a}] = \left[\hat{a}^\dagger, \hat{a}^\dagger\right] = 0$. By performing the multiplication $\hat{a}^\dagger \hat{a}$, we can see that the Hamiltonian in Eq. (2.1.17) may be written as

$$\hat{H} = \hbar\omega \left(\hat{a}^\dagger \hat{a} + \frac{1}{2}\right). \tag{2.1.22}$$

In the Schrödinger picture of quantum mechanics, the eigenequation for a general energy eigenstate ψ_n with eigenvalue E_n is given by

$$\hat{H}\psi_n = E_n \psi_n. \tag{2.1.23}$$

With the above form of the Hamiltonian, it is easy to show the following commutation relations

$$\left[\hat{H}, \hat{a}^\dagger\right] = \hbar\omega\hat{a}^\dagger \quad \text{and} \quad \left[\hat{H}, \hat{a}\right] = -\hbar\omega\hat{a} \tag{2.1.24}$$

and combining these relations with Eq. (2.1.23), we can show that operating on ψ_n with $\hat{H}\hat{a}^\dagger$ yields the following eigenequation

$$\hat{H}\hat{a}^\dagger\psi_n = (\hbar\omega + E_n)\hat{a}^\dagger\psi_n \tag{2.1.25}$$

such that $\hat{a}^\dagger\psi_n$ is an eigenfunction of $\hat{H}$ with eigenvalue $(E_n - \hbar\omega)$. Instead, if we operate on ψ_n with $\hat{H}\hat{a}$, we find that $\hat{a}\psi_n$ is an eigenvalue of $\hat{H}$ with eigenvalue $(E_n - \hbar\omega)$. These relations tell us that the energy of the oscillator comes in discrete packets which can either be removed or added by application of the operator $\hat{a}$ or $\hat{a}^\dagger$, respectively, hence their names. Sometimes in the literature, these operators are referred to as the ladder operators as the energy of the harmonic oscillator can be viewed as a ladder of equally-spaced levels. It can be shown that the bottom rung of the ladder, corresponding to the lowest energy E_0 of the oscillator, is equal to $\hbar\omega/2$. This value is known as the zero-point energy and it is a purely quantum mechanical artefact. It will become clear later that the zero-point energy represents the important vacuum fluctuations in the quantization of the electromagnetic field that are an intrinsic property described by the Heisenberg uncertainty principle [30].

2.1.3 Quantization of the electromagnetic field and the quadrature operators

With an overview of classical electromagnetism and the quantum harmonic oscillator behind us, we now turn our attention to the quantization of the electromagnetic field that is crucial in a complete understanding of the concepts to be introduced in the upcoming chapters. Our starting point is the energy of a single mode of the electromagnetic field labeled $\mathbf{k}\lambda$ within a volume V averaged over an optical cycle, which is given by

$$H = \frac{1}{2}\int_V \left(\epsilon_0\mathbf{E}^2 + \frac{\mathbf{B}^2}{\mu_0}\right) \mathrm{d}^3\mathbf{r} = 2V\epsilon_0\omega^2 A_{\mathbf{k}\lambda}A^*_{\mathbf{k}\lambda}. \tag{2.1.26}$$

It is clear from this expression that the energy of the electromagnetic field looks identical to that of a harmonic oscillator with position and momentum coordinates q and p, respectively given by $(p^2/m + m\omega^2 q^2)/2$. Noting that the generalization to multiple modes is attained as the sum of the energy contributions of each mode, we can achieve quantization of the field by treating each field mode as a quantum harmonic oscillator with canonically-conjugate phase-space coordinates $\hat{q}_{\mathbf{k}\lambda}$ and $\hat{p}_{\mathbf{k}\lambda}$. We may then define a pair of dimensionless operators known as the *quadrature operators* or, simply, the *quadratures*,

$$\hat{Q}_{\mathbf{k}\lambda} = \sqrt{\frac{2m\omega}{\hbar}}\hat{q}_{\mathbf{k}\lambda} = \left(\hat{a}_{\mathbf{k}\lambda} + \hat{a}^{\dagger}_{\mathbf{k}\lambda}\right), \quad \hat{P}_{\mathbf{k}\lambda} = \sqrt{\frac{2}{m\hbar\omega}}\hat{p}_{\mathbf{k}\lambda} = -i\left(\hat{a}_{\mathbf{k}\lambda} - \hat{a}^{\dagger}_{\mathbf{k}\lambda}\right). \quad (2.1.27)$$

In terms of the quadrature operators, the creation and annihilation operators may be written as

$$\hat{a}_{\mathbf{k}\lambda} = \frac{1}{2}\left(\hat{Q}_{\mathbf{k}\lambda} + i\hat{P}_{\mathbf{k}\lambda}\right), \quad \hat{a}^{\dagger}_{\mathbf{k}\lambda} = \frac{1}{2}\left(\hat{Q}_{\mathbf{k}\lambda} - i\hat{P}_{\mathbf{k}\lambda}\right). \quad (2.1.28)$$

The quadratures obey the dimensionless canonical commutation relation $\left[\hat{Q}_{\mathbf{k}\lambda}, \hat{P}_{\mathbf{k}\lambda}\right] = 2i$, hence their definition can be thought of as setting $\hbar = 2$. In the following chapters, we use this convention exclusively, but it is important to note, especially in the interest of readers unfamiliar with the field, that many others are employed in the literature, including but not limited to $\hbar = 1$ and $\hbar = 1/2$. Henceforth, we will exclusively use the quadrature operators when referring to the quantized electromagnetic field, and we will use the lowercase notation $\hat{q}_{\mathbf{k}\lambda}$ and $\hat{p}_{\mathbf{k}\lambda}$ which is most common in the literature.

We are now able to express formulae for the quantum operators describing field potential by replacing the classical field amplitudes $A_{\mathbf{k}\lambda}$ and $A^*_{\mathbf{k}\lambda}$ in Eq. (2.1.12) with their quantum counterparts. We have

$$\hat{A}_{\mathbf{k}\lambda} \rightarrow A_0\hat{a}_{\mathbf{k}\lambda} \quad \text{and} \quad \hat{A}^*_{\mathbf{k}\lambda} \rightarrow A_0\hat{a}^{\dagger}_{\mathbf{k}\lambda}. \quad (2.1.29)$$

The constant A_0, containing all of the dimensional pre-factors, is given by $A_0 = (\hbar/2\epsilon_0\omega_k)^{1/2}$. We may then write the quantized vector potential in analogy with Eq. (2.1.12) as

$$\hat{A}_{\mathbf{k}\lambda} = A_0\left[\hat{a}_{\mathbf{k}\lambda}e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} + \hat{a}^{\dagger}_{\mathbf{k}\lambda}e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)}\right] \quad (2.1.30)$$

and with equations (2.1.15) and (2.1.16), we obtain the quantized electric and magnetic field operators, respectively,

$$\hat{E}_{\mathbf{k}\lambda} = E_0 \left[\hat{a}_{\mathbf{k}\lambda} e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} + \hat{a}^{\dagger}_{\mathbf{k}\lambda} e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)}\right] \tag{2.1.31}$$

$$\hat{B}_{\mathbf{k}\lambda} = B_0 \left[\hat{a}_{\mathbf{k}\lambda} e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} + \hat{a}^{\dagger}_{\mathbf{k}\lambda} e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)}\right], \tag{2.1.32}$$

with $E_0 = \omega_k A_0$ and $B_0 = A_0$. The importance of the quadrature operators becomes clear when they are used to express the electric field operator of a single mode labeled $\mathbf{k}\lambda$. We have

$$\hat{E}_{\mathbf{k}\lambda} = E_0 \left[\hat{q}_{\mathbf{k}\lambda} \cos(\omega_k t - \mathbf{k}\cdot\mathbf{r}) + \hat{p}_{\mathbf{k}\lambda} \sin(\omega_k t - \mathbf{k}\cdot\mathbf{r})\right]. \tag{2.1.33}$$

The quadrature operators represent the in- and out-of-phase components of the field that, unlike the creation and annihilation operators, are observable quantities that can be measured with respect to a reference field. With the aid of Eq. (2.1.28), the Heisenberg uncertainty relation for the quadrature operators can be shown to be

$$\left\langle(\Delta\hat{q}_{\mathbf{k}\lambda})^2\right\rangle \left\langle(\Delta\hat{p}_{\mathbf{k}\lambda})^2\right\rangle \geq \frac{1}{4}\left\langle[\hat{q}_{\mathbf{k}\lambda}, \hat{p}_{\mathbf{k}\lambda}]\right\rangle = 1. \tag{2.1.34}$$

The minimum uncertainty implied by this equation corresponds to the variance of the quantum vacuum fluctuations that are always present due to the laws of quantum mechanics, analogous to the zero-point energy of the quantum harmonic oscillator. In the next section, we will explore the quadrature operators in more detail and consider the energy eigenstates of the field in more detail.

2.2 Phase-space representation

After the brief introduction of the quadrature operators in the previous section, let us take some time to introduce some of their key properties. For convenience, we will consider a single mode with a single polarization such that the operators are labeled $\hat{q}$ and $\hat{p}$.

1. The eigenvalue equations for the operators are given by

$$\hat{q}\left|q\right\rangle = q\left|q\right\rangle \quad \text{and} \quad \hat{p}\left|p\right\rangle = p\left|p\right\rangle, \tag{2.2.35}$$

where $q \in \mathbb{R}$ and $p \in \mathbb{R}$. The eigenstates have unbounded and continuous spectra, hence they are not normalizable and therefore nonphysical. Nevertheless, they are useful as a tool in a variety of applications.

2. They are complete

$$\int_{-\infty}^{+\infty} |q\rangle \langle q| \,\mathrm{d}q = 1, \qquad \int_{-\infty}^{+\infty} |p\rangle \langle p| \,\mathrm{d}p = 1. \tag{2.2.36}$$

3. They are related to one-another by Fourier transform

$$|q\rangle = \frac{1}{2\sqrt{\pi}} \int e^{-iqp/2} |p\rangle \,\mathrm{d}p\,, \quad |p\rangle = \frac{1}{2\sqrt{\pi}} \int e^{iqp/2} |q\rangle \,\mathrm{d}q\,. \tag{2.2.37}$$

In order to establish a general notation for multi-mode light in terms of the quadrature operators, we can group the operators labeled $\hat{q}_i$ and $\hat{p}_i$ into a single operator $\hat{\mathbf{x}}$ such that, for a system of n modes, we have

$$\hat{\mathbf{x}} = (\hat{q}_1, \hat{p}_1, \ldots, \hat{q}_n, \hat{p}_n)^{\mathsf{T}}\,. \tag{2.2.38}$$

In line with the relationship in Eq. (2.2.35), the eigenequation for the vector operator is simply

$$\hat{\mathbf{x}} |\mathbf{x}\rangle = \mathbf{x}^{\mathsf{T}} |\mathbf{x}\rangle \tag{2.2.39}$$

where $\mathbf{x} \in \mathbb{R}^{2N}$. The commutation relation for the operator becomes

$$\left[\hat{\mathbf{x}}, \hat{\mathbf{x}}^{\mathsf{T}}\right] = 2i\boldsymbol{\Omega}, \tag{2.2.40}$$

where $\boldsymbol{\Omega}$ is known as the *symplectic form*, defined for N modes as

$$\boldsymbol{\Omega} = \bigoplus_{k=1}^{N} \boldsymbol{\Omega}_1 \quad \text{with} \quad \boldsymbol{\Omega}_1 := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{2.2.41}$$

The description of a multimode state is most easily visualised in the phase space in terms of the Wigner quasi-probability distribution which, for a general N-mode state of light, is given by

$$W(\mathbf{x}) = \frac{1}{(2\pi)^{2N}} \int_{\mathbb{R}^{2N}} \exp\left(-i\mathbf{x}^{\mathsf{T}} \Omega \boldsymbol{\xi}\right) \chi(\boldsymbol{\xi}) \,\mathrm{d}^{2N}\boldsymbol{\xi}\,, \tag{2.2.42}$$

where $\boldsymbol{\xi} \in \mathbb{R}^{2N}$ and $\chi(\boldsymbol{\xi})$ is the Wigner characteristic function, which, for a state $\hat{\rho}$ is given by

$$\chi(\boldsymbol{\xi}) = \mathrm{tr}\left[\hat{\rho} D(\boldsymbol{\xi})\right], \quad D(\boldsymbol{\xi}) := \exp\left(i\hat{\mathbf{x}}^{\mathsf{T}} \boldsymbol{\Omega} \boldsymbol{\xi}\right), \tag{2.2.43}$$

where $D(\boldsymbol{\xi})$ is the Weyl operator and $\mathrm{tr}(\hat{\rho}O) = \sum_i \langle\psi_i|\hat{\rho}O|\psi_i\rangle$ for an operator O where $\{|\psi_i\rangle\}$ is an orthonormal basis spanning the Hilbert space of $\hat{\rho}$. The Wigner function is always normalized to unity but holds its status as a quasi-probability distribution due to the fact it is generally non-positive. As with any statistical distribution, the Wigner function is characterized by its statistical moments. The first moment is the mean value, which is given by

$$\bar{\mathbf{x}} := \langle\hat{\mathbf{x}}\rangle = \mathrm{tr}\left(\hat{\mathbf{x}}\hat{\rho}\right) \tag{2.2.44}$$

while the second is called the covariance matrix (CM) $\mathbf{V}$, whose elements V_{ij} are defined as

$$V_{ij} := \frac{1}{2}\left\langle\{\Delta\hat{x}_i, \Delta\hat{x}_j\}\right\rangle, \tag{2.2.45}$$

where $\Delta\hat{x}_i := \hat{x}_i - \langle\hat{x}_i\rangle$ and $\{\hat{A},\hat{B}\} = \hat{A}\hat{B} + \hat{B}\hat{A}$ is the anticommutator. The CM of an N-mode state is a $2N\times 2N$ symmetric and positive definite ($\mathbf{V} > 0$) matrix that satisfies the uncertainty principle $\mathbf{V} + i\mathbf{\Omega} \geq 0$.

2.3 Fock representation

The Fock representation (or photon number state representation) is a method of representing quantum states of light based on the harmonic oscillator model. We begin with the states $|n\rangle$ which are the energy eigenstates of the quantum harmonic oscillator with n excited quanta in a mode of angular frequency ω that satisfy the eigenequation

$$\hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right)|n\rangle = \hbar\omega\left(\frac{\hat{q}^2 + \hat{p}^2}{4} + \frac{1}{2}\right)|n\rangle = E_n|n\rangle = \left(n + \frac{1}{2}\right)\hbar\omega\,|n\rangle\,, \tag{2.3.46}$$

where $\hat{a}^\dagger$ and $\hat{a}$ are the creation and annihilation operators for the mode and $\hat{q}$ and $\hat{p}$ are its quadrature operators. We can see immediately that if no quanta are excited, the *zero-point energy* of the oscillator is equal to $\hbar\omega/2$. In the quantized electromagnetic field picture, the states are called Fock states, and a Fock state $|n\rangle$ represents a monochromatic field containing n photons. As mentioned previously, the zero-point energy in this picture represents the inherent quantum mechanical vacuum fluctuations that can be observed in detectors with no incoming photons. The key properties of Fock states can be summarized as follows

1. The Fock states form an orthonormal basis and thus satisfy the relation

$$\langle n|n'\rangle = \delta_{nn'}. \tag{2.3.47}$$

2. Despite forming an infinite set, they are complete

$$\sum_{n=0}^{\infty} |n\rangle \langle n| = 1. \tag{2.3.48}$$

3. In the Fock representation, the creation and annihilation operators are defined according to the following relations

$$\hat{a}^{\dagger} |n\rangle = \sqrt{n+1}\, |n+1\rangle \tag{2.3.49}$$

$$\hat{a} |n\rangle = \sqrt{n}\, |n-1\rangle \,. \tag{2.3.50}$$

Applying the creation operator to Eq. (2.3.50) yields the following result

$$\hat{a}^{\dagger}\hat{a} |n\rangle = \hat{n} |n\rangle = n |n\rangle \,, \tag{2.3.51}$$

where $\hat{n}$ is called the number operator and, when applied to the state $|n\rangle$, it yields the number of photons n.

2.4 Gaussian quantum optics

In this section, we will introduce the Gaussian states of the electromagnetic field, which are a particularly important and useful subset of optical quantum states. The definition of a Gaussian state follows naturally from our discussion of the phase-space representation. It is simply a state that can be completely characterized by the first and second moments of the Wigner distribution, such that $\hat{\rho} = \hat{\rho}(\bar{\mathbf{x}}, \mathbf{V})$ where $\bar{\mathbf{x}}$ and $\mathbf{V}$ are the mean value and CM of the state, respectively. The characteristic function of a Gaussian state takes the following form

$$\chi(\boldsymbol{\xi}) = \exp\left[\frac{1}{2}\boldsymbol{\xi}^{\mathsf{T}}\left(\boldsymbol{\Omega}\mathbf{V}\boldsymbol{\Omega}^{\mathsf{T}}\right)\boldsymbol{\xi} - i(\boldsymbol{\Omega}\bar{\mathbf{x}})^{\mathsf{T}}\boldsymbol{\xi}\right] \tag{2.4.52}$$

such that the Wigner function is, by definition, Gaussian

$$W(\mathbf{x}) = \frac{1}{(2\pi)^{2N}\sqrt{\det \mathbf{V}}} \exp\left[-\frac{1}{2}\left(\mathbf{x}-\bar{\mathbf{x}}\right)^{\mathsf{T}}\mathbf{V}^{-1}\left(\mathbf{x}-\bar{\mathbf{x}}\right)\right], \tag{2.4.53}$$

where N is the number of modes. Gaussian states are of particular importance in this thesis and more generally in the field of quantum optics and quantum information theory as a whole. Their mathematical description is straightforward in terms of Gaussian functions and their evolution is described with Gaussian unitary transformations. Moreover, many important states relevant to CV QKD are Gaussian, as we will describe in the following sections.

The most important definition relevant to Gaussian states is the symplectic decomposition. Williamson's theorem states that every positive-definite real matrix of even dimension can be put into diagonal form by a symplectic transformation [31]. Recall that any N-mode CM $\mathbf{V}$ is a positive-definite real matrix and can, therefore, be expressed as

$$\mathbf{V} = \mathbf{S}\mathbf{V}^{\oplus}\mathbf{S}^{\mathsf{T}}, \quad \mathbf{V}^{\oplus} := \bigoplus_{i=1}^{N} \nu_i \mathbf{I}, \tag{2.4.54}$$

where $\mathbf{I}$ is the $2{\times}2$ identity matrix and $\mathbf{V}^{\oplus}$ is called the Williamson form of the matrix $\mathbf{V}$. The set of N real numbers $\{\nu_i\}$ is called the symplectic spectrum of $\mathbf{V}$ and the elements, called the symplectic eigenvalues, satisfy the condition $\nu_i \geq 1$. They can be obtained in identical pairs by taking the absolute values of the eigenvalues of the matrix $i\mathbf{\Omega}\mathbf{V}$, where $\mathbf{\Omega}$ is the symplectic form given in Eq. (2.2.41). We will see that this important property is the key to the simplicity of the mathematical description of Gaussian states. In the following sections, we will introduce some of the most common Gaussian states and operations which are made use of frequently throughout the following chapters.

2.4.1 Vacuum and thermal states

The most fundamental Gaussian state is the vacuum state, which has the lowest possible energy allowed by quantum mechanics. It is the eigenstate of the annihilation operator with zero eigenvalue ($\hat{a}\left|0\right\rangle = 0$) and it contains zero photons. As a result, its CM is simply the identity matrix. In the phase space, vacuum states are represented by a circle of unit radius which corresponds to the smallest variance allowed by the uncertainty principle (cf. Eq. (2.1.34))

Excited states of light are known thermal states. They are parameterized by a mean number of photons $\bar{n}$ and their CM is given by $\mathbf{V} = (2\bar{n}+1)\mathbf{I}$ where $\mathbf{I}$ is the 2×2 identity matrix. In the Fock basis, a thermal state takes the form

$$\hat{p}^{\text{th}}(\bar{n}) = \sum_{n=0}^{\infty} \frac{\bar{n}^n}{(\bar{n}+1)^{n+1}} \left|n\right\rangle \left\langle n\right| \tag{2.4.55}$$

and, in phase space representation, it is represented by a circle of radius $2\bar{n}+1$.

2.4.2 Coherent states and the displacement operator

The coherent state, represented by $|\alpha\rangle$ is the quantum state that most resembles the classical behavior of light and is equivalent to a classical monochromatic wave. As such, it is a minimum uncertainty state that saturates the uncertainty principle. To describe the mathematics of the coherent state we first introduce the displacement operator, whose action is to displace a state in the phase space. It is defined as

$$D(\alpha) := \exp\left(\alpha\hat{a}^\dagger - \alpha^*\hat{a}\right), \tag{2.4.56}$$

where α is the (complex) magnitude of the displacement. It can be shown that application of the displacement operator on the creation and annihilation operators shifts them by an amount α as

$$D^\dagger(\alpha)\hat{a}D(\alpha) = \hat{a} + \alpha \tag{2.4.57}$$

$$D^\dagger(\alpha)\hat{a}^\dagger D(\alpha) = \hat{a}^\dagger + \alpha^*. \tag{2.4.58}$$

The coherent state is obtained simply by operating on a vacuum state with the displacement operator such that $|\alpha\rangle = D(\alpha)|0\rangle$. It is straightforward to show that a coherent state $|\alpha\rangle$ is an eigenvector of the annihilation operator $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$ and it is readily expressed in the Fock basis as

$$|\alpha\rangle = \exp\left(-\frac{1}{2}|\alpha|^2\right) \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \tag{2.4.59}$$

We can see that the average number of photons, $\bar{n} = \langle\alpha|\hat{n}|\alpha\rangle = |\alpha|^2$ and we can write the probability of observing n photons when performing a photon-number measurement on a coherent state, $p(n)$, as

$$p(n) = |\langle n|\alpha\rangle|^2 = \frac{\bar{n}^n}{n!}e^{-\bar{n}}, \tag{2.4.60}$$

which is a Poisson distribution.

2.4.3 Squeezed states of light

Squeezed states are a particular group of states of light that exhibit quadrature uncertainty less than that associated with the vacuum fluctuations. The term squeezed refers to the fact that the uncertainty circle of the state in the phase-space is 'squeezed' in a particular direction. In accordance with the uncertainty principle, the uncertainty in the conjugate direction is simultaneously increased, or 'anti-squeezed' such that the area of uncertainty remains constant. In this section, we will outline the Gaussian operations which generate squeezed states for either one or two modes. This discussion will lead us to the important notion of two-mode squeezed vacuum states which exhibit Einstein-Podolski-Rosen (EPR) correlations and are the main source of entanglement in quantum optics.

Single-mode squeezing

The process of generating squeezed states is complex, requiring non-linear optical methods. For single-mode squeezing, the underlying method is degenerate optical parametric amplification (OPA), in which a second-order non-linear crystal is placed between two or more mirrors in order to form an optical resonator. The resonator is pumped with bright laser light of frequency 2ω and combined with a signal mode of frequency ω. The non-linearity of the crystal causes the electric field of the signal to be either amplified or deamplified depending on its phase relative to the pump laser, resulting in the mode being squeezed in the phase or amplitude quadrature, respectively. The Gaussian single-mode squeezing operator describing this process is defined as

$$S(r) := \exp\left[\frac{r}{2}\left(\hat{a}^2 - \hat{a}^{\dagger 2}\right)\right], \tag{2.4.61}$$

where r is called the squeezing parameter. If the signal mode is simply the vacuum, we obtain a squeezed vacuum state, which, in the Fock basis, can be written as

$$|0, r\rangle = S(r)\,|0\rangle = \frac{1}{\sqrt{\cosh r}} \sum_{n=0}^{\infty} \frac{\sqrt{(2n)!}}{2^n n!} \tanh r^n \,|2n\rangle\,. \tag{2.4.62}$$

Two-mode squeezing and continuous-variable entanglement

A two-mode squeezed state is one that exhibits uncertainty below that of the vacuum fluctuations in a linear combination of the quadratures of the two fields of a two-mode system. The usual process for generating two-mode squeezed light is non-degenerate OPA in which a non-linear crystal is pumped with laser light as well as light from signal and idler modes. The interaction is described by the Gaussian two-mode squeezing operator, defined as

$$S_2(r) := \exp\left[\frac{r}{2}\left(\hat{a}\hat{b} - \hat{a}^\dagger\hat{b}^\dagger\right)\right], \tag{2.4.63}$$

where $\hat{a}$ and $\hat{b}$ are the annihilation operators of the two modes and r quantifies the two-mode squeezing. If we apply the two-mode squeezing operator to a pair of vacuum modes, we obtain a *two-mode squeezed vacuum (TMSV) state*. In the Fock basis, this process is represented as

$$\begin{aligned} |r\rangle_{\text{TMSV}} &= S_2(r)\left(|0\rangle_a \otimes |0\rangle_b\right) & (2.4.64)\\ &= \sqrt{1-\lambda^2}\sum_{n=0}^{\infty}(-\lambda)^n |n\rangle_a |n\rangle_b\,, & (2.4.65)\end{aligned}$$

where $\lambda = \tanh r$. The TMSV state is particularly important as it exhibits EPR correlations between the quadratures. For this reason, it is a form of continuous-variable entanglement. In the limit $r \to \infty$, we have perfect correlation between the quadratures, and the state is analogous that of two maximally entangled qubits A and B, i.e. one of the following Bell states

$$\begin{aligned} |\Phi^\pm\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle_A \otimes |0\rangle_B \pm |1\rangle_A \otimes |1\rangle_B\right) & (2.4.66)\\ |\Psi^\pm\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle_A \otimes |1\rangle_B \pm |1\rangle_A \otimes |0\rangle_B\right). & (2.4.67)\end{aligned}$$

In the quadrature picture, the CM of a TMSV state, $\mathbf{V}_{\text{TMSV}}$ is parameterised by the variance $\mu = \cosh 2r$. It is given by

$$\mathbf{V}_{\text{TMSV}}(\mu) = \begin{pmatrix} \mu\mathbf{I} & \sqrt{\mu^2-1}\mathbf{Z} \\ \sqrt{\mu^2-1}\mathbf{Z} & \mu\mathbf{I} \end{pmatrix}, \tag{2.4.68}$$

where $\mathbf{I}$ is the 2×2 identity matrix and $\mathbf{Z} := \text{diag}(1, -1)$. We will make use of this formalism frequently throughout the remainder of this thesis as it is of particular importance in CV QKD.

2.4.4 The beam splitter

The beam splitter is one of the most fundamental interactions in quantum optics which is useful in its own right as well as a simple model for several more complex optical devices. A beam splitter is simply a device in which two incoming beams interfere to produce two outgoing beams. The beam splitter interaction is described by a Gaussian unitary operation defined as

$$B(\theta) = \exp\left[\theta\left(\hat{a}^\dagger\hat{b} - \hat{a}\hat{b}^\dagger\right)\right], \tag{2.4.69}$$

where $\hat{a}$ and $\hat{b}$ are the annihilation operators of the incoming beams. The interaction is characterised by transmissivity of the beam splitter, $\tau = \cos^2\theta$. The operation transforms the quadrature operators $\hat{\mathbf{r}}$ as

$$\hat{\mathbf{x}} \to \mathbf{B}(\tau)\hat{\mathbf{x}}, \quad \mathbf{B}(\tau) := \begin{pmatrix} \sqrt{\tau}\mathbf{I} & \sqrt{1-\tau}\mathbf{I} \\ -\sqrt{1-\tau}\mathbf{I} & \sqrt{\tau}\mathbf{I} \end{pmatrix}, \tag{2.4.70}$$

such that the mean value and CM transform as $\bar{\mathbf{x}} \to \mathbf{B}(\tau)\bar{\mathbf{x}}$ and $\mathbf{V} \to \mathbf{B}(\tau)\mathbf{V}\mathbf{B}(\tau)^\mathsf{T}$. This transformation can easily be generalized to an n-mode system of which two modes interact by adding identity blocks in the relevant locations.

2.4.5 Measuring Gaussian states

A measurement process is an essential tool in any quantum protocol. It allows us to extract usable information from any quantum system. Fortunately, in the case of continuous-variable states of light, the measurement process is relatively straightforward and is performed almost exclusively with homodyne detectors. For Gaussian states, in particular, the description of not only the measurement outcome but the post-measurement quantum state has a particularly soluble mathematical form based on the mean value and CM of the signal state. This section will serve as a complete introduction to this mathematical framework that is of the utmost importance in a full understanding of continuous-variable quantum mechanics.

Homodyne detection

The homodyne detector apparatus usually consists of a balanced beam splitter and two photodiodes. At the beam splitter, a signal mode, S, is mixed with a *local* *oscillator* of equivalent frequency. The amplitude of the local oscillator must be much larger than that of the signal, so that we may make the assumption that it behaves classically and its intensity can, therefore, be accurately obtained without disrupting the system.

Let us consider a general n-mode Gaussian state with CM $\mathbf{V}$ that can be written as

$$\mathbf{V}_{AB} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^{\mathsf{T}} & \mathbf{B} \end{pmatrix}, \tag{2.4.71}$$

where $\mathbf{A}$ is the CM of the $(n-1)$-mode subsystem A, $\mathbf{B}$ is the CM of the mode B to be measured and $\mathbf{C}$ is the correlation between the subsystems. The corresponding mean value is $\bar{\mathbf{x}}_{AB} = (\bar{\mathbf{x}}_A, \bar{\mathbf{x}}_B)^{\mathsf{T}}$ where $\bar{\mathbf{x}}_{A(B)}$ is the mean value of subsystem A(B). Let us now assume that mode B is measured with homodyne detection with outcome β. It can be shown that the post-measurement CM of the system becomes [18]

$$\mathbf{V}_{A|\beta} = \mathbf{A} - \mathbf{C}\left(\mathbf{\Pi}\mathbf{B}\mathbf{\Pi}\right)^{-1}\mathbf{C}^{\mathsf{T}}, \tag{2.4.72}$$

where, for q-quadrature detection, $\mathbf{\Pi} = \mathrm{diag}(1,0)$ and, for p-quadrature detection, $\mathbf{\Pi} = \mathrm{diag}(0,1)$. As $\mathbf{\Pi}\mathbf{B}\mathbf{\Pi}$ is singular, $(\mathbf{\Pi}\mathbf{B}\mathbf{\Pi})^{-1}$ is a pseudoinverse (Moor-Penrose inverse) which, for square diagonal matrices such as this, is obtained by taking the reciprocal of each non-zero element[1]. The pseudoinverse is applicable in this case as the measurement has no support in the quadrature conjugate to that which is being measured.

The mean value of the larger system is also affected by the measurement process, after which it takes the following form

$$\bar{\mathbf{x}}_{A|\beta} = \bar{\mathbf{x}}_A - \mathbf{C}\left(\mathbf{\Pi}\mathbf{B}\mathbf{\Pi}\right)^{-1}\mathbf{d}^{\mathsf{T}} \tag{2.4.73}$$

where $\mathbf{d} = \bar{\mathbf{x}}_B - (\beta, 0)^{\mathsf{T}}$ and $\mathbf{d} = \bar{\mathbf{x}}_B - (0, \beta)^{\mathsf{T}}$ for q- and p-quadrature detection, respectively. Finally, the probability of obtaining outcome β upon measurement of

[1] The pseudoinverse of a general matrix M can be obtained by performing singular value decomposition $M = U\Sigma V^*$ such that $M^{-1} = V\Sigma^{-1}U^*$. The pseudoinverse of the rectangular diagonal matrix Σ is obtained by taking the reciprocal of each non-zero diagonal element then taking the transpose of the matrix.

a given quadrature is obtained by integrating the Wigner function $W(q,p)$ over the conjugate quadrature

$$p(\beta) = \int_{-\infty}^{+\infty} W(\beta, p)\,\mathrm{d}p\,, \quad \text{or} \quad p(\beta) = \int_{-\infty}^{+\infty} W(q, \beta)\,\mathrm{d}q\,. \tag{2.4.74}$$

The result can be conveniently expressed in the following form

$$p(\beta) = \frac{1}{\sqrt{2\pi}\sqrt{\det(\mathbf{\Pi B \Pi})}} \exp\left[-\frac{1}{2}\mathbf{d}^{\mathsf{T}}(\mathbf{\Pi B \Pi})^{-1}\mathbf{d}\right], \tag{2.4.75}$$

where $\mathbf{\Pi}$ and $\mathbf{d}$ are defined above. While the efficiencies of modern-day homodyne detectors are particularly high, the detection cannot be implemented with ideal precision. Detector inefficiencies are usually modelled by a beam splitter with a transmissivity that coincides with the efficiency of the detector, which mixes an incoming signal with the vacuum. The transmitted mode is then measured with an ideal detector described by the above formalism.

Heterodyne detection

Homodyne detection can be used to measure a single quadrature of the electromagnetic field, but how can we measure both quadratures of the mode at the same time? The answer to this question is provided by a technique called heterodyne detection. The detection scheme can be seen as follows. The signal mode first passes through a beam splitter where it is mixed with the vacuum. This process effectively duplicates the mode, with the caveat that an extra unit of noise is injected. The outputs from each port of the beam splitter are subsequently measured in independent homodyne detectors.

The mathematical description of the post-measurement CM and mean value can be broached in a similar manner to that of homodyne detection and our starting point again is Eq. (2.4.71). The post-measurement CM of system A after mode B is measured with heterodyne detection with outcome $\boldsymbol{\beta}$ has been shown to be [32]

$$\mathbf{V}_{A|\boldsymbol{\beta}} = \mathbf{A} - \mathbf{C}\,(\mathbf{B} + \mathbf{I})^{-1}\,\mathbf{C}^{\mathsf{T}}, \tag{2.4.76}$$

where the addition of the identity accounts for the additional unit of vacuum noise introduced and is thus specific to our choice of normalization convention. Note that the post-measurement CM is again independent of the measurement outcome, which only appears in the mean value of the remaining system that is given by

$$\bar{\mathbf{x}}_{A|\boldsymbol{\beta}} = \bar{\mathbf{x}}_A - \mathbf{C}\left(\mathbf{B}+\mathbf{I}\right)^{-1}\mathbf{d}, \tag{2.4.77}$$

where $\bar{\mathbf{x}}_A$ is the mean value of the $(n-1)$-mode system A, $\mathbf{d} = \bar{\mathbf{x}}_B - \boldsymbol{\beta}$ and $\boldsymbol{\beta} = (\beta_q, \beta_p)^{\mathsf{T}}$ is the measurement outcome with β_q and β_p being the individual measurement outcomes of the q- and p-quadratures, respectively. Finally, the probability associated with outcome $\boldsymbol{\beta}$ is given by

$$p(\boldsymbol{\beta}) = \frac{\exp\left[-\frac{1}{2}\mathbf{d}^{\mathsf{T}}\left(\mathbf{B}+\mathbf{I}\right)^{-1}\mathbf{d}\right]}{2\pi\sqrt{\det\left(\mathbf{B}+\mathbf{I}\right)}}. \tag{2.4.78}$$

2.5 Measures of information for classical and quantum ensembles

The inherently probabilistic nature of quantum mechanics necessitates a strong understanding of the fundamentals of probability theory to its readers. We will use this section to introduce important definitions from information theory that arise frequently in our forthcoming analysis of QKD protocols and quantum networks. We will then introduce measures of analyzing quantum states and how they pertain to our study of quantum information theory.

2.5.1 Shannon entropy

Perhaps the most important quantity from information theory that we must introduce is the entropy of a random variable, which quantifies the level of uncertainty in its possible outcomes. The concept of entropy was introduced by Claude Shannon [33] and is often referred to as the Shannon entropy, particularly when it is used in the context of binary information.

Definition 2.5.1 (Entropy) *Let X a random variable with corresponding alphabet $\mathcal{X}$ and probability mass function $p(x)$. The entropy of X is given by*

$$H(X) = -\sum_{x\in\mathcal{X}} p(x)\log p(x). \tag{2.5.79}$$

The base of the logarithm in Eq. (2.5.79) should be selected depending on the particular problem being considered, for example, base-2 for bits and base-e for nats. Let us consider a binary random variable X with probability $p = P\{X = 0\} \in [0, 1]$. Using Eq. (2.5.79) it is straightforward to see that the entropy reduces to

$$H(X) = H_2(X) = -p \log p - (1 - p) \log(1 - p), \tag{2.5.80}$$

where $H_2(\cdot)$ is known as the binary entropy function. This function will arise often throughout the following chapters.

Up to this point, we have only considered discrete variables in our discussion. Let us now introduce the differential entropy which allows us to compute the entropy of a continuous random variable.

Definition 2.5.2 (Differential entropy) *Let X be a continuous random variable with probability density function $p(x)$. The differential entropy is defined as*

$$H(X) := -\int_{-\infty}^{+\infty} p(x) \log p(x)\, \mathrm{d}x\,. \tag{2.5.81}$$

The modification is rather straightforward but worthy of inclusion in this discussion as a demonstration of the process required to compute the statistical quantities of continuous variables. The next quantity is somewhat less trivial but of great importance in the upcoming chapters.

Definition 2.5.3 (Conditional entropy) *Let X and Y be random variables with probability mass functions $p(x)$ and $p(y)$. Let us also assume that $p(x|y)$ is a probability mass function which is discrete for every x. The conditional entropy of the distribution X given Y is defined as*

$$H(X|Y) = \sum_{y \in \mathcal{Y}} p(y) H(X|Y = y), \tag{2.5.82}$$

where $H(X|Y = y)$ is the entropy of random variable X conditioned on the outcome of random variable Y being y, given by

$$H(X|Y = y) = -\sum_{x \in \mathcal{X}} p(x|y) \log p(x|y). \tag{2.5.83}$$

For the remainder of the thesis we employ the shorthand notation $H_{X|y} \equiv H(X|Y = y)$ for brevity. The conditional entropy is a measure of the uncertainty on the variable X given the value of the variable Y. Clearly knowledge of Y cannot increase our uncertainty about X, hence we may write the inequality $H(X|Y) \leq H(X)$. The expression for the differential conditional entropy is readily obtained from this definition by replacing the probability mass functions with probability density functions and replacing the sums with integrals.

2.5.2 Mutual information

One statistical quantity that is encountered frequently in the study of quantum information theory is the mutual information between two random variables.

Definition 2.5.4 (Mutual information) *For two random variables X and Y with joint probability mass function $p(x, y)$, marginal distributions $p(x)$ and $p(y)$, and alphabets $\mathcal{X}$ and $\mathcal{Y}$, respectively, the mutual information is given by*

$$\begin{aligned} I(X : Y) &= \sum_{x\in\mathcal{X}} \sum_{y\in\mathcal{Y}} p(x, y) \log \frac{p(x, y)}{p(x)p(y)} && (2.5.84) \\ &= H(X) - H(X|Y) && (2.5.85) \\ &= H(Y) - H(Y|X). && (2.5.86) \end{aligned}$$

In short, the mutual information between two random variables is the amount of information attainable about one variable if the other is known. It is of particular importance in the study of QKD when attempting to estimate the information that the parties share as well as that which an eavesdropper may attain.

2.5.3 Von Neumann entropy

The von Neumann entropy (VNE) is the quantum generalization of the classical entropy which is derived by extending the classical definition from probability distributions to density matrices.

Definition 2.5.5 (Von Neumann entropy) *For a density matrix $\hat{\rho}_X$, the von*

Neumann entropy is defined as

$$S(X) := -\operatorname{tr}(\hat{\rho}_X \log \hat{\rho}_X) = -\sum_i \lambda_i \log \lambda_i \qquad (2.5.87)$$

where $\{\lambda_i\}$ are the eigenvalues of the state $\hat{\rho}_X$.

The VNE of a system X conditioned on the random variable Y with alphabet $\mathcal{Y}$ and probability mass function $p(y)$ is given in analogy with the conditional Shannon entropy by

$$S(X|Y) = \sum_{y\in\mathcal{Y}} p(y) S(\hat{\rho}_{X|y}) \qquad (2.5.88)$$

where $\hat{\rho}_{X|y}$ is the density matrix representing the variable X conditioned on the value y of the random variable Y. If the density matrix in question is that of an N-mode Gaussian state, $\hat{\rho} = \hat{\rho}(\bar{\mathbf{x}}, \mathbf{V})$, the VNE can be obtained straightforwardly in terms of the symplectic eigenvalues $\{\nu_i\}$ of the CM $\mathbf{V}$ by

$$S(\hat{\rho}) = \sum_{i=1}^{N} h(\nu_i) \qquad (2.5.89)$$

where

$$h(\nu) := \frac{\nu+1}{2} \log \frac{\nu+1}{2} - \frac{\nu-1}{2} \log \frac{\nu-1}{2}. \qquad (2.5.90)$$

2.5.4 Quantum relative entropy

Another important entropic quantity in quantum mechanics is the quantum relative entropy, which measures the distinguishability between two quantum states $\hat{\rho}$ and $\hat{\sigma}$

$$S(\hat{\rho}||\hat{\sigma}) := \operatorname{tr}\left[\hat{\rho}\left(\log \hat{\rho} - \log \hat{\sigma}\right)\right]. \qquad (2.5.91)$$

By taking the infimum of the quantum relative entropy over all states $\hat{\sigma}$ in some convex set, we obtain the relative entropy distance which measures the distance between $\hat{\rho}$ and the set of states. If this convex set is the set of separable states $\mathfrak{S}$, the relative entropy distance becomes the relative entropy of entanglement (REE) E_R [34],

$$E_R(\hat{\rho}) = \inf_{\hat{\sigma}\in\mathfrak{S}} S(\hat{\rho}||\hat{\sigma}). \qquad (2.5.92)$$

2.5.5 The Holevo bound

The last quantity that we will introduce is the Holevo bound (or Holevo information) χ which provides an upper bound on the maximum information attainable with any measurement.

Definition 2.5.6 (The Holevo Bound) *Let us suppose that party A prepares states $\hat{\rho}_x$ according to the random variable X with alphabet $\mathcal{X}$ and probability mass function $p(x)$. Party A sends states to party B, who observes the state $\hat{\rho} = \sum_{x \in \mathcal{X}} p(x)\hat{\rho}_x$ and performs measurements with outcomes forming the random variable Y. The mutual information between X and Y is bounded by the Holevo information χ such that*

$$I(X:Y) \leq \chi, \quad \chi := S(\hat{\rho}) - \sum_{x \in \mathcal{X}} p(x) S(\hat{\rho}_x). \tag{2.5.93}$$

The first term in the expression for χ is the total entropy of the system of party B and the second term is the conditional entropy, i.e. the entropy of the system given knowledge of the classical information. The difference, and thus the Holevo bound, is a measure of the inherent quantum information within the system. The bound appears in a variety of tasks within quantum information theory, particularly in QKD, where its importance cannot be overstated as it allows the security of a protocol to be determined under the strong assumption that an eavesdropper is performing the best possible measurement on their data. This allows us to consider some particularly strong eavesdropping regimes which may even exploit future quantum technologies.

2.6 Capacities of quantum channels and networks

The final tool we must add to our collection in order for a full understanding of the upcoming chapters takes us back to the foundational level of quantum information theory. We will examine the current state of the art of establishing the capacities of quantum channels and networks. Recently, substantial progress has been made in this field using a new channel simulation technique dubbed 'teleportation stretching' that we will introduce later. These ideas were first introduced by

Pirandola et al. [20] and used to establish the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound which provides the fundamental limit of repeaterless communications. Teleportation stretching is the foundational principle on which we will seek to establish bounds for quantum networking in the final chapter. We will, therefore, introduce the mathematical framework starting first with single quantum channels and progressing later to quantum networks.

2.6.1 A general adaptive protocol for quantum communication and general bounds

Before we proceed to compute bounds on the capacities of various quantum channels, we must outline a general communication protocol between two parties Alice and Bob separated by a quantum channel $\mathcal{E}$. We will consider the most general strategy which may be assisted by adaptive local operations and classical communications (LOCCs), which may be applied to Alice and Bob's local registers of quantum states, which we label **a** and **b**, respectively. Such a protocol can be summarized in the following steps [20]:

1. Alice and Bob prepare an initial state $\hat{\rho}^0_{ab}$ by applying a LOCC Λ_0 to their individual registers.

2. Alice sends a system a_1 from her register to Bob through the channel. Bob adds the received system b_1 to his register, $b_1\mathbf{b} \to \mathbf{b}$ and a further adaptive LOCC Λ_1 is applied by the parties yielding the output state $\hat{\rho}^1_{ab}$.

3. The process in step 2 is repeated for n uses of the channel, giving a series of LOCCs $\mathcal{P} = \{\Lambda_0, \ldots, \Lambda_n\}$ which characterizes the protocol. The final state of the combined system is, therefore, $\hat{\rho}^n_{ab}$.

The rate of the protocol is R_n if the output state $\hat{\rho}^n_{ab}$ after n transmissions is epsilon-close to a target state $\hat{\phi}_n$ in trace norm, i.e. $||\hat{\rho}^n_{ab} - \hat{\phi}_n|| \leq \epsilon$, with nR_n bits. The capacity of the quantum channel, $\mathcal{C}(\mathcal{E})$ is defined as the optimization over the set of LOCCs in the asymptotic limit of channel uses,

$$\mathcal{C}(\mathcal{E}) := \sup_{\mathcal{P}} \lim_{n} R_n \tag{2.6.94}$$

where $\mathcal{C}$ is a generic symbol for the two-way assisted capacity which can be, for example, the two-way entanglement-distribution capacity D_2, the two-way quantum capacity Q_2, the secret key capacity K or the two-way private capacity P_2 [35, 36].

We can now establish a weak bound on the capacity using the REE introduced in Sec. 2.5.4. Following the definitions of the REE and the relative entropy, the REE of a quantum channel is defined by [20]

$$E_R(\mathcal{E}) := \sup_{\hat{\rho}} E_R[\mathbf{I} \otimes \mathcal{E}(\hat{\rho})] \geq E_R(\hat{\rho}_{\mathcal{E}}), \tag{2.6.95}$$

where $\hat{\rho}_{\mathcal{E}}$ is called the *Choi matrix* of the channel, which is defined by

$$\hat{\rho}_{\mathcal{E}} := (\mathbf{I} \otimes \mathcal{E}) \left(\hat{\Phi}_{AB}\right) \tag{2.6.96}$$

where $\hat{\Phi}_{AB}$ is a maximally entangled (EPR) state with two sites A and B [8]. The Choi matrix is obtained by propagating site B of this state through the channel, leaving site A unchanged. These results lead to the general weak converse theorem [20]

Theorem 2.6.1 (Weak converse theorem) *At any dimension, finite or infinite, the generic two-way capacity of a quantum channel $\mathcal{E}$ is upper-bounded by the REE bound*

$$\mathcal{C}(\mathcal{E}) \leq E_R^{\star}(\mathcal{E}) := \sup_{\mathcal{P}} \lim_{n} \frac{E_R(\hat{\rho}^n_{ab})}{n}. \tag{2.6.97}$$

We will see in the upcoming sections that the weak converse theorem allows us to bound the capacity of a channel using the REE.

2.6.2 Channel simulation and teleportation covariance

Channel simulation is a well-known area of research in the field of quantum communication. It allows complex channels to be modeled with a relatively simple protocol, which has led to many important results. Until recently, the main idea behind channel simulation was teleportation simulation, which is only applicable to certain quantum channels. The first reference to channel simulation was by Bennett et al. [37] for the teleportation simulation of Pauli channels. Since then there has been much attention on the field yielding important and much more general results.

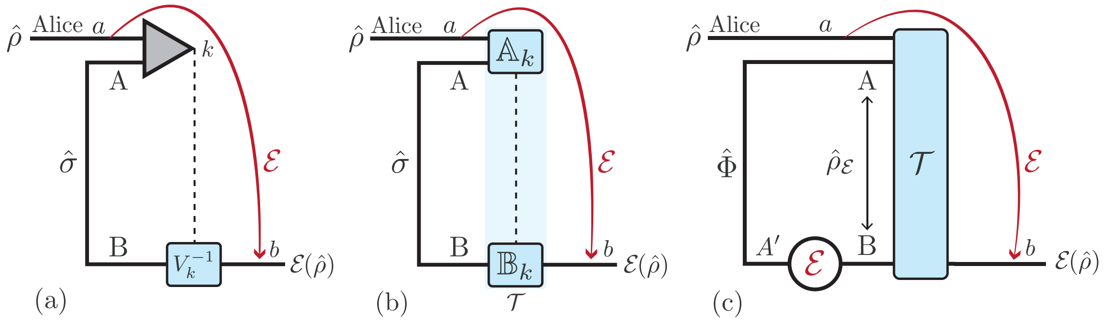

Figure 2.1: Schematic of the simulation of a quantum channel from teleportation simulation to simulation with a general LOCC. (a): Teleportation of Alice's system a in state $\hat{\rho}$ with resource state $\hat{\sigma}$ between two systems A and B. Bell detection is performed on the systems a and A with outcome k that is communicated to Bob who performs a corrective unitary V_k^{-1} undoing the teleportation unitary U_k to recover the original state. On average, performing this teleportation procedure is equivalent to applying a teleportation channel $\mathcal{E}$ from a to b. (b): The teleportation protocol can be replaced by an arbitrary LOCC $\mathcal{T}$. Bell detection is replaced by an arbitrary quantum operation $\mathbb{A}$ and classical information k is communicated to Bob who applies another arbitrary quantum operation $\mathbb{B}$. This protocol is equivalent to the simulation of a channel $\mathcal{E}$ as $\mathcal{E}(\hat{\rho}) = \mathcal{T}(\hat{\rho} \otimes \hat{\sigma})$ if the LOCC is averaged over all k so that it is trace-preserving. (c): If a channel can be simulated by a trace-preserving LOCC $\mathcal{T}$ applied to its Choi matrix $\hat{\rho}_\mathcal{E} := (\mathbf{I} \otimes \mathcal{E})(\hat{\Phi})$, it is said to be 'Choi stretchable'.

The recent work by Pirandola et al. [20] presented a radically new channel simulation formulation for completely arbitrary quantum channels. Moreover, the method is extended to the continuous- as well as discrete-variable formulation. It is this work that we will introduce below that will form the foundation of our analysis of quantum networks.

LOCC simulation of quantum channels

We will begin by considering the teleportation simulation of a channel as shown in Fig. 2.1(a). Alice and Bob are connected by a channel $\mathcal{E}$ which Alice uses to communicate her state $\hat{\rho}$ representing her system a to Bob who receives $\mathcal{E}(\hat{\rho})$. This scenario can be simulated by considering a shared state $\hat{\sigma}$ between Alice and Bob. Bell detection is performed on Alice's system a and her part of the shared state, which we label A, with outcome k, which is communicated to Bob. Bob applies a corrective unitary V_k^{-1} to his system B with outcome b. This teleportation protocol is equivalent to the action of certain quantum channels from Alice to Bob, thus it may be considered a simulation of such channels.

Pirandola et al. showed that the teleportation LOCC in Fig. 2.1(a) can be replaced with an arbitrary LOCC $\mathcal{T}$ and resource state $\hat{\sigma}$ as shown in Fig. 2.1(b). A channel can be simulated in this way if it can be written as

$$\mathcal{E}(\hat{\rho}) = \mathcal{T}(\hat{\rho} \otimes \hat{\sigma}). \tag{2.6.98}$$

If so, we say that the channel is 'σ-stretchable'. In this case, the Bell detection LO is replaced by an arbitrary quantum operation $\mathbb{A}_k$ and Bob applies the corrective operation $\mathbb{B}_k$ after receiving classical information k. A case of particular interest, especially in our work, is that in which the channel can be simulated with a trace-preserving LOCC $\mathcal{T}$ applied to its Choi matrix $\hat{\rho}_{\mathcal{E}}$ defined in Eq. (2.6.96) with the shared resource being an EPR state $\hat{\Phi}$ as shown in Fig. 2.1(c). In this case, the channel is said to be 'Choi stretchable'.

Choi-stretchable channels can be identified by a property known as teleportation covariance. A d-dimensional quantum channel is teleportation covariant if, for any $U \in \mathbb{U}$, where the set $\mathbb{U}$ is that which contains the random unitaries generated by Bell detection,

$$\mathcal{E}\left(U\hat{\rho}U^{\dagger}\right) = V\mathcal{E}(\hat{\rho})V^{\dagger} \tag{2.6.99}$$

where V is another arbitrary unitary. Teleportation covariant channels are of particular importance as they can be teleportation-simulated with the associated corrective teleportation unitary taken outside of the channel and applied later as another corrective unitary. The starting point for understanding this property is the schematic for the simulation of a teleportation covariant channel outlined in Fig. 2.1(c). Replacing the LOCC $\mathcal{T}$ with a teleportation LOCC, Bell detection on Alice's systems a and A creates the state $\hat{\rho}_{A'} = U_k\hat{\rho}_a U_k^{\dagger}$ where U_k is a random teleportation unitary. The state of Bob's system B is given by $\mathcal{E}(\hat{\rho}_{A'}) = \mathcal{E}(U_k\hat{\rho}_a U_k^{\dagger}) =$

$V_k\mathcal{E}(\hat{\rho}_a)V_k^\dagger$ where the last equality is obtained by teleportation covariance. Upon receiving the outcome k of the Bell detection, Bob simply applies V_k^{-1} to obtain $\hat{\rho}_b = V_k^{-1}\hat{\rho}_B(V_k^{-1})^\dagger$. This process describes the simulation of $\mathcal{E}$ by a teleportation LOCC and Choi matrix resource state $\hat{\rho}_\mathcal{E}$ [20]. Some examples of teleportation covariant channels include the erasure, dephasing, and depolarizing channels. One example of a well-known channel that is not teleportation covariant is the amplitude damping channel.

2.6.3 Stretching of adaptive protocols and bounding capacities

We will now outline the key process which allows us to use channel simulation methods to simplify the general quantum communication protocol and easily find upper bounds for quantum channel capacities, following the process outlined in Ref. [20]. Consider the ith transmission through a channel $\mathcal{E}$, such that Alice and Bob share the state $\hat{\rho}_{\mathbf{ab}}^{i-1}$ prior to and $\hat{\rho}_{\mathbf{ab}}^{i}$ after communication. Consider a simulation with a LOCC Δ_i. We know that the output state can be written as

$$\hat{\rho}_{\mathbf{ab}}^{i} = \Delta_i(\hat{\rho}_{\mathbf{ab}}^{i-1} \otimes \hat{\sigma}). \tag{2.6.100}$$

Iterating the formula n times gives

$$\hat{\rho}_{\mathbf{ab}}^{n} = \Lambda\left(\hat{\rho}_{\mathbf{ab}}^{0} \otimes \hat{\sigma}^{\otimes n}\right) \tag{2.6.101}$$

for $\Lambda = \Delta_n \times \cdots \times \Delta_1$. We can include the process of preparing the initial state $\hat{\rho}_{ab}^0$ in the LOCC Λ and average over all local measurements in Λ so that it becomes the trace-preserving LOCC $\bar{\Lambda}$ (see Ref. [20] for a more in-depth discussion of this process). The state can then be written as

$$\hat{\rho}_{\mathbf{ab}}^{n} = \bar{\Lambda}(\hat{\sigma}^{\otimes n}). \tag{2.6.102}$$

If the channel is Choi-stretchable, the resource state is the Choi matrix such that $\hat{\rho}_{\mathbf{ab}}^{n} = \bar{\Lambda}(\hat{\rho}_{\mathcal{E}}^{\otimes n})$. An important property of the REE is that it is monotonic under trace-preserving LOCC. This fact allows us to write

$$E_R(\hat{\rho}_{\mathbf{ab}}^{n}) \leq E_R(\hat{\sigma}^{\otimes n}), \tag{2.6.103}$$

such that the LOCC $\bar{\Lambda}$ is removed. We can now insert the right-hand side of this inequality into the weak converse theorem in Eq. (2.6.97) which allows us to write $E_R^{\star} \leq E_R(\hat{\sigma})$ and, finally, we can write what is known as the one-shot REE bound [20]: *if we stretch an arbitrary quantum channel $\mathcal{E}$ into a resource state $\hat{\sigma}$, its quantum capacity can be bounded by the REE of the resource state,*

$$\mathcal{C}(\mathcal{E}) \leq E_R(\hat{\sigma}). \tag{2.6.104}$$

This equation represents a significantly reduced calculation of the upper bound on the capacity of a quantum channel. Moreover, if $\mathcal{E}$ is Choi-stretchable, the upper bound is obtained simply by the REE of the channel

$$\mathcal{C}(\mathcal{E}) \leq E_R(\hat{\rho}_{\mathcal{E}}) = E_R(\mathcal{E}). \tag{2.6.105}$$

This key result allows us to provide upper bounds on a variety of quantum channels simply through straightforward calculation of their REE.

2.6.4 Capacities and rates of quantum networks

In this section, we will extend the above formalism of the capacities of single quantum channels to the most general case of quantum networks. Our goal is to establish the quantum capacity of arbitrary network structures in which a set of senders (or Alices) $\{A_i\}$ communicate with a set of receivers (or Bobs) $\{B_j\}$ via a set of intermediate nodes that may transmit quantum information in a single direction. Ref. [20] was the first to begin this generalization by considering point-to-point protocols over a quantum channel, while Ref. [38] extended this study to protocols over repeater chains and, more generally, quantum networks. Finally, Ref. [39] further extended the study to quantum communication networks with multiple senders and receivers.

In order to describe arbitrary network configurations in a mathematically succinct way, we must introduce a framework based on graph theory. We will describe a quantum network $\mathcal{N}$ as an undirected graph with nodes (or points) P and edges E. Two points, x and y are connected by an edge $(x, y) \in E$ if and only if there is a corresponding quantum channel $\mathcal{E}_{xy}$ between the two. Each point p has a local register of quantum systems over which LOs are performed and optimized on the basis of two-way CCs with the other nodes. Given a set of senders $\{A_i\}$ and a set of receivers $\{B_j\}$, we define a cut C as a bipartition $(\mathbf{A}, \mathbf{B})$ of the points P such that $\{A_i\} \subset \mathbf{A}$ and $\{B_j\} \subset \mathbf{B}$ which is denoted as $C : \{A_i\}|\{B_j\}$. Then, a cut-set $\tilde{C}$ corresponds to the set of edges (x, y) which are disconnected by the cut C, i.e., such that $x \in \mathbf{A}$ and $y \in \mathbf{B}$.

The most straightforward quantum network communication configuration where we begin our analysis is one that consists of a single sender A and a single receiver B via a single route. For ease of understanding, we will restrict our analysis to networks constructed with teleportation-covariant channels. In this case we must define the *single-edge flow of REE* for a cut $C : A|B$ with cutset $\tilde{C}$ consisting of teleportation-covariant channels and Choi matrix resource state $\hat{\sigma}_{\mathcal{E}_{xy}}$ for edge $\mathcal{E}_{xy}$ as

$$E_R(C) := \max_{(x,y)\in\tilde{C}} E_R(\hat{\sigma}_{\mathcal{E}_{xy}}). \tag{2.6.106}$$

Again in analogy with the previous techniques applied to quantum channels, the two-way assisted quantum capacity of the network is bounded from above by

$$Q_2(\mathcal{N}) \leq \min_{C:A|B} E_R(C) \tag{2.6.107}$$

where the minimization is over all network cuts. We can extend these ideas to a slightly more complicated communication regime under which the parties may make use of all of the edges of the network exactly once by simultaneous routing from Alice to Bob. This type of strategy is known as a flooding protocol. In this case, the quantity of interest is the *multi-edge* flow of REE through cut $C : A|B$ defined by

$$E_R^m(C) = \sum_{(x,y)\in\tilde{C}} E_R(\hat{\sigma}_{\mathcal{E}_{xy}}) \tag{2.6.108}$$

which leads to the following upper bound on the multipath (two-way assisted) quantum capacity

$$Q_2(\mathcal{N}) \leq \min_{C:A|B} E_R^m(C). \tag{2.6.109}$$

A natural next step is to consider a network of an ensemble of Alices $\{A_i\}$ communicating with an ensemble of Bobs $\{B_i\}$. However, the mathematical complexity of this scenario can be alleviated by grouping the ensemble of Alices into a single 'super-Alice' and the ensemble of Bobs into a 'super-Bob'. While the physical structure of the network is the same, the communication problem with respect to these 'super-users' reduces to that examined above. Cuts $C : A|B$ must now be replaced by cuts splitting the super-users, i.e. the two ensembles, $C : \{A_i\}|\{B_j\}$. This treatment of the network leads to an upper bound because the super-users may, in principle, apply non-local quantum operations among their nodes and, therefore, better optimize the transmission rate with respect to the case of ensembles of separate users. As a result, the optimal rate at which qubits can be transmitted from the senders to the receivers is bounded by

$$\mathcal{B}(\mathcal{N}) := \min_{C:\{A_i\}|\{B_j\}} \sum_{(x,y)\in\tilde{C}} E_R(\hat{\sigma}_{\mathcal{E}_{xy}}). \tag{2.6.110}$$

It is also important to note that this is a general bound for multiple multicasts which applies to both the case of single- and multi-message multicasts from senders to receivers. In fact, since we bound the total number of physical qubits that super Alice transmits to super Bob, it does not matter if these qubits are independent (i.e., in a tensor product of different states) or dependent (e.g., in a global Greenberger-Horne-Zeilinger (GHZ) state [40]) when we unravel super Bob back into an ensemble of Bobs.

Chapter 3

Foundations of continuous-variable quantum key distribution

The core idea of quantum key distribution is elegant and comprehensible, however, its mathematical and experimental foundations are complex with many important subtleties. It is for this reason that we have chosen to dedicate a chapter to the introduction of the fundamental ideas of the theory particularly in regard to the continuous-variable regime. We will start with an introduction to the motivation for QKD and proceed to introduce the field of CV QKD. We will then introduce the notion of the secret key rate and different attack strategies an eavesdropper may employ, and subsequently, introduce a one-way CV-QKD protocol exploiting modulated coherent states. This introduction is followed by a brief overview of the classical strategies of privacy amplification and information reconciliation amongst others that play a vital role in guaranteeing the security of the regime.

3.1 The motivation for quantum key distribution

A somewhat startling fact about the most widely-used cryptographic protocols that almost all of us interact with daily is that they are far from provably secure. Worse still, the exponential growth in computational power adds a further layer of uncertainty since the security of these protocols is predicated on the computational difficulty associated with particular mathematical problems such as prime factoring in the case of the well-known RSA protocol. These protocols fall into the category of public-key cryptography. In brief, a public key protocol consists of a legitimate party, Alice, generating a secret key and a related public key that is broadcast. A second legitimate party, Bob, can obtain the public key and encrypts a message before sending the new key back to Alice who can decrypt the message with her secret key. The security of the protocol is entirely based on the algorithm used by Bob to perform the encryption that a malicious party may, in principle, successfully undo, obtaining Bob's message.

Private-key cryptography is a lesser-used alternative method of cryptography with some interesting properties. One of the assumptions of any private key protocol (and simultaneously one of its biggest problems) is that the legitimate communicating parties Alice and Bob must share a secret key. If this is the case, the parties can apply the *one-time pad* algorithm which simply requires Alice to add the secret key to her message and send the result to Bob who then subtracts the secret key to recover the original message. The best feature of private-key cryptography is that, if the main assumption is granted, the regime is provably secure against any possible attack an eavesdropper can employ. The difficulty then is in finding a provably secure key distribution system which, when combined with the one-time pad, will guarantee the security of the entire protocol.

Quantum cryptography aims to address the problem of securely distributing a key for private-key cryptography by providing a provably-secure key distribution protocol that is guaranteed by the laws of physics. The inherent uncertainty of quantum mechanics is the framework on which this possibility emerges. The fundamental difficulty that an eavesdropper faces when attempting to replicate a secret key encoded in quantum states is the no-cloning theorem, which states that it is impossible to duplicate an arbitrary quantum state. Moreover, an attempt to interfere with an incoming state, in an attempt to duplicate it or otherwise, can cause a disturbance in the signal that may be detectable by the legitimate parties. An eavesdropper must, therefore, only employ a relatively passive attack on the communication channel in order to ensure their presence is undetected.

The seminal QKD protocol was introduced by Bennett and Brassard in 1984 and coined the BB84 [17] protocol. In this protocol, the information was encoded in the polarisation of photons communicated between the parties in optical fiber. A series of subsequent protocols aimed to improve the performance of the BB84 protocol, featuring a variety of encoding strategies. However, the early QKD protocols all shared one feature: their encoding exploited physical systems with discrete degrees of freedom. Such schemes are now referred to as *discrete-variable* (DV) QKD. Several years after the inception of QKD, the first protocols exploiting continuous degrees of freedom of the quadrature amplitudes of the electromagnetic field were developed and the field of CV QKD was born.

3.2 A brief history of continuous-variable quantum key distribution

In 1999, T. Ralph published the first QKD protocol which exploited the non-classical behavior of continuous-variable squeezed states of light [41]. This protocol represented a stark deviation from the direction of the field of QKD at the time and it would later lead to the inception of the new field of CV QKD. Several subsequent protocols including those by Hillery [42] and Reid [43] helped secure the foundations of CV QKD by exploiting squeezed states of light in different ways to guarantee security. Two years after the seminal CV-QKD protocol was introduced, it was found that security could also be achieved with coherent states, bypassing the technical difficulty of generating squeezed states [44–48].

The field of CV QKD has drawn much attention mainly due to several appealing advantages it boasts over its DV counterpart: states can be generated and manipulated relatively easily with linear optics and feed-forward techniques, and measurements can be performed with readily-available, inexpensive, and highly efficient homodyne detectors as opposed to single-photon detectors. Furthermore, homodyne detectors offer particularly high bit rates, providing the regime a significant advantage for large-scale communication applications. The combination of these properties means that CV-QKD protocols can be implemented directly into existing network infrastructure where fiber optic cables and homodyne detectors are commonplace.

At this point, the reader should be armed with the knowledge of the key ideas of CV quantum mechanics introduced in the previous chapter. The remainder of this chapter will serve as an introduction to the ideas surrounding CV QKD, in order to ensure a solid understanding of the fundamentals before tackling more complex protocols in the following chapters. The discussion begins with the notion of the secret key rate which is followed by an overview of several ways in which an eavesdropper may attempt to interfere with a CV-QKD protocol. Next, an introduction is given to a fundamental CV-QKD protocol that exploits modulated coherent states, and, finally, the chapter concludes with a brief introduction to classical post-processing techniques.

3.3 Secret key rate

The performance of any QKD protocol is characterized by its secret key rate, R. The secret key rate is the number of secret bits that can be communicated per use of the protocol. In the asymptotic limit of the number of transmitted signals, the Devetak-Winter formula [49] provides an incredibly straightforward expression for the secret key rate,

$$R = I(A : B) - \chi \tag{3.3.1}$$

where $I(A : B)$ is the mutual information between the legitimate parties A and B, conventionally labeled Alice and Bob, respectively, and χ is the Holevo bound quantifying the maximum accessible information of an eavesdropper, whom we will name Eve. Eq. (3.3.1) is the most general form of the secret key rate and its form in a particular protocol is written in terms of Alice's encoding, Bob's best estimate of Alice's encoding and Eve's attack strategy, as we shall see later in the chapter. In a realistic setting, this rate cannot be achieved as the mutual information, $I(A : B)$ should be multiplied by the parameter $\beta \in [0, 1]$ which represents the reconciliation efficiency of the classical post-processing step that we will discuss later. Typical values of $\beta \approx 0.95$ are commonplace in modern CV QKD error-correcting codes [50].

Due to the Holevo bound χ being an upper bound on Eve's accessible information, the rate in Eq. (3.3.1) is a lower bound on that which may be achieved if a suboptimal attack strategy is employed. This property allows us to afford Eve the most generous quantum resources, enabling strong claims on the security of any particular protocol. Despite this, Eq. (3.3.1) only provides an asymptotic secret-key rate in the limit of many uses of a protocol, it alone does not guarantee the security in a realistic setting, but it does indicate the success of the protocol without the need for a detailed security analysis [51].

3.4 Eavesdropping

Clearly, no QKD protocol is complete without an eavesdropper. We will now introduce three possible attack strategies and the required quantum technologies for each. In light of this, we will introduce one particular Gaussian attack that is very frequently considered in CV-QKD protocols and how it can be easily described mathematically.

- *Individual attacks.* An individual attack is the weakest attack Eve may employ as part of her eavesdropping strategy, but it is also expected to be the most realistic at present based on state-of-the-art quantum technologies. For each use of the protocol, Eve prepares an independent ancillary mode that interacts unitarily with the target mode. This is known as an independent and identically distributed (IID) attack. The modified modes are independently measured before the communicating parties perform the post-processing step.

- *Collective attacks.* In this attack strategy, Eve interacts with each target mode with independent ancillary modes, but she can perform an optimal collective measurement on all of her modes after the post-processing is complete or, in general, at any time. This attack necessitates that Eve can store quantum states, potentially for a long time. This is a difficult task with current technologies but it provides a useful bound on Eve's information.

- *Coherent attacks.* This is the most general and, therefore, the most powerful attack available to an eavesdropper. They may prepare a general (entangled) state of an arbitrary number of modes that interact with the incoming target modes. This ancillary system can then be stored and measured collectively at a later time.

The entangling cloner attack

We will now introduce a particularly important type of collective attack which is frequently utilized in CV-QKD protocols due to it being the strongest attack that Eve can employ in the most commonly used CV-QKD protocols. It is known that the optimal attack strategy for protocols based on Gaussian operations, such as homodyne detection, encoding based on Gaussian modulation and channels that perform Gaussian operations, is a collective attack that is based on a Gaussian unitary operation. A classification of all collective Gaussian attacks is given in Ref. [52]. The most commonly employed attack of this form, and that which will be used frequently throughout the analysis in the forthcoming chapters, is known as the entangling cloner [53]. The attack consists of two modes E and e which are initially in a TMSV state of variance ω, the CM of which is given by

$$V_{Ee} = \begin{pmatrix} \omega\mathbf{I} & \sqrt{\omega^2-1}\mathbf{Z} \\ \sqrt{\omega^2-1}\mathbf{Z} & \omega\mathbf{I} \end{pmatrix}. \tag{3.4.2}$$

We assume that Eve is in full control of the quantum channel between Alice and Bob which, without her presence, is an ideal quantum channel, i.e. with unit transmissivity. Eve's strategy is to insert into this channel a beam splitter of transmissivity τ. In this situation, the legitimate parties will attribute the losses associated with the beam splitter to realistic channel loss. Eve uses her beam splitter to mix her mode E with the incoming mode sent by Alice. She then sends the output from one port of the beam splitter to Bob via a perfect quantum channel while she stores the remaining output E' in a quantum memory. Assuming that Eve's quantum memory is lossless and unlimited, she may store the output of every realization of the protocol and operate them collectively after quantum communication between the legitimate parties ceases. In the next section, the entangling cloner is applied to a CV-QKD protocol using coherent states as information carriers.

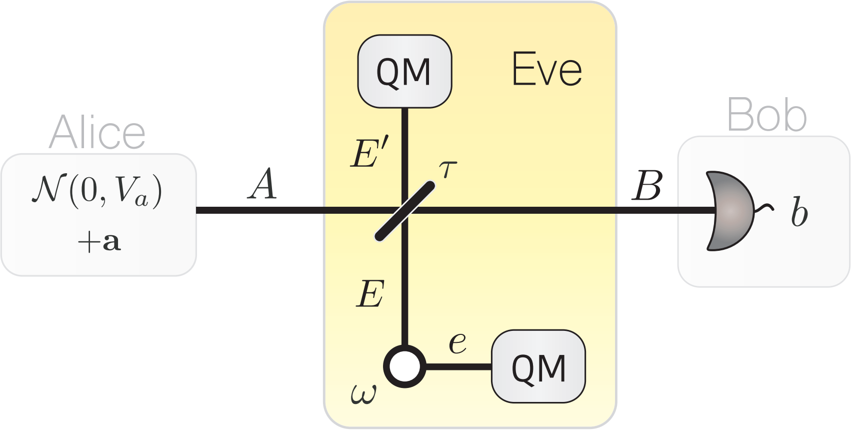

Figure 3.1: Schematic of a one-way CV-QKD protocol. Alice sends Gaussian-modulated coherent states to Bob through an insecure quantum channel of transmissivity τ after displacing the quadratures of her state according to a randomly drawn vector $\mathbf{a}$. Bob performs a homodyne measurement on one quadrature of his received mode. It is assumed that Eve performs a collective entangling cloner attack.

3.5 Continuous-variable quantum key distribution with coherent states

In order to illustrate the principles introduced thus far in a more quantitative manner, we now introduce a foundational CV-QKD protocol based on coherent states encoded with Gaussian modulation. This protocol serves as a useful introduction for readers unfamiliar with CV QKD as the procedure is straightforward to understand while the foundations are transferable to the more complex protocols that are introduced in the subsequent chapters.

As outlined in Fig. 3.1, each realization of this protocol consists of four main steps. Firstly, Alice chooses variables $q \in \mathcal{Q}$ and $p \in \mathcal{P}$ from IID random variables $\mathcal{Q}$ and $\mathcal{P}$ that each follow a zero-mean Gaussian distribution with variance V_a denoted as $\mathcal{N}(0, V_a)$. She uses these variables to modulate the quadratures of a coherent state so that she obtains $|\alpha\rangle = |q + ip\rangle$. For the protocol as a whole, the variance of Alice's signal is $V_A = V_a + 1$ where the additional unit accounts for the vacuum fluctuations. In each round of the protocol, Alice selects one of the quadratures at random to be used in the construction of the secret key. The relevant encoding variable after this choice (q or p) is denoted a. Alice sends her encoded coherent state to Bob via an untrusted quantum channel. The channel may be pure-loss (i.e. with zero thermal noise) but is more generally a thermal-loss channel characterized by a transmissivity τ and excess noise that will be discussed in detail later.

All of the losses and noise associated with the channel are attributed to an eavesdropper, Eve. The fact that all aspects of the protocol (channels, states, and measurements) are Gaussian allows us to make the assumption that Eve employs a collective entangling cloner attack as discussed in Sec. 3.4. We therefore assume she holds a TMSV state of variance ω and modes E and e. She inserts, into an otherwise lossless channel, a beamsplitter of transmissivity τ which mixes her mode E with Alice's mode. After the interaction, her modified mode E' is stored and the remaining output is sent to Bob without loss. When Bob receives the attenuated signal, he performs homodyne detection on either the q- or p-quadrature, selected randomly. His measurement outcome denoted b, is his estimate of Alice's encoding a.

In the final step, the parties perform post-processing. They must first determine in which instances of the protocol their choice of quadrature matched, in a process known as basis reconciliation, before estimating the channel parameters τ and ϵ. Finally, they perform error correction and privacy amplification in order to distill the final key. In the next section, we will introduce these concepts in more detail, but for the purpose of familiarizing the reader with the core ideas of CV QKD, we will assume an infinite number of channel uses so that an ideal secret key rate can be computed directly without concern for classical post-processing measures.

Prior to Alice sending a coherent state through the channel, the CM of the global system conditioned on Alice's encoding a is given by the direct sum of the CM of her coherent state and Eve's TMSV state describing her entangling cloner attack,

$$\mathbf{V}_{AEe|a} = V_0 \mathbf{I}_A \oplus \begin{pmatrix} \omega \mathbf{I} & \sqrt{\omega^2 - 1}\mathbf{Z} \\ \sqrt{\omega^2 - 1}\mathbf{Z} & \omega \mathbf{I} \end{pmatrix}. \tag{3.5.3}$$

where $V_0 = 1$ is the quantum variance of Alice's coherent state. The post-propagation

CM of the system is obtained by applying a beam splitter transformation of the form

$$\mathbf{T} = \begin{pmatrix} \sqrt{\tau}\mathbf{I} & \sqrt{1-\tau}\mathbf{I} \\ -\sqrt{1-\tau}\mathbf{I} & \sqrt{\tau}\mathbf{I} \end{pmatrix} \oplus \mathbf{I} \tag{3.5.4}$$

that mixes Alice's mode with Eve's mode E, resulting in the following CM of the total system

$$\mathbf{V}_{BE'e|a} = \begin{pmatrix} [\tau V_0 + (1-\tau)\omega]\,\mathbf{I} & \sqrt{1-\tau}\sqrt{\tau}(\omega - V_0)\mathbf{I} & \sqrt{1-\tau}\sqrt{\omega^2-1}\mathbf{Z} \\ \sqrt{1-\tau}\sqrt{\tau}(\omega - V_0)\mathbf{I} & [\tau\omega + (1-\tau)V_0]\,\mathbf{I} & \sqrt{\tau}\sqrt{\omega^2-1}\mathbf{Z} \\ \sqrt{1-\tau}\sqrt{\omega^2-1}\mathbf{Z} & \sqrt{\tau}\sqrt{\omega^2-1}\mathbf{Z} & \omega\mathbf{I} \end{pmatrix}. \tag{3.5.5}$$

Tracing out Eve's system from the total CM leaves us with Bob's CM conditioned on Alice's encoding, given by $V_{b|a}\mathbf{I}$ with $V_{b|a} = \tau V_0 + (1-\tau)\omega$. Bob's unconditional variance V_b is obtained by replacing the quantum variance V_0 with the total variance of Alice's input, V_A such that $V_b = \tau V_A + (1-\tau)\omega$. We assume for simplicity that Bob's quadrature variable can be obtained perfectly with ideal homodoyne detection. In this case, the mutual information between Alice and Bob, I_{AB}, can be obtained from these variances using the signal-to-noise ratio [51] as

$$I_{AB} = I(a:b) = \frac{1}{2}\log_2 \frac{V_b}{V_{b|a}}. \tag{3.5.6}$$

At this point, it is common to take Alice's variance V_a to be very large so that all terms in the expression for V_b, in which it doesn't appear, can be ignored. This allows us to obtain the following expression for the mutual information

$$I_{AB} = \frac{1}{2}\log_2 \frac{\tau V_a}{\tau V_0 + (1-\tau)\omega}. \tag{3.5.7}$$

We now turn our attention to Eve's accessible information. The process of obtaining Eve's conditional state requires two steps. First, we trace Bob's mode from the conditional post-propagation CM of the global system, then we replace the quantum variance V_0 in one of the quadratures of Eve's mode E' with Alice's total variance V_A to reflect the fact that Eve is only collecting outcomes for one quadrature due to the the fact that Alice and Bob select a random choice of quadrature in each round. After these steps, Eve's conditional CM is given by

$$\mathbf{V}_{E'e|a} = \begin{pmatrix} \mathbf{E}' & \sqrt{\tau}\sqrt{\omega^2-1}\mathbf{Z} \\ \sqrt{\tau}\sqrt{\omega^2-1}\mathbf{Z} & \omega\mathbf{I} \end{pmatrix}, \tag{3.5.8}$$

with

$$\mathbf{E}' = \begin{pmatrix} \tau\omega + (1-\tau)V_0 & 0 \\ 0 & \tau\omega + (1-\tau)V_A \end{pmatrix}. \tag{3.5.9}$$

The total CM is obtained by replacing the coherent state variance with Alice's total variance in both quadratures of Eve's mode E', which leads to the following expression

$$\mathbf{V}_{E'e} = \begin{pmatrix} [\tau\omega + (1-\tau)V_A]\,\mathbf{I} & \sqrt{\tau}\sqrt{\omega^2-1}\mathbf{Z} \\ \sqrt{\tau}\sqrt{\omega^2-1}\mathbf{Z} & \omega\mathbf{I} \end{pmatrix}. \tag{3.5.10}$$

Eve's total and conditional systems are described by Gaussian states, thus their entropies can be obtained straightforwardly from the corresponding CMs as we saw in the previous chapter. We can thus write the Holevo bound as

$$\chi(E'e : a) = S(\mathbf{V}_{E'e}) - S(\mathbf{V}_{E'e|a}). \tag{3.5.11}$$

The expressions we have now obtained for the mutual information and the Holevo bound allow us to compute the secret key rate of the protocol under what is known as direct reconciliation (DR). This means that Bob is attempting to reconcile his variable with Alice's encoding. Reverse reconciliation (RR) is an alternative strategy in which Alice adapts her key in response to corrective information received by Bob [45]. In this case, the mutual information between Alice and Bob is identical to that of the DR case, while the Holevo bound must be modified such that Eve's conditional entropy is obtained from her state conditioned on Bob's outcome b, which is now the secret variable that Eve is attempting to obtain. The Holevo bound in this setting is given by

$$\chi(E'e : b) = S(\mathbf{V}_{E'e}) - S(\mathbf{V}_{E'e|b}). \tag{3.5.12}$$

where the first term is identical under both DR and RR. In order to obtain the second term, we must first obtain an expression the relevant CM. Our starting point is the post-propagation CM of Bob and Eve conditioned on Alice's choice of encoding. The first step is to replace the variance V_0 with Alice's total variance V_A, which removes the conditioning and provides us with the total CM of Bob and Eve, labeled $\mathbf{V}_{BE'e}$. From here, we can obtain the the conditional CM by performing a homodyne measurement on Bob's mode using the mathematical formalism introduced in Sec. 2.4.5. Without loss of generality, we can assume Bob measures the q-quadrature with outcome b. With some manipulation, the conditional CM is given by

$$\mathbf{V}_{E'e|b} = \begin{pmatrix} \mathbf{E}_1 & \mathbf{C} \\ \mathbf{C}^{\mathsf{T}} & \mathbf{E}_2 \end{pmatrix}. \tag{3.5.13}$$

where we define

$$\mathbf{E}_1 = [\tau\omega + (1-\tau)V_A]\,\mathbf{I} - \frac{\alpha}{\beta}\mathbf{\Pi} \tag{3.5.14}$$

$$\mathbf{E}_2 = \omega\mathbf{I} - \frac{(1-\tau)(\omega^2-1)}{\beta}\mathbf{\Pi} \tag{3.5.15}$$

$$\mathbf{C} = \sqrt{\tau}\sqrt{\omega^2-1}\mathbf{Z} + \frac{\gamma}{\beta}\mathbf{\Pi} \tag{3.5.16}$$

where $\mathbf{\Pi} = \mathrm{diag}(1,0)$ and

$$\alpha := \tau(1-\tau)(V_A-\omega)^2 \tag{3.5.17}$$

$$\beta := V_A\tau + (1-\tau)\omega \tag{3.5.18}$$

$$\gamma := (1-\tau)(V_A-\omega)\sqrt{\tau}\sqrt{\omega^2-1}. \tag{3.5.19}$$

The Holevo bound under RR is obtained by computing the symplectic decomposition of this CM and, subsequently, the von Neumann entropy from the symplectic eigenvalues. As the mutual information is identical in both DR and RR, this calculation is the final element required in order to compute the secret key rate of the protocol under RR.

Having outlined the mathematical procedure that allows for the computation of the secret key rates of the coherent state protocol under both DR and RR, let us now explore these in more detail by plotting them as a function of the channel loss for a variety of values of excess thermal noise, ϵ, in the channel. The excess noise is not a quantity we have dealt with directly thus far, rather, it is a quantity that would be estimated in an experimental implementation of the protocol. Usually, the excess noise originates from imperfections in elements of the experimental setup, but to be as stringent as possible in the security analysis, all of the noise must be attributed to Eve. In the entangling cloner attack, the excess noise can be expressed

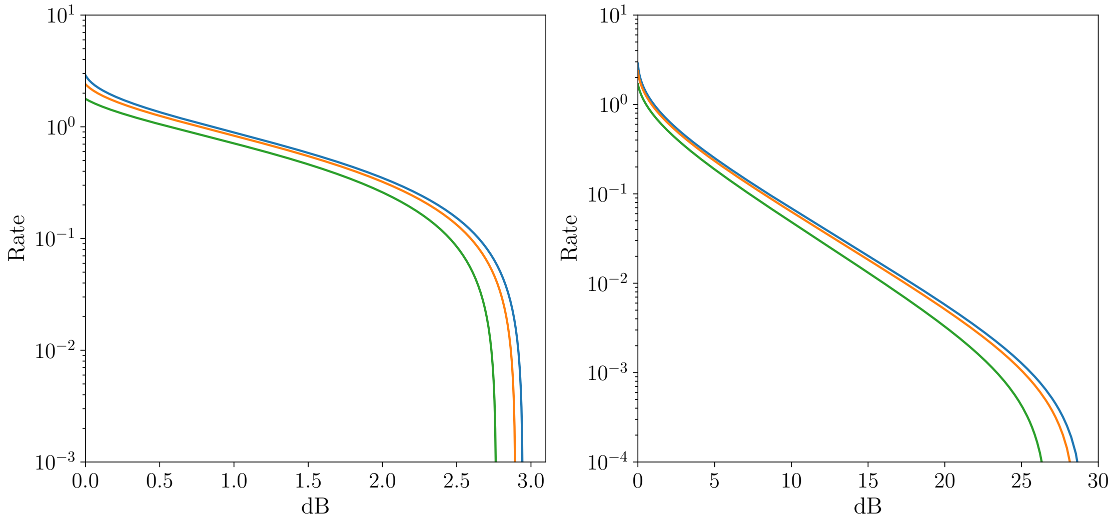

Figure 3.2: Rates of the CV-QKD protocol with coherent states under DR (left-hand side) and RR (right-hand side) as a function of the channel loss in dB with excess noise $\epsilon = 0.01$ (blue), $\epsilon = 0.02$ (orange) and $\epsilon = 0.05$ (green).

in terms of the variance of Eve's TMSV state as

$$\epsilon = \frac{(1-\tau)(\omega-1)}{\tau}. \tag{3.5.20}$$

Given an estimation of the channel noise, this equation can be used to estimate ω. We can thus express the secret key rates in terms of ϵ as opposed to ω. Fig. 3.2 shows the rates of the protocol under both DR and RR with excess noise values of $\epsilon = 0.01$ (blue line), $\epsilon = 0.02$ (orange line) and $\epsilon = 0.05$ (green line). The rates plotted as a function of the channel loss in decibels (dB) is related to the transmissivity as $\tau = 10^{-\mathrm{dB}/10}$. It is clear from the figure that the maximum tolerable loss under DR corresponds to ∼3 dB. In fact, in the ideal case ($\epsilon = 0$), the maximum loss corresponds to a transmissivity of $\tau = 0.5$. A channel loss exceeding this limit would lead to Eve gaining more information than Bob about Alice's signal, rendering it impossible to generate a secret key. Happily, RR provides an elegant solution to this problem, enabling a key rate to be generated at channel losses exceeding 25 dB even with a large amount of excess noise. In the next section, we will provide an overview of the classical post-processing techniques that are required to turn the ideal secret key rates shown here into realistic rates offering practical security for real-life implementations of the protocol.

3.6 Post-processing

The final step of any QKD protocol is classical post-processing and it is a vital component in ensuring security when constructing the final secret key between the trusted parties. Below, we briefly introduce the individual components of a typical post-processing protocol.

- *Basis reconciliation and sifting.* The first step in the post-processing of a CV-QKD protocol that involves a random choice of basis is known as basis reconciliation. It is most commonly used in the context of protocols such as that introduced in the previous section. Each party reveals which quadrature (q or p) they used to encode/measure. This process can be performed most easily if the parties select their quadrature using a random bit, the value of which they can later reveal thus conveying the required information. A process known as sifting is employed in order to remove any data which is obtained from realizations of the protocol in which the parties' choices of quadrature do not coincide. Note that certain CV-QKD protocols are designed to make use of both quadratures. In this case, the basis reconciliation and sifting processes are not required.

- *Parameter estimation.* After performing a sufficient number of realizations of the protocol, Alice and Bob each hold a set of data. In order to estimate the parameters associated with the protocol, for example, the transmissivity of quantum channels and any excess noise, they can broadcast a subset of this data. By constructing Gaussian estimators, the parties can obtain a worst-case bound on the parameters to a high degree of accuracy, usually corresponding to six, seven, or more standard deviations from the mean. With these worst-case estimates, they can compute their reconcilable mutual information βI_{AB} and the Holevo bound χ and thus determine if they can distill a secret key.

- *Information reconciliation.* Information reconciliation is the process by which Alice and Bob ensure both of their keys are identical. Essentially, this process is an error correction protocol and is an active area of research and many of the details involved are beyond the scope of this thesis. The state-of-the-art protocols used in CV QKD are slice reconciliation and multidimensional reconciliation.

- *Confirmation and privacy amplification.* After they perform information reconciliation, the parties each perform a hash function on their key and exchange the resulting hash values. In the worst-case scenario, in which the hash functions are different, they abort the protocol knowing that error correction has failed. Otherwise, they know that error correction has succeeded except with some small probability. If confirmation is successful, the final step in the classical post-processing procedure is privacy amplification, in which the goal is to minimize the probability that Eve can guess the key from any information she has attained throughout the use of the protocol. It is usually achieved by applying a compression algorithm to the secret key to obtain a shorter key of which Eve has negligible information. The compression algorithm usually involves a universal hash function. The difference between the lengths of the keys is determined by an estimate of the amount of information Eve may have obtained about the key.

Chapter 4

Continuous-variable quantum key distribution at terahertz frequencies

Up to this point in the discussion, we have considered only the most foundational CV-QKD protocols that paved the way for CV QKD to compete with its DV counterpart. While these protocols can be implemented relatively easily with inexpensive equipment, they are not without several significant limitations. Shortly after the publication of the seminal CV-QKD protocols, the most pressing of these limitations was the apparent maximum tolerable transmission loss of 3 dB, at which point an eavesdropper would gain more information than Bob about Alice's encoding.

Beating the 3 dB limit became a key target in CV-QKD research, and it was quickly met with the idea of RR in which Alice adapts her key in response to corrective information received by Bob [45] (cf. Chap. 3). More recently, combining RR with two-way communication has been found to achieve secret key rates close to the PLOB bound [54]. An alternative strategy that falls somewhat in between DR and RR was proposed by Silberhorn et al. [55]. The idea was termed post-selection, which refers to the ability of the parties to control which instances of the protocol are included in the final key. This ability can be derived from modifying the protocol so that the information carriers remain Gaussian-modulated states, while the secret encoding is a discrete binary variable that relates to two possible positions of the displaced state in phase space. If the absolute values of Alice's phase-space displacement and Bob's measurement outcome are known to both Alice and Bob in each instance, they can calculate their mutual information and that of an eavesdropper with respect to the discrete encoding. This knowledge allows them to establish which instances offer them an informational advantage. By including in the final key only these instances, the secret key rate is always positive and its magnitude is the only limiting factor when considering the range over which the parties may communicate securely. The post-selection technique was rapidly generalized to thermal loss channels [56, 57] and it has since been supported by proof-of-concept experiments [58, 59].

In modern CV-QKD theory, much interest has been directed at thermal states as information carriers. High-frequency thermal states with a small mean photon number display quantum mechanical properties similar to those of optical coherent states, hence they are appropriate candidates for CV-QKD protocols away from optical frequencies. As the required operating frequency of a protocol decreases, DV strategies become unfeasible as there is no direct way to detect individual photons [60], hence developing comprehensive CV-QKD protocols in this regime is of the utmost importance. The viability of such protocols has been demonstrated in several works under DR [61,62] and RR with two-way communication [63]. Furthermore, a finite-size analysis has demonstrated its viability in a realistic setting [64]. The reason for the more recent interest in this area is the feasibility of CV QKD as a means of secure communications at frequencies within the terahertz band. Edholm's law, which predicts a doubling in telecommunication bandwidth every 18 months [24], continues to hold true 50 years after its inception, accelerating the demand for high-rate communications towards the point at which operating frequencies in the terahertz band are required. CV QKD at terahertz frequencies has so far been proposed under atmospheric conditions [21] and as a means of inter-satellite communication [22]. In the atmosphere, high secret-key rates are achievable but security is only guaranteed at very short distances of the order of meters.

In this chapter, we will begin by briefly outlining the original CV-QKD protocol for communication within the terahertz band in the atmosphere. We will

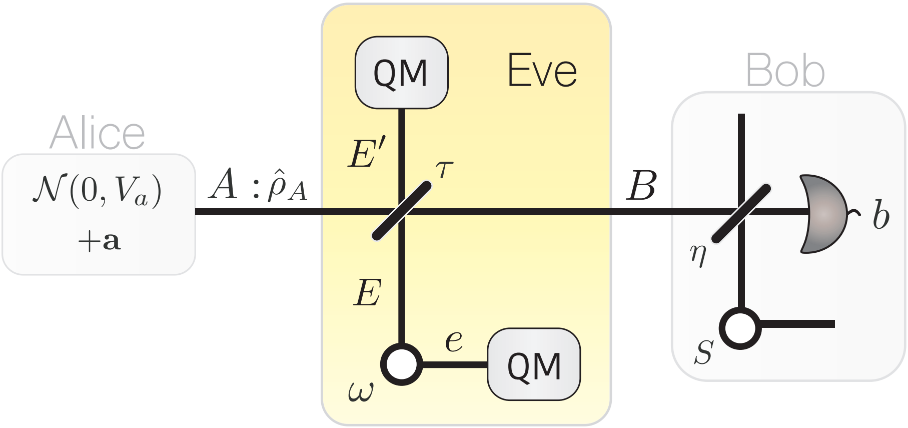

Figure 4.1: Schematic of the one-way CV-QKD protocol using Gaussian-modulated thermal states. Alice sends states to Bob via an untrusted quantum channel with transmissivity τ after displacing the quadratures by a random tuple $\mathbf{a}$. Bob performs a homodyne measurement on his received mode. Eve performs an entangling cloner attack. She is in possession of a TMSV state, one mode of which interacts with the channel via the beam splitter. Furthermore, she has access to a quantum memory which is optimally measured after quantum communication between the trusted parties ceases.

subsequently introduce an original post-selected CV-QKD protocol that allows for communication at frequencies within, or below, the terahertz band. We formulate the protocol by assuming Alice sends thermal states via an insecure quantum channel operated by an eavesdropper who may perform a collective entangling cloner attack. Comparing with the original protocol, we find that post-selection offers a significantly longer range and thus extends the viability of the regime to a variety of new applications.

4.1 Quantum key distribution at terahertz frequencies with Gaussian encoding

In this section, we will introduce the first CV-QKD protocol for communication at terahertz frequencies in the atmosphere, introduced by Ottaviani et al. [21] and outlined schematically in Fig. 4.1. In this protocol, the sender, Alice, transmits thermal states with thermal noise variance V_0 to Bob. She has access to IID random variables $\mathcal{Q}$ and $\mathcal{P}$ that each follow a zero-mean Gaussian distribution with variance V_a denoted as $\mathcal{N}(0, V_a)$. She encodes each state by applying a displacement $\mathbf{a} = (q_A, p_A)$ to its quadrature amplitudes with $q_A \in \mathcal{Q}$ and $p_A \in \mathcal{P}$. Finally, she randomly chooses either q_A or p_A as her variable a that will be used in the generation of the final key.

The process of preparing and sending the encoded thermal states can be viewed as the action of the quadrature operator $\hat{A} = \hat{0} + \hat{\mathbf{a}}$ on the vacuum where $\hat{0}$ is the 'THz quadrature operator' [21], which applies the background thermal noise, and $\hat{\mathbf{a}}$ is the displacement operator that displaces the state in phase space according to the vector $\mathbf{a}$. The variance of this operator (and, therefore, the variance of Alice's signal) is $V_A = V_0 + V_a$, where $V_0 := 2\bar{n} + 1$ is the total quantum noise variance with the vacuum contribution normalized to unity and the remaining thermal noise parameterized by the mean photon number $\bar{n}$, related to the frequency, ν of the radiation at temperature t by Planck's law,

$$\bar{n}^{\text{th}} = \left[\exp\left(\frac{h\nu}{k_B t}\right) - 1\right]^{-1}, \tag{4.1.1}$$

where k_B is the Boltzmann constant and h is the Planck constant. During transmission to Bob, Alice's mode A is subject to channel loss, all of which we attribute to an eavesdropper, Eve. Despite the terahertz protocol being somewhat more complex than the coherent state protocol introduced in Sec. 3.5, it is still comprised exclusively of Gaussian operations (channels, states, and measurements). We can therefore assume Eve performs the collective entangling cloner attack as introduced in Sec. 3.4. We label the modes of Eve's TMSV state E and e and the associated variance ω. Alice's mode A is mixed with Eve's mode E in a beam splitter of transmissivity τ. Eve's modified mode E' is stored in a quantum memory for later measurement (that may involve all rounds of the protocol) and the remaining output becomes Bob's mode B.

Upon receiving his mode, Bob converts the incoming terahertz signal to optical light and performs a homodyne detection on one randomly-chosen quadrature of the resulting mode, obtaining outcome b. The conversion process performed by Bob has a limited efficiency that requires consideration in the security analysis with typical values expected to be just 10% at the time of writing, based on recent developments in THz-optical conversion hardware [65]. This detection inefficiency can be modeled by placing a beam splitter of transmissivity η in front of a perfect detector, mixing the incoming mode with some noise of variance S that can be modeled by a TMSV state of equivalent variance. The noise S and the output of the beam splitter can be considered to be either trusted or untrusted, however, we will only consider the former in our analysis as this is a realistic assumption for wireless communications in the atmosphere.

In each round of the protocol after Alice selects her variable a prior to the onset of quantum communication, the CM of the entire system can be written as the direct sum of each of the subsystems

$$\mathbf{V}_{AES|a} = V_0\mathbf{I} \oplus \mathbf{V}_{\mathrm{TMSV}}(\omega) \oplus \mathbf{V}_{\mathrm{TMSV}}(S) \tag{4.1.2}$$

where the system S represents the detection noise and $\mathbf{V}_{\mathrm{TMSV}}(\mu)$ is the CM of a TMSV state with variance μ, given by

$$\mathbf{V}_{\mathrm{TMSV}}(\mu) = \begin{pmatrix} \mu\mathbf{I} & \sqrt{\mu^2-1}\mathbf{Z} \\ \sqrt{\mu^2-1}\mathbf{Z} & \mu\mathbf{I} \end{pmatrix}. \tag{4.1.3}$$

To obtain the post-propagation CM, we apply a global beam splitter operation, $\mathbf{T} = \mathbf{T}_\eta\mathbf{T}_\tau$ to the initial CM, that encapsulates the combined effect of the beam splitter controlled by Eve, given by

$$\mathbf{T}_\tau = \begin{pmatrix} \sqrt{\tau}\mathbf{I}_2 & \sqrt{1-\tau}\mathbf{I}_2 \\ -\sqrt{1-\tau}\mathbf{I}_2 & \sqrt{\tau}\mathbf{I}_2 \end{pmatrix} \oplus \mathbf{I}_6, \tag{4.1.4}$$

and the beam splitter modeling detector inefficiencies, given by

$$\mathbf{T}_\eta = \begin{pmatrix} \sqrt{\eta}\mathbf{I}_2 & \mathbf{0} & \sqrt{1-\eta}\mathbf{I}_2 \\ \mathbf{0} & \mathbf{I}_4 & \mathbf{0} \\ -\sqrt{1-\eta}\mathbf{I}_2 & \mathbf{0} & \sqrt{\eta}\mathbf{I}_2 \end{pmatrix} \oplus \mathbf{I}_2, \tag{4.1.5}$$

where $\mathbf{I}_n$ is the $n \times n$ identity matrix and $\mathbf{0}$ is the null matrix of implicit dimensions. After this interaction, the variance of Bob's mode conditioned on Alice's encoding can be extracted from the post-propagation CM as

$$V_{b|a} = \eta\tau V_0 + \eta(1-\tau)\omega + (1-\eta)S. \tag{4.1.6}$$

The mutual information between Alice and Bob is obtained from the signal-to-noise ratio, which in this case, is the ratio of Bob's total variance over all rounds, V_b, and the variance $V_{b|a}$ above. Bob's total variance is obtained by replacing the inherent thermal variance V_0 in Eq. (4.1.6) with Alice's total variance V_A. If the variance V_a of Alice's Gaussian distributions $\mathcal{Q}$ and $\mathcal{P}$ is large, Bob's total variance can be approximated as the dominant term of the resulting expression, $\eta\tau V_a$, allowing us to write the following formula for the mutual information

$$I_{AB} = \frac{1}{2}\log_2 \frac{V_b}{V_{b|a}} = \frac{\eta\tau V_a}{\eta\tau V_0 + \eta(1-\tau)\omega + (1-\eta)S}. \tag{4.1.7}$$

Turning our attention now to Eve, the computation of the Holevo bound is a little more complicated and depends on whether the parties employ DR or RR. For the purposes of comparison with our post-selection protocol, we will consider only DR and refer the reader to Ref. [21] for a complete discussion. Labeling Eve's total state $\hat{\rho}_{E'e}$ and conditional state $\hat{\rho}_{E'e|a}$, the Holevo bound can be written as

$$\begin{aligned}\chi(E'e:a) &= S(\hat{\rho}_{E'e}) - S(\hat{\rho}_{E'e|a}) &(4.1.8)\\ &= S(\mathbf{V}_{E'e}) - S(\mathbf{V}_{E'e|a}), &(4.1.9)\end{aligned}$$

where the second equality is due to the fact that Eve's total and conditional states are both Gaussian and their entropies can be computed directly from their CMs. The Holevo bound is, of course, different depending on whether the noise at the detector is trusted or untrusted, however, we will concentrate exclusively on the former scenario as already mentioned. In this case, the CM of Eve's conditional state is obtained by tracing out all but Eve's part of the global post-propagation CM. It can be written as

$$\mathbf{V}_{eE'} = \begin{pmatrix} W\mathbf{I} & \sqrt{\tau}\sqrt{\omega^2-1}\mathbf{Z} \\ \sqrt{\tau}\sqrt{\omega^2-1}\mathbf{Z} & [\tau\omega + (1-\tau)V_0]\,\mathbf{I} \end{pmatrix}. \tag{4.1.10}$$

The total CM is obtained by replacing the quantum variance V_0 in Eq. (4.1.10) with the total variance of Alice's signal, V_A in one of the quadratures of Eve's mode E' in order to model the fact that only one quadrature is used for key generation. Taking the limit of large Gaussian variance ($V_a \gg 1$), the symplectic spectrum of Eve's total CM becomes

$$\{\nu_1, \nu_2\} = \{\omega, (1-\tau)V_a\}, \tag{4.1.11}$$

while that of the conditional CM becomes

$$\{\tilde{\nu}_1, \tilde{\nu}_2\} = \left\{\sqrt{\frac{\omega[\tau + (1-\tau)\omega V_0]}{\tau\omega + (1-\tau)V_0}}, \quad \sqrt{(1-\tau)V_a[\tau\omega + (1-\tau)V_0]}\right\}. \tag{4.1.12}$$

Using the VNE of Gaussian states (cf. Sec. 2.5.3) and some algebraic manipulation, taking into account the limit of large variance, we can write the Holevo bound in the following form

$$\chi(E'e : a) = h(\omega) - h(\tilde{\nu}_1) + \frac{1}{2}\log_2 \frac{(1-\tau)V_a}{\tau\omega + (1-\tau)V_0}. \tag{4.1.13}$$

Finally, with the results obtained thus far, we are able to compute the secret key rate of the protocol. This quantity is given by the difference in the mutual information between the legitimate parties, given by the mutual information between Alice's encoding a and Bob's measurement outcome b, and the Holevo bound quantifying Eve's maximum accessible information on Alice's encoding,

$$R := I(a : b) - I(E'e : a). \tag{4.1.14}$$

Using equations (4.1.7) and (4.1.13) and some algebraic manipulation, we arrive at an expression for the rate as a function of all of the parameters associated with the protocol under the assumption of large variance

$$\begin{aligned} R(V_0, \tau, \omega, \eta, S) = \frac{1}{2}\log_2 &\frac{\tau\eta[\tau\omega + (1-\tau)V_0]}{(1-\tau)[\eta\tau V_0 + (1-\tau)\eta\omega + (1-\eta)S]} \\ &+ h\left[\sqrt{\frac{\omega[\tau + (1-\tau)\omega V_0]}{\tau\omega + (1-\tau)V_0}}\right] - h(\omega). \end{aligned} \tag{4.1.15}$$

In order to give Eve the strongest attack, we can assume that she exploits all of the thermal noise associated with the state. Symbolically, this means that we set $\omega = V_0$. Moreover, the rate turns out to be minimized by setting $S = 1$. Under these conditions, the rate reduces to the following straightforward formula of three variables

$$R(V_0, \tau, \eta) = h\left[\sqrt{\tau + (1-\tau)V_0^2}\right] - h(V_0) + \frac{1}{2}\log_2 \frac{\tau\eta V_0}{(1-\tau)(\eta V_0 + 1 - \eta)}. \tag{4.1.16}$$

This convenient analytic form of the secret key rate will serve as an important benchmark for our original post-selection protocol which we will introduce in the next section and we will explore its behavior as a function of its parameters therein.

4.2 Quantum key distribution at terahertz frequencies with post-selection

4.2.1 Protocol overview

In order to enable post-selection in a one-way CV-QKD protocol, we must make several modifications to the usual one-way scheme, including introducing a discrete encoding alphabet. Let us now introduce our protocol in the abstract as outlined schematically in Fig. 4.2. As with the protocol introduced above, Alice has access to IID random variables $\mathcal{Q}$ and $\mathcal{P}$, both of the form $\mathcal{N}(0, V_a)$. In each use of the protocol, she constructs the random tuple $\boldsymbol{\alpha} = (q_A, p_A)$ by choosing real elements $q_A \in \mathcal{Q}$ and $p_A \in \mathcal{P}$. She separates q_A into a sign κ and modulus $\mathbb{A}$ and p_A into a sign κ' and modulus $\mathbb{A}'$ and stores the tuples $\boldsymbol{\kappa} = (\kappa, \kappa')$ and $\mathbf{a} = (\mathbb{A}, \mathbb{A}')$. She uses these variables to encode the mean value $\bar{\mathbf{x}}_A$ of a thermal state $\hat{\rho}_A$ that she prepares in her mode A such that $\bar{\mathbf{x}}_{A|\boldsymbol{\kappa}\mathbf{a}} = (\kappa\mathbb{A}, \kappa'\mathbb{A}')$ and $\hat{\rho}_A \to \hat{\rho}_{A|\boldsymbol{\kappa}\mathbf{a}}$. She subsequently sends her mode to Bob via an untrusted quantum channel. The mean thermal photon number of Alice's signal, $\bar{n}^{\text{th}}$ is related to the frequency, ν of the radiation by Planck's law in Eq. (4.1.1) and the variance of the mode is $V_0 = 2\bar{n}^{\text{th}} + 1$. The total variance of Alice's signal is again $V_A = V_0 + V_a$.

We assume that Eve performs an entangling cloner attack and we label her modes E and e with variance ω and the channel transmissivity is τ. After the interaction, Alice's mode A becomes Bob's mode B, and Eve's mode E' is stored for later measurement. As with the protocol introduced in the previous section, the post-selection protocol consists of Gaussian measurements, channels, and states. However, it will become clear later that there is a non-Gaussian component that emerges in the calculation of Eve's information due to the binary encoding. We must therefore only conjecture that the optimal attack is based on a Gaussian unitary, leaving the proof as the focus of further investigation. This conjecture is reasonable as Eve's interaction with Alice's information may only occur in each channel use where all aspects are Gaussian.

Upon receiving his mode B, Bob performs a *heterodyne* measurement, with out-

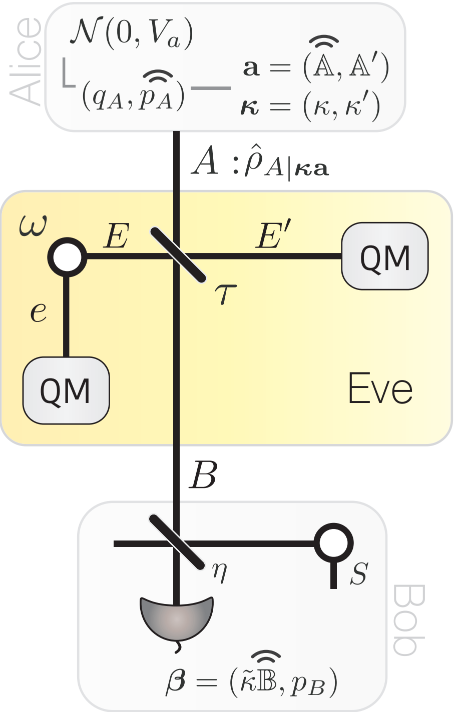
Alice
$\mathcal{N}(0, V_a)$
$(q_A, \widehat{p_A})$
$\mathbf{a} = (\widehat{\mathbb{A}}, \mathbb{A}')$
$\boldsymbol{\kappa} = (\kappa, \kappa')$
$A : \hat{\rho}_{A|\boldsymbol{\kappa}\mathbf{a}}$
ω
E
E'
QM
τ
e
QM
Eve
B
η
S
Bob
$\boldsymbol{\beta} = (\widehat{\tilde{\kappa}\mathbb{B}}, p_B)$

Figure 4.2: Schematic of the post-selected one-way protocol with thermal states assuming the q-quadrature is used for generation of the secret key. Alice sends thermal states of variance V_0 to Bob via a quantum channel with transmissivity τ who performs a heterodyne measurement on his received mode. Eve performs an entangling cloner attack. She is in possession of a TMSV state, one mode of which interacts with the channel via the beam splitter. Furthermore, she has access to a quantum memory which is optimally measured after quantum communication between the trusted parties ceases.

come $\boldsymbol{\beta} = (q_B, p_B)$. He separates q_B into a sign $\tilde{\kappa}$ and modulus $\mathbb{B}$ and p_B into a sign $\tilde{\kappa}'$ and modulus $\mathbb{B}'$. He stores the tuples $\tilde{\boldsymbol{\kappa}} = (\tilde{\kappa}, \tilde{\kappa}')$ and $\mathbf{b} = (\mathbb{B}, \mathbb{B}')$. We adopt the same model of detection efficiencies as outlined in the previous section. A beam splitter of transmissivity η is placed in front of an ideal detector and mixes the incoming mode with some *trusted* noise of variance S.

After quantum communication ceases, the parties perform the classical post-processing step of basis reconciliation. At the start of the protocol, both Alice and Bob select either the q- or p-quadrature at random. In this step, they each reveal their choice to the other. If the parties both selected the q-quadrature, the variables

κ' and $\tilde{\kappa}'$ are ignored. Alice publicly broadcasts $\mathbb{A}$ and p_A while Bob broadcasts $\mathbb{B}$ and p_B and attempts to reconcile his variable $\tilde{\kappa}$ with Alice's variable κ. Alternatively, if the p-quadrature is chosen, the relevant variables become κ' and $\tilde{\kappa}'$. Alice broadcasts $\mathbb{A}'$ and q_A while Bob broadcasts $\mathbb{B}'$ and q_B. In the computation of the secret key rate in the asymptotic number of channel uses, it is sufficient to assume that the parties always agree on a particular quadrature, leading to a simplification of the analysis. The reason why this strategy is possible will become clear as we compute the outputs of the protocol in the next section.

4.2.2 Propagation of the modes

Let us now follow the propagation of the modes of the total system assuming a particular choice of **a** and $\boldsymbol{\kappa}$. The CM of the total system in this case can be written as the direct sum of the individual systems of Alice, Eve and Bob (whose initial system, labeled S, consists of the detector with thermal noise),

$$\begin{aligned} \mathbf{V}_{ASEe|\boldsymbol{\kappa}\mathbf{a}} &= \mathbf{V}_{A|\boldsymbol{\kappa}\mathbf{a}} \oplus \mathbf{V}_S \oplus \mathbf{V}_{Ee} & (4.2.17) \\ &= V_0\mathbf{I} \oplus \mathbf{V}_{\mathrm{TMSV}}(S) \oplus \mathbf{V}_{\mathrm{TMSV}}(\omega). & (4.2.18) \end{aligned}$$

Alice's encoding imposes a generally non-zero mean value on Alice's mode of the form $\bar{\mathbf{x}}_{A|\boldsymbol{\kappa}\mathbf{a}} = (\kappa\mathbb{A}, \kappa'\mathbb{A}')^{\mathsf{T}}$ while that of the remaining system can be taken to be zero. The post-propagation CM and mean value are obtained by applying the global beam splitter $\mathbf{T}$ such that

$$\begin{aligned} \mathbf{V}_{BS'E'e|\boldsymbol{\kappa}\mathbf{a}} &= \mathbf{T}\mathbf{V}_{ASEe|\boldsymbol{\kappa}\mathbf{a}}\mathbf{T}^{\mathsf{T}} & (4.2.19) \\ \text{and} \quad \bar{\mathbf{x}}_{BS'E'e|\boldsymbol{\kappa}\mathbf{a}} &= \mathbf{T}\bar{\mathbf{x}}_{ASEe|\boldsymbol{\kappa}\mathbf{a}}. & (4.2.20) \end{aligned}$$

The system S' contains the modes of the TMSV state at the detector after interaction with the incoming mode from the channel. As we assume the detection noise is trusted, this system can be ignored in the remaining calculations by tracing it from the total system. The remaining system of Bob and Eve may be written in the following block form

$$\mathbf{V}_{\mathrm{B}E'e|\boldsymbol{\kappa}\mathbf{a}} = \begin{pmatrix} \mathbf{B} & \mathbf{C} \\ \mathbf{C}^{\mathsf{T}} & \mathbf{E} \end{pmatrix}, \qquad (4.2.21)$$

where $\mathbf{B}$ represents Bob's CM, given by

$$\mathbf{B} = V_{B|\boldsymbol{\kappa}\mathbf{a}}\mathbf{I} \quad \text{with} \quad V_{B|\boldsymbol{\kappa}\mathbf{a}} = \eta\tau V_0 + \eta(1-\tau)\omega + (1-\eta)S \tag{4.2.22}$$

and its corresponding mean value is

$$\bar{\mathbf{x}}_{B|\boldsymbol{\kappa}\mathbf{a}} = \left(\kappa\mathbb{A}\sqrt{\eta\tau}, \kappa'\mathbb{A}'\sqrt{\eta\tau}\right)^{\mathsf{T}}. \tag{4.2.23}$$

Block $\mathbf{E}$ represents Eve's CM,

$$\mathbf{E} = \begin{pmatrix} [(1-\tau)V_0 + \tau\omega]\mathbf{I} & \sqrt{\tau}\sqrt{\omega^2-1}\mathbf{Z} \\ \sqrt{\tau}\sqrt{\omega^2-1}\mathbf{Z} & \omega\mathbf{I} \end{pmatrix} \tag{4.2.24}$$

with corresponding mean value

$$\bar{\mathbf{x}}_{E|\boldsymbol{\kappa}\mathbf{a}} = \left(-\kappa\mathbb{A}\sqrt{1-\tau}, -\kappa'\mathbb{A}'\sqrt{1-\tau}, 0, 0\right)^{\mathsf{T}}. \tag{4.2.25}$$

Finally, the correlations between Bob and Eve are given by

$$\mathbf{C} = (\theta\mathbf{I}, \phi\mathbf{Z}), \tag{4.2.26}$$

where we define the quantities

$$\theta = \sqrt{\eta\tau(1-\tau)}(\omega - V_0) \tag{4.2.27}$$

$$\text{and} \quad \phi = \sqrt{\eta(1-\tau)}\sqrt{\omega^2-1}. \tag{4.2.28}$$

In the final step, Bob performs a heterodyne measurement on his mode B. He obtains the outcome $\boldsymbol{\beta} = (q_B, p_B)$ from which he records signs $\tilde{\boldsymbol{\kappa}} = (\tilde{\kappa}, \tilde{\kappa}')$ and absolute values $\mathbf{b} = (\mathbb{B}, \mathbb{B}')$. The probability of outcome $\boldsymbol{\beta}$ is derived from Eq. (2.4.78) as described in Sec. 2.4.5 using

$$p(\boldsymbol{\beta}|\boldsymbol{\kappa}\mathbf{a}) = p(\boldsymbol{\kappa}\mathbf{b}|\boldsymbol{\kappa}\mathbf{a}) = \frac{\exp\left[-\frac{1}{2}\mathbf{d}^{\mathsf{T}}\left(\mathbf{B}+\mathbf{I}\right)^{-1}\mathbf{d}\right]}{2\pi\sqrt{\det\left(\mathbf{B}+\mathbf{I}\right)}}, \tag{4.2.29}$$

where $\mathbf{d} = \bar{\mathbf{x}}_{B|\boldsymbol{\kappa}\mathbf{a}} - \boldsymbol{\beta}$. The probability can be separated into the product of the probabilities of the individual quadrature outcomes. We have

$$p(\tilde{\kappa}\mathbb{B}|\kappa\mathbb{A}) = \frac{1}{\sqrt{2\pi}\sqrt{V_{B|\boldsymbol{\kappa}\mathbf{a}}+1}}\exp\left[-\frac{1}{2}\frac{\left(\tilde{\kappa}\mathbb{B} - \kappa\mathbb{A}\sqrt{\eta\tau}\right)^2}{V_{B|\boldsymbol{\kappa}\mathbf{a}}+1}\right], \tag{4.2.30}$$

and

$$p(\tilde{\kappa}'\mathbb{B}'|\kappa'\mathbb{A}') = \frac{1}{\sqrt{2\pi}\sqrt{V_{B|\boldsymbol{\kappa}\mathbf{a}}+1}}\exp\left[-\frac{1}{2}\frac{\left(\tilde{\kappa}'\mathbb{B}' - \kappa'\mathbb{A}'\sqrt{\eta\tau}\right)^2}{V_{B|\boldsymbol{\kappa}\mathbf{a}}+1}\right]. \tag{4.2.31}$$

Note that the probability of each quadrature outcome is independent of Alice's encoding in the conjugate quadrature. It is this fact that allows us to simplify the computation of the secret key rate by assuming the parties always agree on one of the two quadratures. Moreover, the independence of the quadratures ensures that any variables relating to the quadrature conjugate to that which is assumed to be used for key generation do not affect the secret key rate and can thus be ignored in the calculations.

Eve's CM after Bob's measurement can be expressed in terms of the blocks in Eq. (4.2.21) as

$$\mathbf{V}_{E'e|\boldsymbol{\kappa}\mathbf{a}\tilde{\boldsymbol{\kappa}}\mathbf{b}} = \mathbf{E} - \mathbf{C}\left(\mathbf{B}+\mathbf{I}\right)^{-1}\mathbf{C}^{\mathsf{T}}, \tag{4.2.32}$$

which we can write in the following block form

$$V_{E'e|\boldsymbol{\kappa}\mathbf{a}\tilde{\boldsymbol{\kappa}}\mathbf{b}} = \begin{pmatrix} \mathcal{E}_1\mathbf{I} & \mathcal{C}\mathbf{Z} \\ \mathcal{C}\mathbf{Z} & \mathcal{E}_2\mathbf{I} \end{pmatrix}, \tag{4.2.33}$$

where we have defined

$$\mathcal{E}_1 = (1-\tau)V_0 + \tau\omega - \frac{\theta^2}{V_B+1} \tag{4.2.34}$$

$$\mathcal{E}_2 = \omega - \frac{\phi^2}{V_B+1} \tag{4.2.35}$$

$$\mathcal{C} = \sqrt{\tau}\sqrt{\omega^2-1} - \frac{\theta\phi}{V_B+1}. \tag{4.2.36}$$

Finally, the mean value of Eve's state after Bob's measurement is given by

$$\bar{\mathbf{x}}_{E'e|\boldsymbol{\kappa}\mathbf{a}\tilde{\boldsymbol{\kappa}}\mathbf{b}} = \bar{\mathbf{x}}_{E'e|\boldsymbol{\kappa}\mathbf{a}} - \mathbf{C}\left(\mathbf{B}+\mathbf{I}\right)^{-1}\mathbf{d} \tag{4.2.37}$$

from which we obtain

$$\mathbf{x}_{E'e|\boldsymbol{\kappa}\mathbf{a}\tilde{\boldsymbol{\kappa}}\mathbf{b}} = \begin{pmatrix} -\kappa\mathbb{A}\sqrt{1-\tau} + \left(\tilde{\kappa}\mathbb{B} - \kappa\mathbb{A}\sqrt{\eta\tau}\right)\frac{\theta}{V_B+1} \\ -\kappa'\mathbb{A}'\sqrt{1-\tau} + \left(\tilde{\kappa}'\mathbb{B}' - \kappa'\mathbb{A}'\sqrt{\eta\tau}\right)\frac{\theta}{V_B+1} \\ \left(\tilde{\kappa}\mathbb{B} - \kappa\mathbb{A}\sqrt{\eta\tau}\right)\frac{\phi}{V_B+1} \\ \left(\tilde{\kappa}'\mathbb{B}' - \kappa'\mathbb{A}'\sqrt{\eta\tau}\right)\frac{\phi}{V_B+1} \end{pmatrix}. \tag{4.2.38}$$

4.2.3 Mutual information

Let us begin our computation of the secret key rate by computing the mutual information between the legitimate parties. At this point, in the asymptotic limit of channel uses, the mutual information between the parties is equivalent to the mutual information between κ and $\tilde{\kappa}$ (or equivalently κ' and $\tilde{\kappa}'$) such that

$$I(\kappa : \tilde{\kappa}\,|\mathbb{A}\mathbb{B}) = 1 - H(\kappa|\,\tilde{\kappa}\,\mathbb{A}\mathbb{B}). \tag{4.2.39}$$

The second term on the right-hand side of the mutual information is a differential conditional entropy which may be written as

$$H(\kappa|\,\tilde{\kappa}\,\mathbb{A}\mathbb{B}) = \int p(\mathbb{A}\mathbb{B}) \sum_{\tilde{\kappa}} p(\tilde{\kappa}\,|\mathbb{A}\mathbb{B}) H_{\kappa|\,\tilde{\kappa}\,\mathbb{A}\mathbb{B}}\, \mathrm{d}\mathbb{A}\, \mathrm{d}\mathbb{B}\,, \tag{4.2.40}$$

where we note that $p(\tilde{\kappa}\,|\mathbb{A}\mathbb{B}) = 1/2$ since there is no correlation between the variables involved. The conditional entropy $H_{\kappa|\,\tilde{\kappa}\,\mathbb{A}\mathbb{B}}$ is given by

$$\begin{aligned} H_{\kappa|\,\tilde{\kappa}\,\mathbb{A}\mathbb{B}} &= \sum_{\kappa} p(\kappa|\,\tilde{\kappa}\,\mathbb{A}\mathbb{B}) \log_2 p(\kappa|\,\tilde{\kappa}\,\mathbb{A}\mathbb{B}) && (4.2.41) \\ &= H_2(p_{\mathrm{err}})\ \forall\, \tilde{\kappa} && (4.2.42) \end{aligned}$$

where $H_2(p_{\mathrm{err}}) = -p_{\mathrm{err}} \log_2 p_{\mathrm{err}} - (1 - p_{\mathrm{err}}) \log_2(1 - p_{\mathrm{err}})$ is the binary entropy of the error probability, p_{err}, i.e. the probability that Bob's sign $\tilde{\kappa}$ does not coincide with Alice's sign κ given the values $\mathbb{A}$ and $\mathbb{B}$, which can be obtained by first calculating

$$p(\tilde{\kappa}\,|\kappa\mathbb{A}\mathbb{B}) = \frac{p(\tilde{\kappa}\,\mathbb{B}|\kappa\mathbb{A})}{\sum_{\tilde{\kappa}} p(\tilde{\kappa}\,\mathbb{B}|\kappa\mathbb{A})} = \frac{1}{1 + \exp\left[-2\kappa\,\tilde{\kappa}\,\mathbb{A}\mathbb{B}\sqrt{\eta\tau}(V_{B|\boldsymbol{\kappa}\mathbf{a}} + 1)^{-1}\right]}, \tag{4.2.43}$$

then noting that $p(+|-\mathbb{A}\mathbb{B}) = p(-|+\mathbb{A}\mathbb{B}) = p_{\mathrm{err}}$ with

$$p_{\mathrm{err}} = \frac{1}{1 + \exp\left[2\mathbb{A}\mathbb{B}\sqrt{\eta\tau}(V_{B|\boldsymbol{\kappa}\mathbf{a}} + 1)^{-1}\right]}. \tag{4.2.44}$$

We may then write the mutual information in the following compact form

$$I(\kappa : \tilde{\kappa}\,|\mathbb{A}\mathbb{B}) = 1 - \int p(\mathbb{A}\mathbb{B}) H_2(p_e)\, \mathrm{d}\mathbb{A}\, \mathrm{d}\mathbb{B} \tag{4.2.45}$$

where the probability $p(\mathbb{A}\mathbb{B})$ is given by

$$p(\mathbb{A}\mathbb{B}) = \sum_{\kappa,\tilde{\kappa}} p(\tilde{\kappa}\,\mathbb{B}|\kappa\mathbb{A}) p(\kappa\mathbb{A}). \tag{4.2.46}$$

The variance of Alice's Gaussian distributions, V_a enters the calculation in the probability $p(\kappa\mathbb{A})$ above, however, it is not a directly relevant factor in the calculation of the secret key rate. As such, its value is largely flexible and can be selected in order to maximize the rate.

4.2.4 Eve's accessible information

Let us now turn our attention to Eve's accessible information about Alice's encoding which can be taken to be κ. In order to provide an upper bound on this quantity, we make use of the Holevo bound, which, in this case, is given by

$$\chi(E'e : \kappa|\mathbb{A}\mathbb{B}) = S(E'e|\mathbb{A}\mathbb{B}) - S(E'e|\kappa\mathbb{A}\mathbb{B}), \tag{4.2.47}$$

where the terms on the right-hand side are conditional von Neumann entropies (cf. Sec 2.5.3). The calculation of these terms requires the total and conditional states which may be obtained from the output state of a given instance of the protocol, $\hat{\rho}_{E'e|\kappa\mathbb{A}\,\tilde{\kappa}\,\mathbb{B}}$ as follows:

$$\begin{aligned}\hat{\rho}_{E'e|\mathbb{A}\mathbb{B}} &= \sum_{\kappa,\tilde{\kappa}} p(\kappa, \tilde{\kappa}\,|\mathbb{A}\mathbb{B})\hat{\rho}_{E'e|\kappa\mathbb{A}\,\tilde{\kappa}\,\mathbb{B}}. && (4.2.48)\\ &= \frac{1}{2}\sum_{\kappa}\hat{\rho}_{E'e|\kappa\mathbb{A}\mathbb{B}}, && (4.2.49)\end{aligned}$$

where the conditional state $\hat{\rho}_{E'e|\kappa\mathbb{A}\mathbb{B}}$ is given by

$$\hat{\rho}_{E'e|\kappa\mathbb{A}\mathbb{B}} = \sum_{\tilde{\kappa}} p(\tilde{\kappa}\,|\kappa\mathbb{A}\mathbb{B})\hat{\rho}_{E'e|\kappa\mathbb{A}\,\tilde{\kappa}\,\mathbb{B}}. \tag{4.2.50}$$

While Eve's output state from each use of the protocol is Gaussian, the same is not true of her total nor her conditional state and we cannot apply the simple rules for the entropy of Gaussian states. Instead, we must obtain the total and conditional states by expressing the protocol output state $\hat{\rho}_{E'e|\kappa\mathbb{A}\,\tilde{\kappa}\,\mathbb{B}}$ in the Fock basis before using the relationships outlined above. Fortunately, there exists an efficient way to obtain the density matrix of a Gaussian state, which is to relate its form to that of the generating function for the multivariate Hermite polynomials [66], given by

$$\exp\left(\mathbf{y}\mathbf{A}\boldsymbol{\beta}^{\mathsf{T}} - \frac{1}{2}\boldsymbol{\beta}\mathbf{A}\boldsymbol{\beta}^{\mathsf{T}}\right) = \sum_{\mathbf{m}\geq\mathbf{0}}\prod_{i=1}^{l}\frac{\beta_i^{m_i}}{m_i!}\mathbf{H}_{\mathbf{m}}^{(\mathbf{A})}(\mathbf{y}). \tag{4.2.51}$$

This connection was first drawn by Kok et al. in 2001 for single-photon states [67]. It was later used in the computation of pure Gaussian states [68, 69] and later generalized to mixed states by Dodonov et al. [70] (see Ref. [71] for an open source implementation of this method).

We will now follow the method introduced by Dodonov et al. in order to find the density matrix form of Eve's states. The first step in this process is to attain the CM $\boldsymbol{\sigma}$ and mean value $\boldsymbol{\beta}$ in terms of the quadrature amplitudes

$$\alpha_i = \frac{1}{2}(q_i + ip_i). \tag{4.2.52}$$

To do so, it is convenient to change the ordering of the vector of quadrature operators $\hat{\mathbf{x}}$ by applying the matrix $\mathbf{O}$ such that $\hat{\mathbf{x}} = (\hat{q}_1, \hat{p}_1, \hat{q}_2, \hat{p}_2) \to \mathbf{O}\hat{\mathbf{x}}\mathbf{O}^{\mathsf{T}} = (\hat{q}_1, \hat{q}_2, \hat{p}_1, \hat{p}_2)$ where $\mathbf{O}$ is defined as

$$\mathbf{O} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{4.2.53}$$

This causes the quadrature CM and mean value to transform according to $\mathbf{V} \to \mathbf{OVO}^{\mathsf{T}}$ and $\mathbf{x} \to \mathbf{Ox}$. We then define the following matrix

$$\mathbf{R} := \frac{1}{\sqrt{2}} \begin{pmatrix} \mathbf{I} & i\mathbf{I} \\ \mathbf{I} & -i\mathbf{I} \end{pmatrix}, \tag{4.2.54}$$

which, when applied to the quadrature CM and mean value yield the CM $\boldsymbol{\sigma}$ and mean value $\boldsymbol{\beta}$ as

$$\boldsymbol{\sigma} = \frac{1}{2}\mathbf{RVR}^{\dagger} \quad \text{and} \quad \boldsymbol{\beta} = \mathbf{R}\bar{\mathbf{x}}. \tag{4.2.55}$$

We can then introduce the Husumi-Q matrix, given by

$$\boldsymbol{\Sigma} = \boldsymbol{\sigma} + \frac{1}{2}\mathbf{I}, \tag{4.2.56}$$

which allows us to define the parameters $\mathbf{A}$ and $\mathbf{y}$ of the multivariate Hermite polynomials as

$$\mathbf{A} = \left(\mathbf{I} - \boldsymbol{\Sigma}^{-1}\right)^{*} \mathbf{X} \tag{4.2.57}$$

and

$$\mathbf{y} = \boldsymbol{\beta} - \mathbf{A}\boldsymbol{\beta}. \tag{4.2.58}$$

At this point, we must introduce the parameter N, which represents the truncation point of the infinite-dimensional Hilbert space of the state. With respect to the Hermite polynomials, the parameter l in Eq. (4.2.51) becomes the parameter N. The required value of N is determined by examining the convergence of the entropy of the total and conditional states, which is dependent on all of the protocol parameters. Once they are generated, the entropy of the $N^2 \times N^2$ approximate density matrices of the total and conditional states can be determined by the VNE, which, we recall, for a state $\hat{\rho}$ with eigenvalues $\{\lambda_i\}$ is given by

$$S(\hat{\rho}) = -\sum_i \lambda_i \log_2 \lambda_i. \tag{4.2.59}$$

4.2.5 Single-point rate and post-selection

Having derived the mutual information and Eve's accessible information, we are in a position to compute the secret key rate $R = \beta I - \chi$ where β is the reconciliation efficiency. However, to allow for post-selection, it is useful to re-write the rate as a single intergral over $\mathbb{A}$ and $\mathbb{B}$. To do this, we first express the mutual information in the following single-integral form

$$I(\kappa : \tilde{\kappa}\,|\mathbb{AB}) = \int p(\mathbb{AB})\tilde{I}(\mathbb{A},\mathbb{B})\,\mathrm{d}\mathbb{A}\,\mathrm{d}\mathbb{B}\,, \tag{4.2.60}$$

where we have defined the *single-point* reconcilable mutual information $\tilde{I}(\mathbb{A},\mathbb{B}) := \beta(1 - H_{\kappa|\,\tilde{\kappa}\,\mathbb{AB}})$. Similarly, we may re-write the Holevo bound as

$$\chi(E'e : \kappa|\mathbb{AB}) = \int p(\mathbb{AB})\tilde{\chi}(\mathbb{A},\mathbb{B})\,\mathrm{d}\mathbb{A}\,\mathrm{d}\mathbb{B} \tag{4.2.61}$$

with $\tilde{\chi} := S(\hat{\rho}_{E'e|\mathbb{AB}}) - \frac{1}{2}\sum_\kappa S(\hat{\rho}_{E'e|\kappa\mathbb{AB}})$. Then, the rate in full is expressed as

$$R = \int p(\mathbb{AB})\,\tilde{R}(\mathbb{A},\mathbb{B})\,\mathrm{d}\mathbb{A}\,\mathrm{d}\mathbb{B}\,, \tag{4.2.62}$$

where $\tilde{R} := \tilde{I} - \tilde{\chi}$ is the single-point rate. Post-selection is defined as the process of removing protocol instances in which the mutual information between Alice and Bob is less than that which is accessible by Eve. To model this process in our expression for the rate, we simply take the maximum of the single-point rate and zero in Eq. (4.2.62), such that the post-selected rate is given by

$$R_{\mathrm{PS}} = \int p(\mathbb{AB})\,\max\left\{\tilde{R}(\mathbb{A},\mathbb{B}), 0\right\}\mathrm{d}\mathbb{A}\,\mathrm{d}\mathbb{B}\,. \tag{4.2.63}$$

The post-selected rate may also be obtained by integrating the single-point rate with weighting $p(\mathbb{AB})$ over the *post-selection area* Γ, defined as the region in the

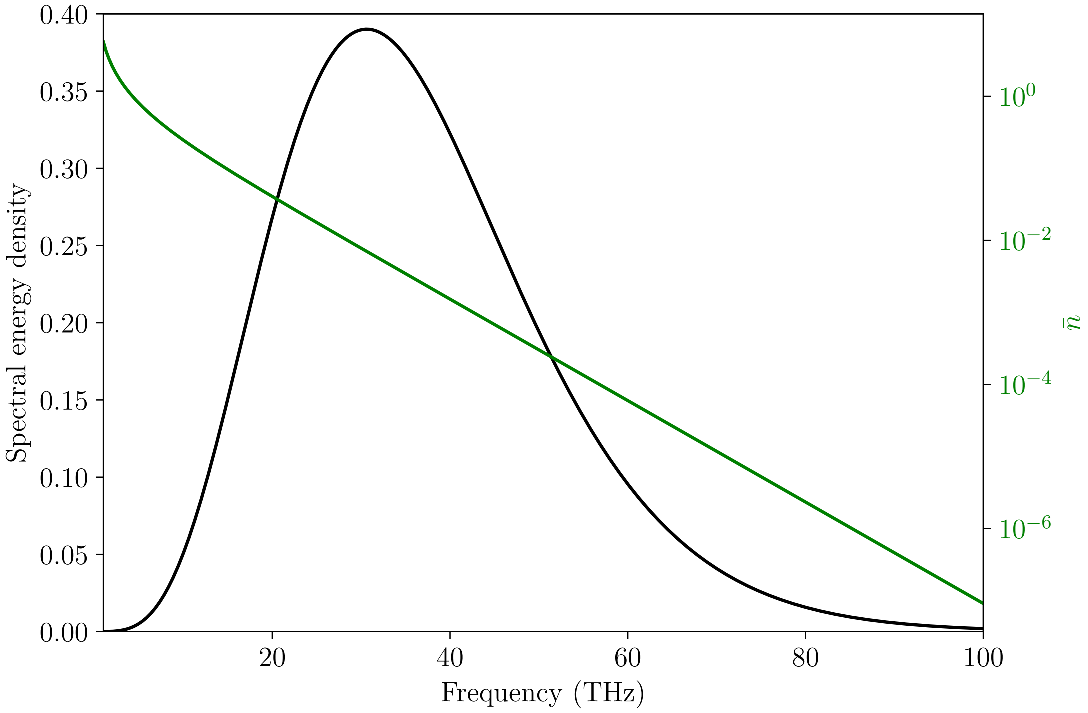

Figure 4.3: Plot of the spectral energy density as a function of frequency in the terahertz range at room temperature (296 K). Also plotted is the mean photon number of thermal states used in the protocol as a function of the operating frequency at the same temperature.

$\mathbb{A}$-$\mathbb{B}$ plane in which the single-point rate is positive,

$$R_{\mathrm{PS}} = \int_{\Gamma} p(\mathbb{A}\mathbb{B})\tilde{R}(\mathbb{A},\mathbb{B})\,\mathrm{d}\mathbb{A}\,\mathrm{d}\mathbb{B}\,. \tag{4.2.64}$$

4.2.6 Results

With the framework for our protocol in place, let us now present the results of numerical calculations of the secret key rate under a variety of parameters. For all of the forthcoming results, we have assumed $t = 296\,\mathrm{K}$ as we anticipate that most applications of the technology will occur around room temperature. Fig. 4.3 shows the spectral energy density of the background radiation at room temperature as a function of frequency, a distribution that peaks within the range of frequencies of interest. The same figure shows the mean photon number of the thermal states used in the protocol over the same frequency range. This curve demonstrates that thermal states with frequencies in the high terahertz range can closely resemble

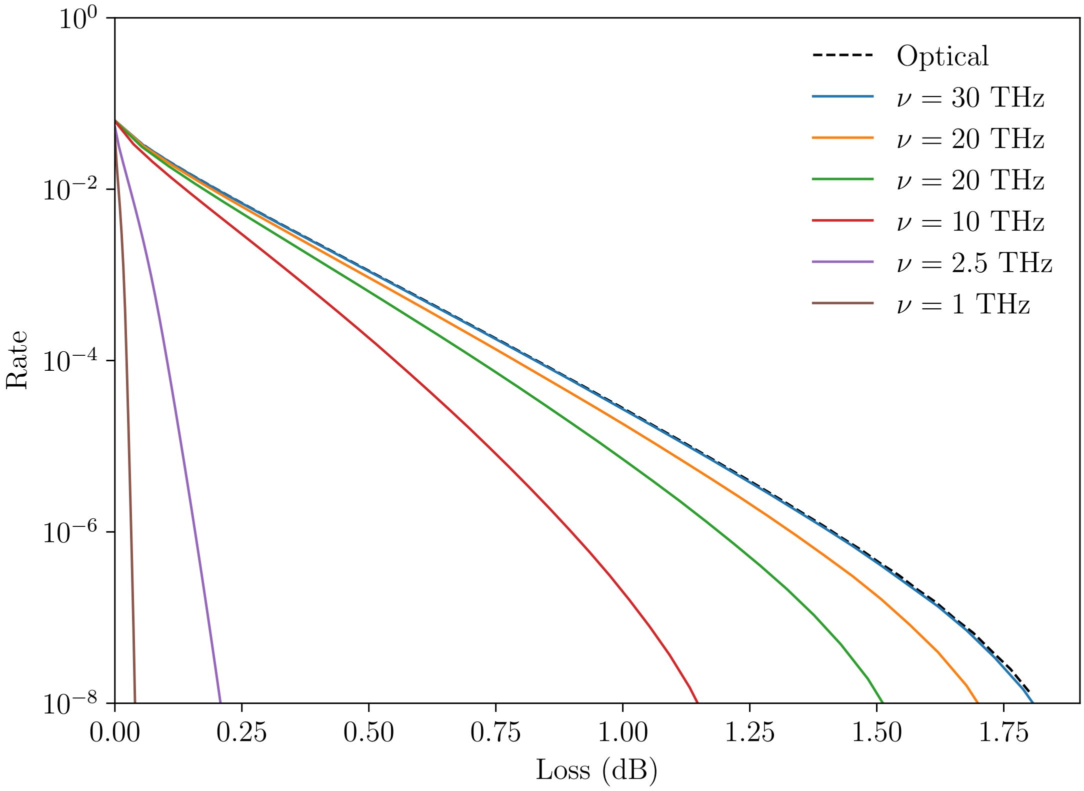

Figure 4.4: Rates of the post-selection protocol at a variety of terahertz frequencies as a function of the channel loss in dB. We set $\omega = V_0$ and assume a detection efficiency of 10%. For comparison, we include the rate of the protocol with coherent states and a pure-loss attack (dashed black line).

optical coherent states due to the mean photon number being orders of magnitude smaller than the variance of the vacuum fluctuations.

It is convenient to express the secret key rate as a function of the distance d, between Alice and Bob using the relation $\tau = 10^{-\delta d/10}$ where δ is the loss in dB per unit distance. The parameter δ is dependent on the medium through which the parties communicate. For example, if the quantum channel is a fiber optic cable, a typical value of δ is $0.2\,\mathrm{dB/km}$. For wireless communication in the atmosphere, the situation is far more complex and is the subject of active research. A comprehensive review of results and simulation packages may be found in Ref. [72].

We will begin by temporarily ignoring δ and plotting the rates of the protocol for a variety of frequencies as a function of the channel loss in dB. In order to afford Eve the best-case scenario and remain in line with the original Gaussian-

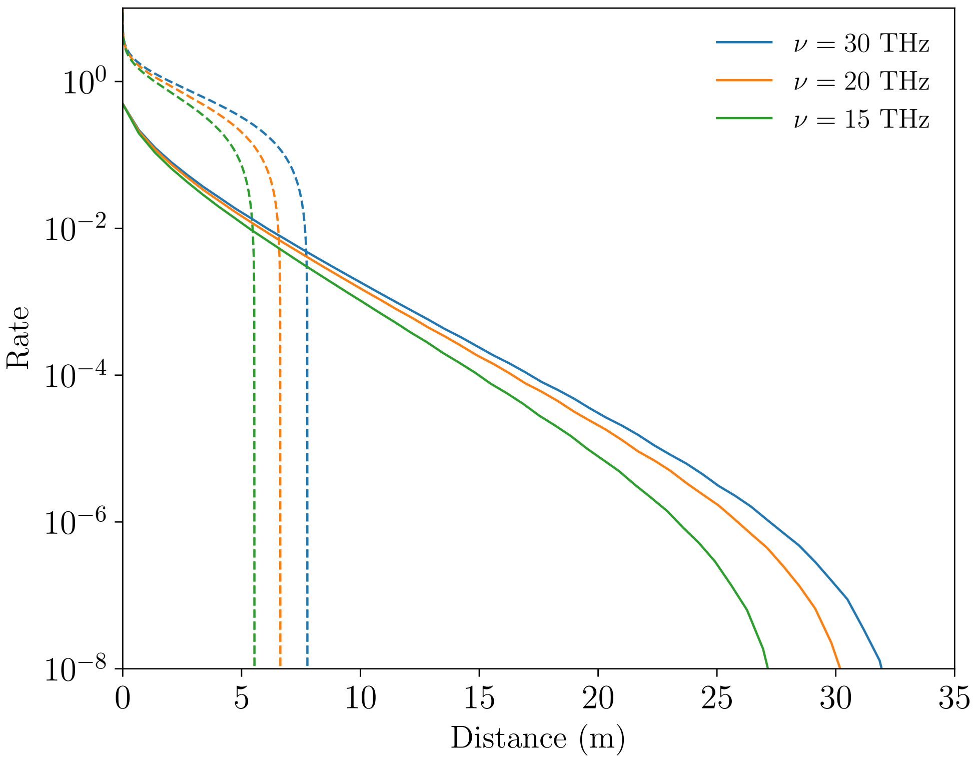

Figure 4.5: Rates of the Gaussian (dashed lines) and post-selection (solid lines) protocols as a function of the maximum transmission distance in meters for a range of frequencies within a window in which $\delta = 50\,\mathrm{dB/km}$. We assume $\omega = V_0$ and a detection efficiency of 10%.

modulated protocol, we set $\omega = V_0$ and we assume a realistic detection efficiency of 10%. For comparison, we include the case of coherent states ($V_0 = 1$) where Eve's action is reduced to a pure-loss attack [51]. The secret key rates for a variety of frequencies are shown in Fig. 4.4. The general trend is that an increase in thermal noise (corresponding to a lower frequency) leads to a rapid reduction in tolerable channel loss. This behavior can be attributed to the fact that the lower-frequency background radiation creates states that behave in a manner that becomes close to classical in nature, thus eliminating the uncertainty of quantum mechanics that enables security.

In Fig. 4.5, we consider the performance of our protocol at three frequencies which fall into an frequency window between 15 and 34 THz where the loss per unit distance, δ, is relatively low at 50 dB/km [72]. Again we assume $\omega = V_0$ and $\eta = 0.1$ and, for comparison, we include the corresponding rates of the protocol with Gaus-

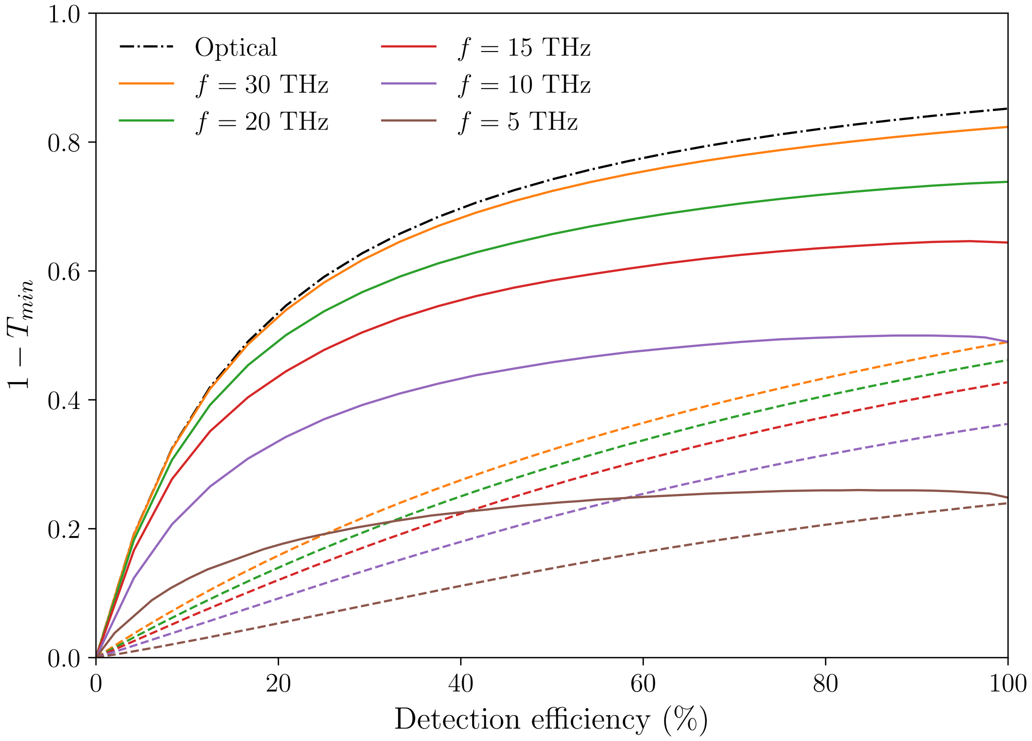

Figure 4.6: Rates of the protocol as a function of the distance between Alice and Bob under atmospheric parameters with 10% detection efficiency and with $V_a = 2$. We have assumed $\delta = 50$ for the transmission window encompassing the frequencies considered. For comparison, we include the equivalent rates of the protocol with Gaussian encoding under direct reconciliationq introduced previously (dashed lines).

sian encoding introduced previously. It is clear that our protocol offers a significant improvement to the maximum distance at which security can be guaranteed. We observe a roughly five-fold improvement in the maximum range for all of the frequencies considered. This improvement can be attributed entirely to the addition of post-selection. By only including a round of the protocol in which the parties have an informational advantage over the eavesdropper, the parties can communicate securely over a longer range, with the caveat that the rate in the short-distance regime is reduced. This process can be performed independently of the frequency of the thermal states used, hence the rate-distance behavior with respect to frequency is broadly equivalent across the post-selected and Gaussian-encoded protocols.

So far, we have only considered one typical detection efficiency value in our analysis. Let us first introduce the maximum tolerable loss, which is defined equal to $1-\tau_{\mathrm{min}}$ where τ_{min} is the value of the channel transmissivity at which $R_{\mathrm{PS}} = 10^{-10}$. In Fig. 4.6 we plot the maximum tolerable loss as a function of the detection efficiency for the full range of possible values with $\omega = V_0$. The dotted lines correspond to the original Gaussian-encoded protocol and the solid lines correspond to our post-selection protocol. We also include the rate with coherent states which is shown in black. For all of the frequencies considered, we observe a significant advantage when post-selection is applied. The advantage is most pronounced at lower detection efficiencies which makes the scheme particularly valuable with realistic hardware implementations available today.

4.3 Conclusions

The results we have presented in this chapter give credence to CV QKD as a method of high-rate secure communication at frequencies within the terahertz band. We have successfully introduced a protocol that can be implemented straightforwardly due to the continuous-variable framework on which it is constructed. Our protocol surpasses the range of the existing CV-QKD protocol designed to operate in the atmosphere. This significant advantage naturally extends the range of applicability of this regime, for example, applications such as short-range covert communications, that would otherwise require RR, can be implemented with our protocol. The next step towards an in-field implementation of our protocol is a finite-size analysis which will provide an important and necessary benchmark.

Chapter 5

Measurement-device-independent quantum key distribution

The one-way QKD protocols introduced in the previous chapter are incredibly powerful tools for private communication between two parties. However, one thing that we did not consider is that certain implementations may be susceptible to quantum hacking, in which an eavesdropper may exploit production flaws in the measurement apparatus to gain information. Such attacks are known as side-channel attacks and they are a difficult obstacle to overcome when attempting to prove the complete security of one-way QKD. One way to avoid the risk of side-channel attacks at the parties' stations is to transfer the liability of measurement to a third (generally untrusted) party. This strategy is known as measurement-device-independent (MDI) QKD.

In most MDI-QKD protocols, two parties, Alice and Bob, communicate through the means of a relay which may be entirely under the control of an eavesdropper, Eve. The role of the relay is to create the necessary correlations between the signals received from the communicating parties to enable a secret key to be constructed. The responsibility of the parties is therefore reduced simply to preparing and sending signals. Any potential eavesdropper at the relay must remain clandestine by ensuring that the relay output is predictable by the parties, who would otherwise cease communication. However, their attack may take into account any information attainable at the relay as well as from any form of attack on the Alice-relay and

Bob-relay links.

MDI QKD was initially proposed independently by S. L. Braunstein et al. [25] and H. K. Lo et al. [26] in 2012. Since then, a plethora of studies have aimed to improve the rate and range of both DV and CV protocols. Several DV-MDI protocols have recently been devised that can enable secure communication over a very long distance, exceeding the PLOB bound. The first protocols to achieve this feat all belong to the so-called twin-field (TF) regime in which Alice and Bob send phase-randomized optical fields to the relay [73–75]. TF-inspired protocols offering improvements on the original scheme include the phase-matching protocol [76] and the sending-or-not-sending protocol [77, 78].

The first CV-MDI protocol was introduced in 2013 by Pirandola et al. and was demonstrated in a proof-of-concept experiment to achieve very high secret key rates [79]. Furthermore, finite-size analyses exist which demonstrate the practicality of the protocol in a realistic setting [80, 81]. Unfortunately, the range of the protocol is limited, particularly in the 'symmetric' configuration in which the relay is positioned equidistant between Alice and Bob where the maximum tolerable loss on each link is a mere 0.75 dB. In an asymmetric configuration, particularly if the relay is positioned very close to one of the parties, the range is increased to metropolitan distances, but still falls well short of that offered by the TF protocols. As a result, developing a protocol that allows exploitation of the practicality of the CV-MDI regime at long distance is an active area of research in modern QKD theory. Several noteworthy efforts include protocols based on virtual photon subtraction [82,83], unidimensional modulation [84], and discrete modulation [85]. While these protocols offer an improvement in the range of the asymmetric configuration, their applicability in the symmetric configuration is very limited. Only Refs. [82, 83] offered any improvement over the original CV-MDI protocol in the symmetric configuration.

In this chapter, we will first introduce the seminal CV-MDI-QKD protocol before introducing an original alternative protocol in which we employ post-selection. Our goal is to improve the range of the CV-MDI regime, particularly in the symmetric configuration in which the rate-distance performance discrepancy between the DV and CV-MDI regimes is most pronounced. We find that with post-selection, we are able to achieve a significant improvement over the original protocol which is largest in more symmetric configurations. We also consider a restricted eavesdropping scenario, which allows for secure communication exceeding 50 km. As a result, we can begin to bridge the gap between DV and CV-MDI protocols while maintaining the advantages of the CV scheme.

5.1 Measurement-device-independent quantum key distribution with Gaussian encoding

Let us now introduce the seminal CV-MDI-QKD protocol by Pirandola et al. [79], which will provide an important benchmark for our post-selection protocol that we will introduce subsequently. The schematic for this protocol is shown in Fig. 5.1. Alice and Bob both prepare Gaussian-modulated coherent states in modes A and B, respectively, that are sent to the relay. At the relay, a Bell detection is performed in which the incoming modes A' and B' are mixed in a balanced beam splitter with outputs A'' and B'' that are subsequently measured with homodyne detection in the p- and q-quadratures, respectively. The corresponding outcomes γ_p and γ_q are publicly broadcast as $\boldsymbol{\gamma} = (\gamma_q, \gamma_p)$.

As all elements of the protocol are based on Gaussian operations, the optimal eavesdropping strategy is known to be based on a Gaussian unitary operation [86]. We can consider a general strategy that involves two modes E_1 and E_2 that interact directly with the quantum channels connecting the trusted parties to the relay, as well as a reservoir of additional modes which we label $\mathbf{e}$. We assume that Eve inserts beam splitters of transmissivity τ_A and τ_B into the otherwise lossless Alice-relay and Bob-relay channels, respectively, which mix Alice's mode A with her mode E_1 and Bob's mode B with her mode E_2. After the interaction, the modified modes E_1' and E_2' may interact with the ancillary modes $\mathbf{e}$ before being stored in a quantum memory. The conjugate outputs A' and B' are sent to the relay without loss. Any attack involving unitary operations applied to all of Eve's modes over many rounds of the protocol and higher-rank measurements of Eve's quadratures can be reduced to this attack with suitable reasoning [79], thus this model of the attack is the strongest we may consider. In general, the modes E_1 and E_2 are correlated while the attack reduces to dual one-mode entangling cloners if the correlations are zero. It was shown in the studies of the CV-MDI-QKD protocol that the optimal attack is the so-called 'negative EPR attack' [79,87].

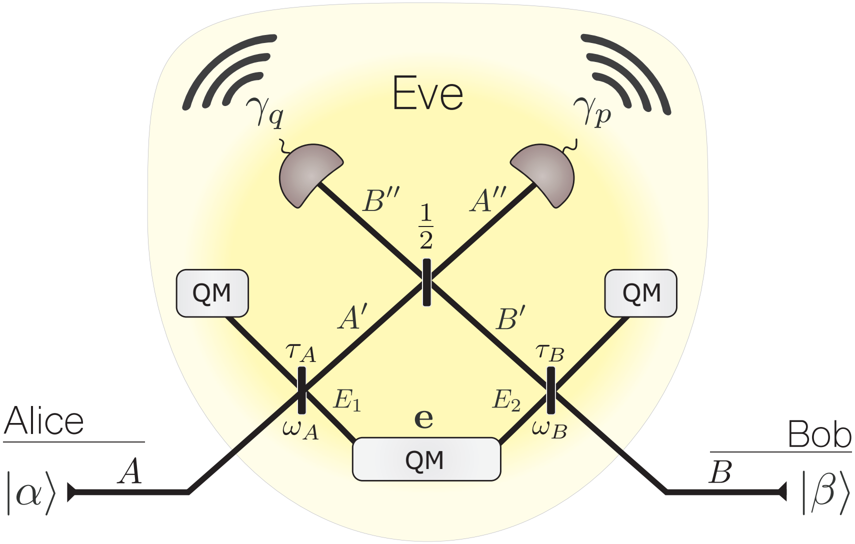

Figure 5.1: Schematic of the Gaussian CV-MDI-QKD protocol. Alice and Bob send coherent states in modes labeled A and B which interact with Eve's modes E_1 and E_2 via beam splitter interactions of transmissivities τ_A and τ_B, respectively. Eve stores her outputs in a reservoir of quantum states $(E_1, E_2, \mathbf{e})$ and may perform an optimal quantum measurement after communication ceases. The remaining outputs are sent to the relay where they are measured with Bell detection.

The protocol is most mathematically soluble by considering an *entanglement-based representation* in which we assume each of the legitimate parties holds a TMSV state of the form

$$\mathbf{V}_{Aa} = \mathbf{V}_{Bb} = \begin{pmatrix} \mu\mathbf{I} & \sqrt{\mu^2-1}\mathbf{Z} \\ \sqrt{\mu^2-1}\mathbf{Z} & \mu\mathbf{I} \end{pmatrix} \tag{5.1.1}$$

while Eve holds the general two-mode state

$$\mathbf{V}_E = \begin{pmatrix} \omega_A\mathbf{I} & \mathbf{G} \\ \mathbf{G} & \omega_B\mathbf{I} \end{pmatrix}, \quad \mathbf{G} = \begin{pmatrix} g & 0 \\ 0 & g' \end{pmatrix}. \tag{5.1.2}$$

By measuring one mode of their TMSV states with heterodyne detection, Alice and Bob prepare coherent states $|\alpha\rangle$ and $|\beta\rangle$. In the limit of large modulation, this process is identical to the direct preparation of coherent states in that the mean value of the resulting coherent states are identical. For smaller modulation, the mean values associated with the regimes differ, however this can be rectified by rescaling the modulation of one regime in accordance with the set value of that of its conjugate.

After Alice and Bob's modes interact with Eve's beam splitters and the Bell detection is performed at the relay, the global system of Alice, Bob and Eve is $\hat{\rho}_{abE_1'E_2'\mathbf{e}|\gamma}$. This state is pure, and as a result, all of the calculations regarding the secret key rate of the protocol can be performed using only the part of the state belonging to Alice and Bob while Eve holds the purifying system. As this state is Gaussian, since all of the protocol is performed with Gaussian states and operations, all of the relevant information is contained within its CM, which is given by

$$\mathbf{V}_{ab|\gamma} = \begin{pmatrix} \mu\mathbf{I} & 0 \\ 0 & \mu\mathbf{I} \end{pmatrix} - \left(\mu^2 - 1\right) \begin{pmatrix} \frac{\tau_A}{\theta} & 0 & -\frac{\sqrt{\tau_A\tau_B}}{\theta} & 0 \\ 0 & \frac{\tau_A}{\theta'} & 0 & \frac{\sqrt{\tau_A\tau_B}}{\theta'} \\ -\frac{\sqrt{\tau_A\tau_B}}{\theta} & 0 & \frac{\tau_B}{\theta} & 0 \\ 0 & \frac{\sqrt{\tau_A\tau_B}}{\theta'} & 0 & \frac{\tau_B}{\theta} \end{pmatrix}, \quad (5.1.3)$$

where we define

$$\theta = (\tau_A + \tau_B)\mu + \lambda, \quad \theta' = (\tau_A + \tau_B)\mu + \lambda' \quad (5.1.4)$$

with

$$\lambda = (1 - \tau_A)\omega_A + (1 - \tau_B)\omega_B - 2g\sqrt{(1 - \tau_A)(1 - \tau_B)} \quad (5.1.5)$$

$$\text{and} \quad \lambda' = (1 - \tau_A)\omega_A + (1 - \tau_B)\omega_B + 2g'\sqrt{(1 - \tau_A)(1 - \tau_B)} \quad (5.1.6)$$

In the following sections we will compute the mutual information between Alice and Bob, I_{AB} and the Holevo bound χ which allow us to compute the secret key rate, $R = \beta I_{AB} - \chi$, where β is the reconciliation efficiency.

Mutual information

The mutual information between Alice and Bob can be computed relatively straightforwardly using the following formula

$$I_{AB} = \frac{1}{2}\log_2 \Sigma, \quad (5.1.7)$$

where we define

$$\Sigma := \frac{1 + \det \mathbf{V}_{b|\gamma} + \operatorname{tr} \mathbf{V}_{b|\gamma}}{1 + \det \mathbf{V}_{b|\gamma\boldsymbol{\alpha}} + \operatorname{tr} \mathbf{V}_{b|\gamma\boldsymbol{\alpha}}}. \tag{5.1.8}$$

$\mathbf{V}_{b|\gamma}$ and $\mathbf{V}_{b|\gamma\boldsymbol{\alpha}}$, respectively are Bob's total and conditional CMs with respect to Alice's encoding $\boldsymbol{\alpha}$ or the measured value of the quadratures of Alice's coherent state in the entanglement-based representation. The total CM can be derived from Eq. (5.1.3) simply by tracing out Alice's mode such that

$$\mathbf{V}_{b|\gamma} = \begin{pmatrix} \mu - \frac{(\mu^2-1)\tau_B}{\theta} & 0 \\ 0 & \mu - \frac{(\mu^2-1)\tau_B}{\theta'} \end{pmatrix} \tag{5.1.9}$$

while the second is obtained from the same equation by applying heterodyning detection to Alice's mode a

$$\mathbf{V}_{b|\gamma\boldsymbol{\alpha}} = \begin{pmatrix} \mu - \frac{(\mu^2-1)\tau_B}{\tau_A+\tau_B\mu+\lambda} & 0 \\ 0 & \mu - \frac{(\mu^2-1)\tau_B}{\tau_A+\tau_B\mu+\lambda'} \end{pmatrix}. \tag{5.1.10}$$

Alternatively, the mutual information can be expressed in terms of the signal-to-noise ratio such that $I_{AB} = \log_2 \mu/\chi$ where $\chi = \mu\Sigma^{-1/2}$ is called the *equivalent noise*. An important parameter we will require in our subsequent analysis is the excess noise ϵ which is given by the difference in the equivalent noise and the noise attributed to channel loss

$$\epsilon := \chi - \chi_{\text{loss}}, \tag{5.1.11}$$

where χ_{loss} is computed from the mutual information in the case of a pure-loss attack ($\omega_A = \omega_B = 1$ and $g = g' = 0$).

Eve's accessible information

Due to the purity of the global state, the Holevo bound can be computed from the CM of the combined system of Alice and Bob's in Eq (5.1.3) and Bob's conditional CM in Eq. (5.1.10). It can be written in terms of the density matrices as

$$\chi = S(\hat{\rho}_{ab|\gamma}) - S(\hat{\rho}_{b|\gamma\boldsymbol{\alpha}}). \tag{5.1.12}$$

The first term can be calculated first by obtaining the symplectic spectrum $\{\nu_1, \nu_2\}$ of Bob's conditional CM $\mathbf{V}_{b|\gamma\boldsymbol{\alpha}}$ such that $S(\hat{\rho}_{b|\gamma\boldsymbol{\alpha}}) = S(\mathbf{V}_{b|\gamma\boldsymbol{\alpha}}) = h(\nu_1) + h(\nu_2)$ where $h(\cdot)$ is defined in Sec. 2.5.3. The entropy of the second term is simply given by $S(\hat{\rho}_{b|\gamma\boldsymbol{\alpha}}) = h(\nu)$ where ν is the single symplectic eigenvalue of Bob's CM $\mathbf{V}_{b|\gamma}$, which can be easily calculated as

$$\nu = \sqrt{\det \mathbf{V}_{b|\gamma\boldsymbol{\alpha}}}. \tag{5.1.13}$$

Secret key rate

Combining the results from the previous two sections, we may write the secret key rate in full as

$$R = \beta I_{AB} - \chi = \frac{\xi}{2}\log_2 \Sigma + h(\nu) - h(\nu_1) - h(\nu_2). \tag{5.1.14}$$

This formula is the most general form of the rate that depends on all of the parameters of the protocol, $R = R(\mu, \tau_A, \tau_B, \omega_A, \omega_B, g, g')$. Under ideal reconciliation efficiency ($\beta = 1$), the optimal modulation variance μ tends to infinity. Taking this into account and assuming the optimal negative EPR attack in which $g' = -g$, the rate can be reduced to a simple analytic expression in terms of fixed equivalent noise $\chi = \chi_{\text{loss}}(\tau_A, \tau_B) + \epsilon$. We have

$$R(\tau_A, \tau_B\ , \chi) = \log_2\left[\frac{2(\tau_A + \tau_B)}{e|\tau_A - \tau_B\chi}\right] + h\left[\frac{\tau_A\chi}{\tau_A + \tau_B} - 1\right] - h\left[\frac{\tau_A\tau_B\chi - (\tau_A + \tau_B)^2}{|\tau_A - \tau_B|(\tau_A + \tau_B)}\right], \tag{5.1.15}$$

while in the symmetric case we obtain

$$R(\chi) = h\left(\frac{\chi}{2} - 1\right) + \log_2\left[\frac{16}{e^2\chi(\chi - 4)}\right]. \tag{5.1.16}$$

Unfortunately, in the upcoming sections when using the Gaussian CV-MDI-QKD protocol as a benchmark for our post-selection protocol, we are not often able to exploit these expressions as we will consider a variety of parameters where optimization is necessary. However, it is appropriate to outline the remarkably simple mathematical description of the protocol under ideal conditions made possible by its Gaussian nature.

5.2 Measurement-device-independent quantum key distribution with post-selection

We will now introduce our original CV-MDI protocol which allows the communicating parties to perform post-selection. We first outline the actions of the parties and the eavesdropper before following the evolution of the modes in a single use of the protocol. From the protocol outputs, we derive the mutual information, the Holevo bound, and thus the asymptotic secret key rate. We then describe how post-selection can be applied in order to improve the range of the protocol. Finally, we compare our results with the original CV-MDI protocol under a variety of parameters.

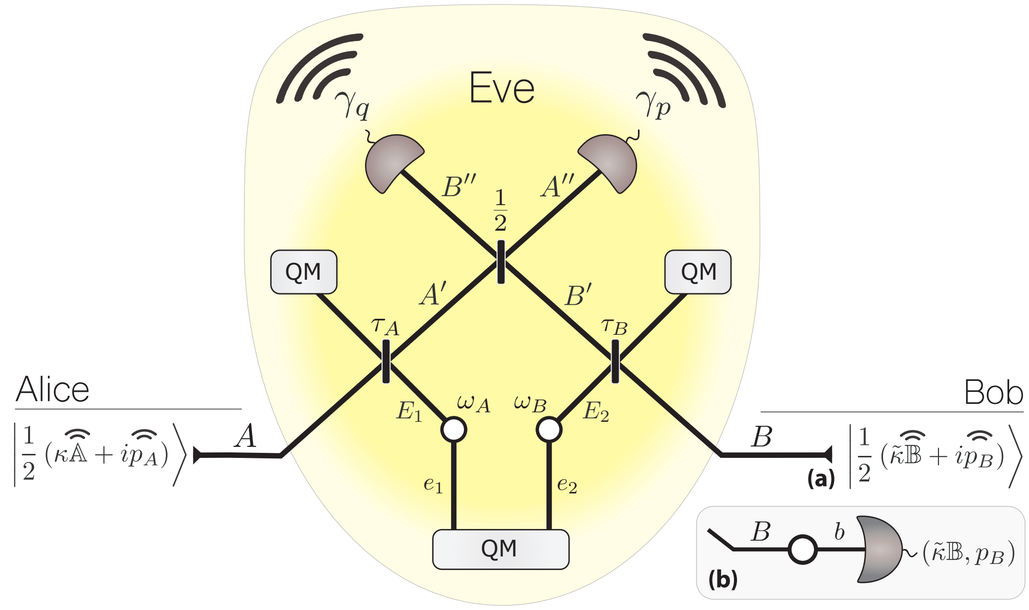
Eve
γ_q
γ_p
B''
A''
$\frac{1}{2}$
QM
QM
A'
B'
τ_A
τ_B
Alice
Bob
$\left|\frac{1}{2}(\kappa\widehat{\mathbb{A}}+i\widehat{p_A})\right\rangle$
A
E_1
ω_A
ω_B
E_2
B
(a)
$\left|\frac{1}{2}(\tilde{\kappa}\widehat{\mathbb{B}}+i\widehat{p_B})\right\rangle$
e_1
e_2
QM
B
b
$(\tilde{\kappa}\mathbb{B}, p_B)$
(b)

Figure 5.2: Schematic of a single use of the protocol assuming the q-quadrature is chosen by the parties for reconciliation. (a): Alice and Bob send coherent states to the relay which interact with Eve's modes. At the relay, a Bell detection is performed and the outputs γ_q and γ_p are publicly announced. After quantum communication ceases, Alice broadcasts $\mathbb{A}$ and p_A while Bob broadcasts $\mathbb{B}$ and p_B. (b): In the restricted eavesdropping scenario Bob's action is modeled in the entanglement-based representation. He measures, with heterodyne detection, one mode b of a TMSV state of variance μ obtaining the outcome $(\tilde{\kappa}\,\mathbb{B}, p_B)$. This action prepares coherent states in the conjugate mode B that is subsequently sent to the relay.

5.2.1 Protocol overview

Trusted parties

Application of post-selection of the case of CV-MDI QKD draws many similarities with the process outlined in Chap. 4 for the one-way protocol with the main difference being that both parties now prepare and send signals to the relay. We will limit our analysis to the case in which Alice and Bob send coherent states as this process ensures Eve's state is pure and the Holevo bound can be computed without considering the photon statistics of multimode states. This being the case, extending the analysis to thermal states is an interesting albeit difficult avenue for future work.

The preparation step requires the assumption that both parties have access to IID random variables $\mathcal{Q}$ and $\mathcal{P}$ that each follow a zero-mean Gaussian distribution of the form $\mathcal{N}(0, \sigma)$ where the variance σ can be adjusted freely. In each use of the protocol, Alice draws the random numbers $q_A \in \mathcal{Q}$ and $p_A \in \mathcal{P}$ with variance σ_A. From these two numbers, she extracts absolute values $|q_A| = \mathbb{A}$ and $|p_A| = \mathbb{A}'$ and signs κ and κ', respectively. The values of the signs κ and κ' define the binary encoding alphabet i.e. Alice records bit value 0(1) if the sign is positive(negative). She stores tuples $\mathbf{a} = (\mathbb{A}, \mathbb{A}')$ and $\boldsymbol{\kappa} = (\kappa, \kappa')$ and proceeds to prepare a coherent state of the form $\left|\frac{1}{2}(\kappa\mathbb{A} + i\kappa'\mathbb{A}')\right\rangle$ which she sends to the relay via a quantum channel. Bob follows a similar procedure, generating two random numbers q_B and p_B from his Gaussian distributions with a generally different variance σ_B. He generates a state of the form $\left|\frac{1}{2}(\tilde{\kappa}\mathbb{B} + i\tilde{\kappa}'\mathbb{B}')\right\rangle$ and sends it to the relay while storing tuples $\mathbf{b} = (\mathbb{B}, \mathbb{B}')$ and $\tilde{\boldsymbol{\kappa}} = (\tilde{\kappa}, \tilde{\kappa}')$.

After quantum communication ceases, the parties perform basis reconciliation. If the q-quadrature is chosen, the variables κ' and $\tilde{\kappa}'$ are discarded. Alice broadcasts $\mathbb{A}$ and p_A while Bob broadcasts $\mathbb{B}$ and p_B. Bob attempts to reconcile his variable $\tilde{\kappa}$ with Alice's variable κ. Alternatively, if the p-quadrature is chosen, the relevant variables become κ' and $\tilde{\kappa}'$. Alice broadcasts $\mathbb{A}'$ and q_A while Bob broadcasts $\mathbb{B}'$ and q_B.

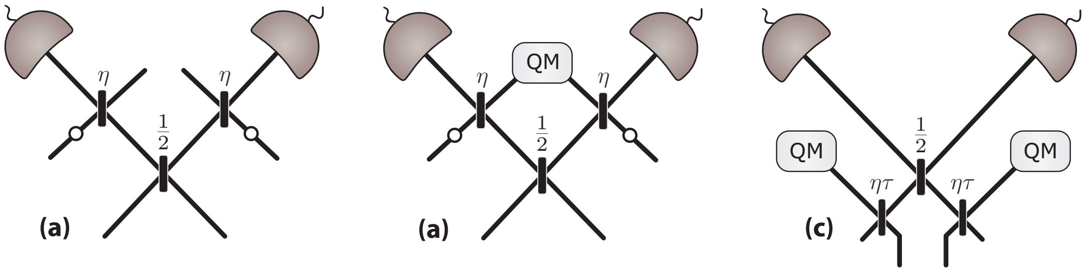

Figure 5.3: Models of inefficiency in homodyne detection at the relay using beam splitters. (a) depicts a trusted noise scenario in which it is assumed that Eve does not have access to the output of the beam splitters. (b) assumes that the outputs of the beam splitters are added to Eve's quantum memory for later measurement. (c) depicts a simplification in the symmetric case ($\tau_A = \tau_B = \tau$) and with $S = 1$

Complete and restricted eavesdropping

We will see later that our post-selection scheme does not allow the secret key of our protocol to be computed simply from the state of Alice and Bob. As a result, we cannot consider an unknown reservoir of states as in the case of the original protocol with Gaussian encoding as we must be able to fully and independently describe Eve's state. We, therefore, assume that Eve employs dual collective entangling cloner attacks as introduced in Section 3.4 in which she inserts beam splitters of transmissivity τ_A and τ_B into lossless Alice-relay and Bob-relay channels, respectively. She uses the beam splitters to mix Alice's mode A with her mode E_1 and Bob's mode B with her mode E_2. The modes E_1 and E_2 each form one half of independent TMSV states with conjugate modes e_1 and e_2, and variances ω_A and ω_B, respectively. She stores the outputs from one port of each beam splitter in a quantum memory and sends the remaining outputs A' and B' to the relay where the usual Bell detection is performed and outcomes $\boldsymbol{\gamma} = (\gamma_q, \gamma_p)$ are broadcast.

As the channels, measurements, and states sent by the parties are all Gaussian, we conjecture that this attack, based on a Gaussian unitary, is optimal and accounts for any general attack that may include higher-rank measurements applied by Eve, in line with that of the original CV-MDI protocol introduced in the previous section. However, we will see later that a non-Gaussian component emerges in Eve's system due to the discrete modulation required for post-selection, hence proving the optimality of the Gaussian attack in this context is an open problem.

In order to ensure our protocol description is as general as possible, we allow the homodyne detection to have an associated efficiency η which can be modeled by assuming modes A'' and B'' pass through beam splitters of transmissivity η where they are each mixed with one half of separate TMSV states with identical variance S before arriving at 100% efficient homodyne detectors. We may assume that the noise of the detectors is untrusted, in which case we assume the TMSV states are part of Eve's state and are included in the calculation of Eve's information, or trusted, in which case they are discarded. If $S = 1$, and $\tau_A = \tau_B = \tau$, the detector inefficiencies can be modeled without considering beam splitter interactions at the relay by absorbing them into the transmissivities of the links such that $\tau \rightarrow \eta\tau$. We outline each model schematically in Fig. 5.3.

Bob's Broadcasting of the tuple $(\mathbb{B}, p_B)$ or $(q_B, \mathbb{B}')$ achieves the task of ensuring that both parties can independently establish which instances of the protocol should be included in the final key. Such a communication step is likely a necessity in any post-selection protocol, however, it is possible that there is a more optimal strategy that reduces the amount of information Bob must broadcast and therefore the amount of information Eve gains. Such a strategy would yield a secret key rate that lies in between the achievable lower bound in which Bob broadcasts $(\mathbb{B}, p_B)$ or $(q_B, \mathbb{B}')$ in every use of the protocol and the upper bound in which no information is broadcast by Bob. An alternative way to think about the latter is to consider a restricted eavesdropping scenario in which Eve does not use the information broadcast by Bob in her attack. In the following sections, we will compute the secret key rate of the lower bound as well as that of what we will henceforth refer to as the restricted eavesdropping scenario. To establish Eve's state under restricted eavesdropping, we need to consider an entanglement-based version of the protocol as shown in Fig. 5.2(b). Bob's action may be modeled as measuring one mode of a TMSV state with modulation μ. The amplitude of the coherent states $|\tilde{\beta}\rangle$ remotely prepared as a result of this process is related to the measurement outcome $\boldsymbol{\beta}$ by

$$\tilde{\beta} = \xi \boldsymbol{\beta}^*, \quad \xi = \sqrt{\frac{\mu+1}{\mu-1}} \tag{5.2.17}$$

and we label Bob's heterodyne measurement outcome as $(\tilde{\kappa}\,\mathbb{B}, \tilde{\kappa}'\,\mathbb{B}')$.

5.2.2 Mode propagation

Our goal in the forthcoming sections is to establish the post-selected asymptotic key rate of the protocol, R_{PS}. However, our initial objective is to obtain a formula for the usual asymptotic secret key rate R given by

$$R = \beta I_{AB} - \chi, \tag{5.2.18}$$

where I_{AB} is the mutual information between Alice and Bob, β is the reconciliation efficiency and χ is the Holevo bound. To this end, we follow the propagation of the covariance matrix (CM) of the total Alice-Bob-Eve system and its associated mean value. With the individual uses of the protocol being Gaussian, these are the only tools we need to compute the probabilities and states needed to derive the key rate. After completing this task, we will proceed to explain the post-selection procedure which allows us to extend the range of the protocol.

Let us begin with the initial CM of the total system which is simply the direct sum of the CMs of the constituent systems,

$$\mathbf{V}_{AB\,\mathfrak{E}\,|\boldsymbol{\kappa}\mathbf{a}\tilde{\boldsymbol{\kappa}}\mathbf{b}} = \mathbf{I}_A \oplus \mathbf{I}_B \oplus \mathbf{V}_{\mathfrak{E}} \tag{5.2.19}$$

where $\mathbf{V}_{\mathfrak{E}}$ is Eve's initial CM, which, assuming she controls the detector noise at the relay, is given by

$$\mathbf{V}_{\mathfrak{E}} = \mathbf{V}_{\mathrm{TMSV}}(\omega_A) \oplus \mathbf{V}_{\mathrm{TMSV}}(\omega_B) \oplus \mathbf{V}_{\mathrm{TMSV}}(S) \oplus \mathbf{V}_{\mathrm{TMSV}}(S),$$

with $\mathbf{V}_{\mathrm{TMSV}}(\mu)$ being the CM of a TMSV state with variance μ. The mean value of the combined system of Alice and Bob is given by

$$\bar{\mathbf{x}}_{AB|\boldsymbol{\kappa}\mathbf{a}\tilde{\boldsymbol{\kappa}}\mathbf{b}} = (\kappa\mathbb{A}, \kappa'\mathbb{A}', \tilde{\kappa}\mathbb{B}, \tilde{\kappa}'\mathbb{B}')^{\mathsf{T}}, \tag{5.2.20}$$

while the mean value of Eve's system can be taken initially as zero. The action of all of the beam splitters can be encapsulated by the matrix $\mathbf{T}$ that, when applied to the system, gives the post-propagation CM $\mathbf{V}_{A''B''E'e|\boldsymbol{\kappa}\mathbf{a}\tilde{\boldsymbol{\kappa}}\mathbf{b}}$ and mean value $\bar{\mathbf{x}}_{A''B''E'e|\boldsymbol{\kappa}\mathbf{a}\tilde{\boldsymbol{\kappa}}\mathbf{b}}$. Eve's CM with conditioning on $\boldsymbol{\gamma}$ is obtained by performing the homodyne measurements at the relay on the modes A'' and B'' in the p- and q-quadrature, respectively. The measurement outcome in the q-quadrature, γ_q with conditioning on the measurement outcome of the p-quadrature, γ_p, is given by

$$p(\gamma_q|\boldsymbol{\kappa}\mathbf{a}\tilde{\boldsymbol{\kappa}}\mathbf{b}\gamma_p) = \frac{1}{\sqrt{2\pi\upsilon}}\exp\left[-\frac{1}{2\upsilon}\left(\gamma+\sqrt{\frac{\eta}{2}}(\kappa\mathbb{A}\sqrt{\tau_A}-\tilde{\kappa}\mathbb{B}\sqrt{\tau_B})\right)^2\right] \tag{5.2.21}$$

and in the reverse case we have

$$p(\gamma_p|\boldsymbol{\kappa}\mathbf{a}\tilde{\boldsymbol{\kappa}}\mathbf{b}\gamma_q) = \frac{1}{\sqrt{2\pi\upsilon}}\exp\left[-\frac{1}{2\upsilon}\left(\gamma-\sqrt{\frac{\eta}{2}}\left(\kappa'\mathbb{A}'\sqrt{\tau_A}+\tilde{\kappa}'\mathbb{B}'\sqrt{\tau_B}\right)\right)^2\right] \tag{5.2.22}$$

where

$$\upsilon = (1-\eta)S + \frac{\eta}{2}[\tau_A+\tau_B+(1-\tau_A)\omega_A+(1-\tau_B)\omega_B]. \tag{5.2.23}$$

Note that the two quadratures are independent, we have

$$p(\gamma_q|\boldsymbol{\kappa}\mathbf{a}\tilde{\boldsymbol{\kappa}}\mathbf{b}\gamma_p) = p(\gamma_q|\kappa\tilde{\kappa}\mathbb{A}\mathbb{B}) \tag{5.2.24}$$

$$p(\gamma_p|\boldsymbol{\kappa}\mathbf{a}\tilde{\boldsymbol{\kappa}}\mathbf{b}\gamma_q) = p(\gamma_p|\kappa'\tilde{\kappa}'\mathbb{A}'\mathbb{B}'). \tag{5.2.25}$$

As in Chap. 4 for the one-way protocol, we may compute the asymptotic secret key rate by assuming that the parties always agree on one particular quadrature for encoding. In doing so, we simplify our calculation of the rate by ignoring the variables associated with the conjugate quadrature. Note, however, that the rate is independent of this choice of quadrature. We will arbitrarily choose the q-quadrature for our forthcoming calculation of the rate and we will employ the refined notation $\gamma \equiv \gamma_q$ while ignoring the variables κ', $\tilde{\kappa}'$, $\mathbb{A}'$ and $\mathbb{B}'$.

Restricted eavesdropping

In the restricted eavesdropping case, we again consider only the q-quadrature for our calculations. After applying the beam splitter operation to the CM and mean value, we obtain the relay measurement outcome $\gamma \equiv \gamma_q$ with probability

$$p(\gamma|\kappa\mathbb{A}) = \frac{1}{\sqrt{2\pi\tilde{\upsilon}}}\exp\left[-\frac{1}{2\tilde{\upsilon}}\left(\gamma+\kappa\mathbb{A}\sqrt{\frac{1}{2}\eta\tau_A}\right)^2\right], \tag{5.2.26}$$

where

$$\tilde{\upsilon} = (1-\eta)S + \frac{\eta}{2}\left[\tau_A+\tau_B\mu+(1-\tau_A)\omega_A+(1-\tau_B)\omega_B\right]. \tag{5.2.27}$$

After the relay measurements, the CM and mean value of the remaining system become $\mathbf{V}_{bE'e|\kappa\mathbb{A}\boldsymbol{\gamma}}$ and $\bar{\mathbf{x}}_{bE'e|\kappa\mathbb{A}\boldsymbol{\gamma}}$. Eve's CM and mean value are obtained by tracing out

Bob's remaining mode b. In the final step, Bob performs a heterodyne measurement on his retained mode. The associated probability distribution for this measurement is $p(\tilde{\kappa}\,\mathbb{B}, p_B|\kappa\mathbb{A}\gamma)$ and by integrating over p_B we obtain

$$p(\tilde{\kappa}\,\mathbb{B}|\kappa\mathbb{A}\gamma) = \frac{1}{\sqrt{2\pi V_b}}\exp\left\{-\frac{1}{2V_b}\left[\tilde{\kappa}\,\mathbb{B} - \frac{1}{\tilde{\upsilon}}\sqrt{(\mu^2-1)\frac{\eta\tau_B}{2}}\left(\gamma + \kappa\mathbb{A}\sqrt{\frac{\eta\tau_A}{2}}\right)\right]^2\right\}, \tag{5.2.28}$$

where

$$V_b = (\mu+1)\left(1 - \frac{\mu-1}{\upsilon}\frac{\eta\tau_B}{2}\right). \tag{5.2.29}$$

In the following sections, we will derive the secret key rate of the protocol for both eavesdropping scenarios based on the secret encoding variable κ and Bob's variable $\tilde{\kappa}$. We first compute the mutual information then the Holevo bound and, finally, we will introduce the post-selection procedure and calculate the post-selected rate.

5.2.3 Mutual information

Armed with expressions for the protocol outputs, we are now in a position to be able to compute the mutual information between Alice and Bob and thus the first term of the asymptotic secret key rate. The mutual information formula is given, independent of the eavesdropping strategy under consideration, by

$$I(\kappa : \tilde{\kappa}\,|\mathbb{A}\mathbb{B}\gamma) = H(\kappa|\mathbb{A}\mathbb{B}\gamma) - H(\kappa|\,\tilde{\kappa}\,\mathbb{A}\mathbb{B}\gamma), \tag{5.2.30}$$

where $H(X|Y)$ is the conditional Shannon entropy of X given Y (cf. Sec. 2.5.1). We may express the mutual information as the following single integral

$$I(\kappa : \tilde{\kappa} : \mathbb{A}\mathbb{B}\gamma) = \int p(\mathbb{A}\mathbb{B}\gamma)\left[H_{\kappa|\mathbb{A}\mathbb{B}\gamma} - \sum_{\tilde{\kappa}} p(\tilde{\kappa}|\mathbb{A}\mathbb{B}\gamma)H_{\kappa|\tilde{\kappa}\mathbb{A}\mathbb{B}\gamma}\right]\mathrm{d}\mathbb{A}\,\mathrm{d}\mathbb{B}\,\mathrm{d}\gamma\,. \tag{5.2.31}$$

The key components of the mutual information are the entropies $H_{\kappa|\mathbb{A}\mathbb{B}\gamma}$ and $H_{\kappa|\,\tilde{\kappa}\,\mathbb{A}\mathbb{B}\gamma}$ which reduce to binary entropies of respective probabilities $p(\kappa|\mathbb{A}\mathbb{B}\gamma)$ and $p(\kappa|\,\tilde{\kappa}\,\mathbb{A}\mathbb{B}\gamma)$. The majority of the following section is dedicated to determining their form for both complete and restrictive eavesdropping. The main mathematical tool required in this process is Baye's rule, which we apply repeatedly in order to attain these probabilities from the known output of the protocol, $p(\gamma|\kappa\mathbb{A}\mathbb{B})$ and the initial probabilities $p(\kappa\mathbb{A})$ and $p(\tilde{\kappa}\mathbb{B})$.

Considering the strongest eavesdropping scenario first, the conditional probability $p(\kappa|\,\tilde{\kappa}\,\mathbb{A}\mathbb{B}\gamma)$ can be computed as follows

$$\begin{aligned} p(\kappa|\,\tilde{\kappa}\,\mathbb{A}\mathbb{B}\gamma) &= \frac{p(\gamma|\kappa\,\tilde{\kappa}\,\mathbb{A}\mathbb{B})p(\kappa|\,\tilde{\kappa}\,\mathbb{A}\mathbb{B})}{\sum_{\kappa} p(\gamma|\kappa\,\tilde{\kappa}\,\mathbb{A}\mathbb{B})p(\kappa|\,\tilde{\kappa}\,\mathbb{A}\mathbb{B})} \\ &= \frac{1}{1+\exp\left[2\kappa\mathbb{A}\sqrt{\frac{1}{2}\eta\tau_A}\left(\gamma - \tilde{\kappa}\,\mathbb{B}\sqrt{\frac{1}{2}\eta\tau_B}\right)\upsilon^{-1}\right]}, \end{aligned} \tag{5.2.32}$$

where υ is defined in Eq. (5.2.23) and we have used the fact that κ, $\tilde{\kappa}$, $\mathbb{A}$ and $\mathbb{B}$ are independent variables. Using the same logic, we arrive at the following expression for the reverse probability

$$p(\,\tilde{\kappa}\,|\kappa\mathbb{A}\mathbb{B}\gamma) = \frac{1}{1+\exp\left[-2\,\tilde{\kappa}\,\mathbb{B}\sqrt{\frac{1}{2}\eta\tau_B}\left(\gamma + \kappa\mathbb{A}\sqrt{\frac{1}{2}\eta\tau_A}\right)\upsilon^{-1}\right]}. \tag{5.2.33}$$

The next step is to compute the total probabilities $p(\kappa|\mathbb{A}\mathbb{B}\gamma)$ and $p(\tilde{\kappa}|\mathbb{A}\mathbb{B}\gamma)$. For the former we obtain

$$\begin{aligned} p(\kappa|\mathbb{A}\mathbb{B}\gamma) &= \frac{\sum_{\tilde{\kappa}} p(\gamma|\kappa\,\tilde{\kappa}\,\mathbb{A}\mathbb{B})p(\kappa\,\tilde{\kappa}\,|\mathbb{A}\mathbb{B})}{\sum_{\kappa,\tilde{\kappa}} p(\gamma|\kappa\,\tilde{\kappa}\,\mathbb{A}\mathbb{B})p(\kappa\,\tilde{\kappa}\,|\mathbb{A}\mathbb{B})} \\ &= \frac{1}{1+\left(\frac{p(+|1\mathbb{A}\mathbb{B}\gamma)}{p(-|0\mathbb{A}\mathbb{B}\gamma)}\right)^{\kappa}\exp\left[2\kappa\sqrt{\frac{1}{2}\eta}(\mathbb{B}\sqrt{\tau_B}+\mathbb{A}\sqrt{\tau_A})\upsilon^{-1}\right]}, \end{aligned} \tag{5.2.34}$$

where we note that $p(\kappa\,\tilde{\kappa}\,|\mathbb{A}\mathbb{B}) = 1/4$ for all combinations of κ and $\tilde{\kappa}$ due to the independence of the variables. Using the same logic we obtain the last probability required for the calculation of the conditional entropies,

$$p(\tilde{\kappa}\,|\mathbb{A}\mathbb{B}\gamma) = \frac{1}{1+\left(\frac{p(0|-\mathbb{A}\mathbb{B}\gamma)}{p(1|+\mathbb{A}\mathbb{B}\gamma)}\right)^{\tilde{\kappa}}\exp\left[-2\,\tilde{\kappa}\,\sqrt{\frac{1}{2}\eta}(\mathbb{B}\sqrt{\tau_B}+\mathbb{A}\sqrt{\tau_A})\upsilon^{-1}\right]}. \tag{5.2.35}$$

The final probability we require is the total probability of all of the post-selection variables which is simply given by $p(\mathbb{A}\mathbb{B}\gamma) = \sum_{\kappa,\tilde{\kappa}} p(\gamma|\kappa\,\tilde{\kappa}\,\mathbb{A}\mathbb{B})p(\kappa\mathbb{A})p(\tilde{\kappa}\,\mathbb{B})$.

Restricted eavesdropping

The computation of the probabilities required for the mutual information in the restricted eavesdropping scenario are slightly cumbersome due to Bob's TMSV state, however, the first conditional probability is easily attainable as

$$p(\tilde{\kappa}\,|\kappa\mathbb{A}\mathbb{B}\gamma) = \frac{p(\tilde{\kappa}\,\mathbb{B}|\kappa\mathbb{A}\gamma)}{\sum p(\tilde{\kappa}\,\mathbb{B}|\kappa\mathbb{A}\gamma)} = \frac{1}{1+\exp\left[-2\,\tilde{\kappa}\,\mathbb{B}\left(\gamma+\kappa\mathbb{A}\sqrt{\frac{1}{2}\eta\tau_A}\right)\Delta\;\tilde{\upsilon}'^{-1}\right]}. \tag{5.2.36}$$

By setting $\mu = 1$ in the expression for $\tilde{\upsilon}$ in Eq. (5.2.27), we define the variance $\tilde{\upsilon}'$,

$$\tilde{\upsilon}' = (1-\eta)S + \frac{\eta}{2}\left[\tau_A + \tau_B + \omega_A(1-\tau_A) + \omega_B(1-\tau_B)\right] \tag{5.2.37}$$

and we also define

$$\Delta = \sqrt{\frac{\eta}{2}\frac{1}{\tau_B}}\sqrt{\frac{\mu-1}{\mu+1}}. \tag{5.2.38}$$

In order to calculate the reverse probability $p(\kappa|\,\tilde{\kappa}\,\mathbb{A}\mathbb{B}\gamma)$, we first compute

$$p(\kappa|\mathbb{A}\gamma) = \frac{p(\gamma|\kappa\mathbb{A})}{\sum_\kappa p(\gamma|\kappa\mathbb{A})} = \frac{1}{1+\exp\left(2\kappa\mathbb{A}\gamma\sqrt{\frac{1}{2}\eta\tau_A}\tilde{\upsilon}^{-1}\right)} \tag{5.2.39}$$

then the required probability can be derived as

$$p(\kappa|\,\tilde{\kappa}\,\mathbb{A}\mathbb{B}\gamma) = \frac{p(\tilde{\kappa}\,\mathbb{B}|\kappa\mathbb{A}\gamma)p(\kappa|\mathbb{A}\gamma)}{\sum_\kappa p(\tilde{\kappa}\,\mathbb{B}|\kappa\mathbb{A}\gamma)p(\kappa|\mathbb{A}\gamma)} = \frac{1}{1+\exp\left[2\kappa\mathbb{A}\sqrt{\frac{1}{2}\eta\tau_A}\left(\gamma' - \tilde{\kappa}\,\mathbb{B}\Delta\right)\tilde{\upsilon}'^{-1}\right]} \tag{5.2.40}$$

where we have defined

$$\gamma' = \frac{1}{\tilde{\upsilon}}\left(\tilde{\upsilon}' + \frac{\eta}{2}\frac{1}{\tau_B}(\mu-1)\right)\gamma. \tag{5.2.41}$$

We can now compute the total probabilities of κ and $\tilde{\kappa}$ as

$$\begin{aligned} p(\kappa|\mathbb{A}\mathbb{B}\gamma) &= \frac{\sum_{\tilde{\kappa}} p(\tilde{\kappa}\,\mathbb{B}|\kappa\mathbb{A}\gamma)p(\kappa|\mathbb{A}\gamma)}{\sum_{\kappa,\tilde{\kappa}} p(\tilde{\kappa}\,\mathbb{B}|\kappa\mathbb{A}\gamma)p(\kappa|\mathbb{A}\gamma)} \\ &= \frac{1}{1+\Xi_\kappa\exp\left[2\kappa\mathbb{A}\sqrt{\frac{1}{2}\eta\tau_A}\left(\gamma' + \mathbb{B}\Delta\right)\tilde{\upsilon}'^{-1}\right]} \end{aligned} \tag{5.2.42}$$

and

$$p(\tilde{\kappa}\,|\mathbb{A}\mathbb{B}\gamma) = \frac{1}{1+\Xi_{\tilde{\kappa}}\exp\left[-2\,\tilde{\kappa}\,\mathbb{B}\left(\gamma - \mathbb{A}\sqrt{\frac{1}{2}\eta\tau_A}\right)\Delta\;\tilde{\upsilon}'^{-1}\right]} \tag{5.2.43}$$

with

$$\Xi_m = \left(\frac{p(1|+\mathbb{A}\mathbb{B}\gamma)}{p(1|-\mathbb{A}\mathbb{B}\gamma)}\right)^m. \tag{5.2.44}$$

Finally, the total probability of the three post-selection variables becomes $p(\mathbb{A}\mathbb{B}\gamma) = \sum_{\kappa,\tilde{\kappa}} p(\tilde{\kappa}\,\mathbb{B}|\kappa\mathbb{A}\gamma)p(\gamma|\kappa\mathbb{A})p(\kappa\mathbb{A})$.

5.2.4 Eve's accessible information

We now turn to the task of quantifying Eve's accessible information on the secret variable. As we are assuming collective entangling cloner attacks, we make use of the Holevo bound χ, to establish the maximum amount of information Eve may attain using any strategy permitted by the laws of quantum mechanics. The Holevo bound is given by

$$\chi(\mathfrak{E}' : \kappa|\mathbb{A}\mathbb{B}\gamma) = S(\mathfrak{E}'|\mathbb{A}\mathbb{B}\gamma) - S(\mathfrak{E}'|\kappa\mathbb{A}\mathbb{B}\gamma), \tag{5.2.45}$$

where the first term can be written in terms of Eve's total state $\hat{\rho}_{\mathfrak{E}'|\mathbb{A}\mathbb{B}\gamma}$ as

$$S(\mathfrak{E}'|\mathbb{A}\mathbb{B}\gamma) = \int p(\mathbb{A}\mathbb{B}\gamma) S(\hat{\rho}_{\mathfrak{E}'|\mathbb{A}\mathbb{B}\gamma})\, \mathrm{d}\mathbb{A}\, \mathrm{d}\mathbb{B}\, \mathrm{d}\gamma\,, \tag{5.2.46}$$

where $S(\hat{\rho})$ is the VNE of state $\hat{\rho}$ introduced in Section 2.5. The second term of the Holevo bound is established using Eve's state conditioned on the clandestine variable, $\hat{\rho}_{\mathfrak{E}'|\kappa\mathbb{A}\mathbb{B}\gamma}$. It may be written as

$$S(\mathfrak{E}'|\kappa\mathbb{A}\mathbb{B}\gamma) = \int p(\mathbb{A}\mathbb{B}\gamma) \sum_{\kappa} p(\kappa|\mathbb{A}\mathbb{B}\gamma) S\left(\hat{\rho}_{\mathfrak{E}'|\kappa\mathbb{A}\mathbb{B}\gamma}\right) \mathrm{d}\mathbb{A}\, \mathrm{d}\mathbb{B}\, \mathrm{d}\gamma\,. \tag{5.2.47}$$

Access to both the total and conditional states is obtained by manipulation of the post-propagation state of Eve's system, $\hat{\rho}_{\mathfrak{E}'|\kappa\mathbb{A}\,\tilde{\kappa}\,\mathbb{B}\gamma}$ which can be derived from the corresponding CM and mean value. We may write her total and conditional states as

$$\hat{\rho}_{\mathfrak{E}'|\mathbb{A}\mathbb{B}\gamma} = \sum_{\kappa,\tilde{\kappa}} p(\kappa\,\tilde{\kappa}\,|\mathbb{A}\mathbb{B}\gamma)\hat{\rho}_{\mathfrak{E}'|\kappa\mathbb{A}\,\tilde{\kappa}\,\mathbb{B}\gamma} \tag{5.2.48}$$

$$\text{and} \quad \hat{\rho}_{\mathfrak{E}'|\kappa\mathbb{A}\mathbb{B}\gamma} = \sum_{\tilde{\kappa}} p(\tilde{\kappa}\,|\kappa\mathbb{A}\mathbb{B}\gamma)\hat{\rho}_{\mathfrak{E}'|\kappa\,\tilde{\kappa}\,\mathbb{A}\mathbb{B}\gamma}. \tag{5.2.49}$$

Neither the total nor the condition states are Gaussian, and computing their entropy directly in the Fock basis is a difficult problem due to Eve now being in possession of four modes. Instead, we follow a method originally used for post-selection of one-way coherent state protocol originating from Refs [56, 57]. With little added complexity, we can derive the equivalent method for the MDI protocol.

Let us first note that Eve's state emerging after the propagation of the modes is pure and can be written in the bra-ket notation as

$$\hat{\rho}_{\mathfrak{E}'|\kappa\,\tilde{\kappa}\,\mathbb{A}\mathbb{B}\gamma} = \hat{\mathfrak{E}}'^{\mathbb{A}\mathbb{B}\gamma}_{\kappa\,\tilde{\kappa}} = \left|\mathfrak{E}'^{\mathbb{A}\mathbb{B}\gamma}_{\kappa\,\tilde{\kappa}}\right\rangle \left\langle\mathfrak{E}'^{\mathbb{A}\mathbb{B}\gamma}_{\kappa\,\tilde{\kappa}}\right|. \tag{5.2.50}$$

For convenience, we also introduce the shorthand notation

$$p^{\mathbb{A}\mathbb{B}\gamma}_{\kappa\,\tilde{\kappa}} \equiv p(\kappa\,\tilde{\kappa}\,|\mathbb{A}\mathbb{B}\gamma) \quad \text{and} \quad p^{\mathbb{A}\mathbb{B}\gamma}_{\tilde{\kappa}\,|\kappa} \equiv p(\tilde{\kappa}\,|\kappa\mathbb{A}\mathbb{B}\gamma). \tag{5.2.51}$$

Using the broadcast values $\mathbb{A}$, p_A, $\mathbb{B}$, p_B and $\boldsymbol{\gamma}$, Eve knows that her total state is a convex combination of the four states $\left|\mathfrak{E}'^{\mathbb{A}\mathbb{B}\gamma}_{0+}\right\rangle$, $\left|\mathfrak{E}'^{\mathbb{A}\mathbb{B}\gamma}_{0-}\right\rangle$, $\left|\mathfrak{E}'^{\mathbb{A}\mathbb{B}\gamma}_{1+}\right\rangle$ and $\left|\mathfrak{E}'^{\mathbb{A}\mathbb{B}\gamma}_{1-}\right\rangle$ and it can therefore be expressed in a four-dimensional Hilbert space. Let us note at this point that in our notation we use Alice's assigned bit values 0(1) to represent $\kappa = +(-)$ in order to aide distinguishability between κ and $\tilde{\kappa}$. Eve's total state in Eq. (5.2.48) may be expressed conveniently in this shorthand notation as

$$\hat{\rho}_{\mathfrak{E}'|\mathbb{A}\mathbb{B}\gamma} = \sum_{\kappa,\tilde{\kappa}} p^{\mathbb{A}\mathbb{B}\gamma}_{\kappa\,\tilde{\kappa}} \left|\mathfrak{E}'^{\mathbb{A}\mathbb{B}\gamma}_{\kappa\,\tilde{\kappa}}\right\rangle \left\langle\mathfrak{E}'^{\mathbb{A}\mathbb{B}\gamma}_{\kappa\,\tilde{\kappa}}\right| . \tag{5.2.52}$$

The next step in our task of determining Eve's state is to compute the matrix of all overlaps $\mathbf{S}$, whose elements are given by the combinations of the overlaps $\left\langle\mathfrak{E}'^{\mathbb{A}\mathbb{B}\gamma}_{\kappa_1\,\tilde{\kappa}_1}\middle|\mathfrak{E}'^{\mathbb{A}\mathbb{B}\gamma}_{\kappa_2\,\tilde{\kappa}_2}\right\rangle$ of Eve's possible states. We may write the matrix of overlaps as

$$\mathbf{S} = \begin{array}{cccc|c} 0+ & 0- & 1+ & 1- & \\ 1 & B & A & AB & 0+ \\ B & 1 & AB & A & 0- \\ A & AB & 1 & B & 1+ \\ AB & A & B & 1 & 1- \end{array} \tag{5.2.53}$$

where we have ignored irrelevant phase factors by noting that they may always be removed by multiplying the states $\left|\mathfrak{E}'^{\mathbb{A}\mathbb{B}\gamma}_{\kappa\,\tilde{\kappa}}\right\rangle$ by other appropriate phase factors without modifying the nature of the state. The matrix of overlaps reveals the interrelationship between the basis vectors in Eve's total state. It can be seen that the matrix is expressible in tensor product form as

$$\mathbf{S} = \begin{pmatrix} 1 & A \\ A & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & B \\ B & 1 \end{pmatrix} \tag{5.2.54}$$

which implies that Eve's state is the product of two states in two-dimensional Hilbert spaces, which we write as

$$\left|\mathfrak{E}'^{\mathbb{A}\mathbb{B}\gamma}_{\kappa\,\tilde{\kappa}}\right\rangle = \left|\mathfrak{E}'^{\mathbb{A}\mathbb{B}\gamma}_{\kappa}\right\rangle \left|\mathfrak{E}'^{\mathbb{A}\mathbb{B}\gamma}_{\tilde{\kappa}}\right\rangle . \tag{5.2.55}$$

The individual states can be expanded as

$$\left|\mathfrak{E}_0'^{\mathbb{A}\mathbb{B}\gamma}\right\rangle = c_0\left|\Phi_0\right\rangle + c_1\left|\Phi_1\right\rangle, \quad \left|\mathfrak{E}_1'^{\mathbb{A}\mathbb{B}\gamma}\right\rangle = c_0\left|\Phi_0\right\rangle - c_1\left|\Phi_1\right\rangle \tag{5.2.56}$$

and

$$\left|\mathfrak{E}_+'^{\mathbb{A}\mathbb{B}\gamma}\right\rangle = c_+\left|\Phi_+\right\rangle + c_-\left|\Phi_-\right\rangle, \quad \left|\mathfrak{E}_-'^{\mathbb{A}\mathbb{B}\gamma}\right\rangle = c_+\left|\Phi_+\right\rangle - c_-\left|\Phi_-\right\rangle, \tag{5.2.57}$$

where $\{\left|\Phi_0\right\rangle, \left|\Phi_1\right\rangle\}$ and $\{\left|\Phi_+\right\rangle, \left|\Phi_-\right\rangle\}$ are orthonormal basis sets for the Hilbert spaces spanned by $\left|\mathfrak{E}_\kappa'^{\mathbb{A}\mathbb{B}\gamma}\right\rangle$ and $\left|\mathfrak{E}_{\tilde{\kappa}}'^{\mathbb{A}\mathbb{B}\gamma}\right\rangle$, respectively. Our focus now turns to relating the coefficients to the overlaps A and B. We perform the following inner products

$$\left\langle\mathfrak{E}_0'^{\mathbb{A}\mathbb{B}\gamma}\middle|\mathfrak{E}_0'^{\mathbb{A}\mathbb{B}\gamma}\right\rangle = |c_0|^2 + |c_1|^2 = 1 \tag{5.2.58}$$

$$\left\langle\mathfrak{E}_0'^{\mathbb{A}\mathbb{B}\gamma}\middle|\mathfrak{E}_1'^{\mathbb{A}\mathbb{B}\gamma}\right\rangle = |c_0|^2 - |c_1|^2 = A \tag{5.2.59}$$

from which we obtain expressions for the absolute values of the coefficients c_0 and c_1 of

$$|c_0|^2 = \frac{1}{2}(1 + A) \tag{5.2.60}$$

$$\text{and} \quad |c_1|^2 = \frac{1}{2}(1 - A), \tag{5.2.61}$$

and following a similar calculation we arrive at the following expressions for the absolute values of the remaining coefficients

$$|c_+|^2 = \frac{1}{2}(1 + B) \tag{5.2.62}$$

$$\text{and} \quad |c_-|^2 = \frac{1}{2}(1 - B). \tag{5.2.63}$$

The elements of the matrix of overlaps and, therefore, the values A and B, are computed from the overlap formula for Gaussian states [88], which, for two pure states $\hat{\rho}_1$ and $\hat{\rho}_2$ with the same CM, $\mathbf{V}$ and different mean values $\bar{\mathbf{x}}_1$ and $\bar{\mathbf{x}}_2$, reduces to

$$\operatorname{tr}(\hat{\rho}_1\hat{\rho}_2) = \exp\left[-\frac{1}{4}(\bar{\mathbf{x}}_1 - \bar{\mathbf{x}}_2)^\mathsf{T}\mathbf{V}^{-1}(\bar{\mathbf{x}}_1 - \bar{\mathbf{x}}_2)\right] \tag{5.2.64}$$

and our coefficients A and B become

$$A = \left\langle\mathfrak{E}_0'^{\mathbb{A}\mathbb{B}\gamma}\middle|\mathfrak{E}_1'^{\mathbb{A}\mathbb{B}\gamma}\right\rangle = \exp\left[-\frac{1}{2}\mathbb{A}^2\left(1 - \frac{\eta\tau_A}{\upsilon}\right)\right] \tag{5.2.65}$$

and

$$B = \left\langle \mathfrak{E}_{+}^{\prime\mathbb{A}\mathbb{B}\gamma} \middle| \mathfrak{E}_{-}^{\prime\mathbb{A}\mathbb{B}\gamma} \right\rangle = \exp\left[-\frac{1}{2}\mathbb{B}^2\left(1-\frac{\eta\tau_B}{\upsilon}\right)\right]. \tag{5.2.66}$$

Note that the overlaps are independent of the relay measurement outcomes. At this point we have derived the necessary tools required to compute Eve's total state using Eq. (5.2.52). We arrive at the following matrix

$$\hat{\mathfrak{E}}^{\prime\mathbb{A}\mathbb{B}\gamma} = \tag{5.2.67}$$

$$\begin{pmatrix} |c_0|^2|c_+|^2 & & h.c. & \\ |c_0|^2 c_- c_+^* \Lambda(+,-,+,-) & |c_0|^2|c_-|^2 & & \\ |c_+|^2 c_1 c_0^* \Lambda(+,+,-,-) & c_1 c_+ c_0^* c_-^* \Lambda(+,-,-,+) & |c_1|^2|c_+|^2 & \\ c_1 c_- c_0^* c_+^* \Lambda(+,-,-,+) & |c_-|^2 c_1 c_0^* \Lambda(+,+,-,-) & |c_1|^2 c_0 c_+^* \Lambda(+,-,+,-) & |c_1|^2|c_-|^2 \end{pmatrix} \tag{5.2.68}$$

where h.c. represents the hermitian conjugate of the lower triangle of the matrix and the function Λ is defined as

$$\Lambda(s_1,s_2,s_3,s_4) = s_1 p_{0+}^{\mathbb{A}\mathbb{B}\gamma} + s_2 p_{0-}^{\mathbb{A}\mathbb{B}\gamma} + s_3 p_{1+}^{\mathbb{A}\mathbb{B}\gamma} + s_4 p_{1-}^{\mathbb{A}\mathbb{B}\gamma}. \tag{5.2.69}$$

To obtain the entropy of the total state, we first compute the eigenvalues of Eq. (5.2.68) which amounts to solving a quartic equation in which the coefficients are combinations of the absolute values of the basis coefficients. From these eigenvalues, the VNE is readily obtained and can then be substituted into Eq. (5.2.46) to obtain the first term of the Holevo bound.

In order to compute the conditional state and the second term of the Holevo bound, we construct the density matrices of the conditional states. Using the separable nature of the state, we are able to write

$$\hat{\mathfrak{E}}_0^{\prime\mathbb{A}\mathbb{B}\gamma} = \left|\mathfrak{E}_0^{\prime\mathbb{A}\mathbb{B}\gamma}\right\rangle\left\langle\mathfrak{E}_0^{\prime\mathbb{A}\mathbb{B}\gamma}\right| \otimes \left(p_{+|0}^{\mathbb{A}\mathbb{B}\gamma}\left|\mathfrak{E}_+^{\prime\mathbb{A}\mathbb{B}\gamma}\right\rangle\left\langle\mathfrak{E}_+^{\prime\mathbb{A}\mathbb{B}\gamma}\right| + p_{-|0}^{\mathbb{A}\mathbb{B}\gamma}\left|\mathfrak{E}_-^{\prime\mathbb{A}\mathbb{B}\gamma}\right\rangle\left\langle\mathfrak{E}_-^{\prime\mathbb{A}\mathbb{B}\gamma}\right|\right) \tag{5.2.70}$$

and

$$\hat{\mathfrak{E}}_1^{\prime\mathbb{A}\mathbb{B}\gamma} = \left|\mathfrak{E}_1^{\prime\mathbb{A}\mathbb{B}\gamma}\right\rangle\left\langle\mathfrak{E}_1^{\prime\mathbb{A}\mathbb{B}\gamma}\right| \otimes \left(p_{+|1}^{\mathbb{A}\mathbb{B}\gamma}\left|\mathfrak{E}_+^{\prime\mathbb{A}\mathbb{B}\gamma}\right\rangle\left\langle\mathfrak{E}_+^{\prime\mathbb{A}\mathbb{B}\gamma}\right| + p_{-|1}^{\mathbb{A}\mathbb{B}\gamma}\left|\mathfrak{E}_-^{\prime\mathbb{A}\mathbb{B}\gamma}\right\rangle\left\langle\mathfrak{E}_-^{\prime\mathbb{A}\mathbb{B}\gamma}\right|\right). \tag{5.2.71}$$

It is then straightforward to obtain the sets of eigenvalues

$$\lambda_{1,2}^{0} = \frac{1}{2}\left(1 \pm \sqrt{1-16 p_{+|0}^{\mathbb{A}\mathbb{B}\gamma} p_{-|0}^{\mathbb{A}\mathbb{B}\gamma}|c_-|^2|c_+|^2}\right) \tag{5.2.72}$$

and

$$\lambda^{1}_{1,2} = \frac{1}{2}\left(1 \pm \sqrt{1 - 16 p^{\mathbb{AB}\gamma}_{+|1} p^{\mathbb{AB}\gamma}_{-|1} |c_-|^2 |c_+|^2}\right), \tag{5.2.73}$$

from which we compute the second term of the Holevo bound using Eq. (5.2.47). It is interesting to note that unlike in the case of the one-way protocol, the sets of eigenvalues are not degenerate. This is a consequence of the correlations created by the relay.

Restricted eavesdropping

Let us now consider Eve's accessible information in the restricted eavesdropping scenario. In this case, Eve has to distinguish between two states corresponding to the two possible values of κ. Under these conditions, it is possible to consider both individual and collective attacks as we will outline in the following.

Let us first examine the most straightforward case in which Eve employs individual attacks, and may not access a quantum memory. In this case the mutual information between Alice and Eve, I_{AE}, can be estimated by from Eve's error probability using the fidelity, F of Eve's two possible states, $\hat{\rho}_{\mathfrak{E}'|+\mathbb{A}\gamma}$ and $\hat{\rho}_{\mathfrak{E}'|-\mathbb{A}\gamma}$ which we compute using Eq. (5.2.64). We apply the lower bound

$$F_- = \frac{1 - \sqrt{1 - F}}{2} \tag{5.2.74}$$

in order to bound Eve's error probability from below, modeling a worst-case scenario for Alice and Bob [89]. The total expression for the mutual information I_{AB} becomes

$$I_{AE} = \int p(\mathbb{A}\gamma)\,[1 - H_2(F_-)]\,\mathrm{d}\mathbb{A}\,\mathrm{d}\gamma\,, \tag{5.2.75}$$

where $H_2(p)$ is the binary entropy.

In the case of collective attacks we must compute the Holevo bound in order to establish an upper-bound on Eve's accessible information. The Holevo bound is given by

$$\chi^{\mathrm{RE}}(\mathfrak{E}' : \kappa|\mathbb{A}\gamma) = S(\mathfrak{E}'|\mathbb{A}\gamma) - S(\mathfrak{E}'|\kappa\mathbb{A}\gamma), \tag{5.2.76}$$

where the first term can be written as

$$S(\mathfrak{E}'|\mathbb{A}\gamma) = \int p(\mathbb{A}\gamma) S(\hat{\rho}_{\mathfrak{E}'|\mathbb{A}\gamma})\,\mathrm{d}\mathbb{A}\,\mathrm{d}\gamma\,, \tag{5.2.77}$$

where $\hat{\rho}_{\mathfrak{E}'|\mathbb{A}\gamma}$ is the total state, given by

$$\hat{\rho}_{\mathfrak{E}'|\mathbb{A}\gamma} = \sum_{\kappa} p(\kappa|\mathbb{A}\gamma)\hat{\rho}_{\mathfrak{E}'|\kappa\mathbb{A}\gamma}. \tag{5.2.78}$$

As it is derived from the sum of two Gaussian states, the total state is non-Gaussian. To avoid the difficulty in obtaining the entropy of this state from its photon statistics, we may employ a non-Gaussian entropy approximation which we derive in Appendix A. Using the main result we may write the CM of the total state as

$$\mathbf{V}_{\mathfrak{E}'|\mathbb{A}} = \mathbf{V}_{\mathfrak{E}'|\kappa\mathbb{A}} + p(+|\mathbb{A}\gamma)p(-|\mathbb{A}\gamma)\Delta\bar{\mathbf{x}}_{\mathfrak{E}'} \cdot \Delta\bar{\mathbf{x}}^{\mathsf{T}}_{\mathfrak{E}'}, \tag{5.2.79}$$

where $\Delta\bar{\mathbf{x}}_{\mathfrak{E}'} = \bar{\mathbf{x}}_{\mathfrak{E}'|+\mathbb{A}\gamma} - \bar{\mathbf{x}}_{\mathfrak{E}'|-\mathbb{A}\gamma}$. Taking the entropy of this state via the symplectic eigenvalues, $\{\nu_i\}$ of its CM provides an upper bound on the exact entropy of Eve's total state as it assumes this state to be Gaussian. We therefore have

$$S(\hat{\rho}_{\kappa\mathbb{A}\gamma}) \leq S(\mathbf{V}_{\mathfrak{E}'|\kappa\mathbb{A}\gamma}) = \sum_i h(\nu_i) \tag{5.2.80}$$

where we recall the following expression from Sec. 2.5.3

$$h(x) = \frac{x+1}{2}\log_2\frac{x+1}{2} - \frac{x-1}{2}\log_2\frac{x-1}{2}. \tag{5.2.81}$$

Meanwhile, the second term of the Holevo bound involves a Gaussian state and can be computed directly from the protocol output, independent of any measurement outcome. As described in Section 5.2.2, Eve's CM $\mathbf{V}_{\mathfrak{E}'|\kappa\mathbb{A}}$ after the relay measurements is obtained by tracing out Bob's remaining mode. The entropy is then simply computed from the symplectic eigenvalues, $\{\upsilon_i\}$ of the remaining CM by

$$S(\hat{\rho}_{\mathfrak{E}'|\kappa\mathbb{A}}) = S(\mathbf{V}_{\mathfrak{E}'|\kappa\mathbb{A}}) = \sum_i h(\upsilon_i). \tag{5.2.82}$$

The Holevo bound is then reduced to the following expression

$$\chi(\mathfrak{E}' : \kappa|\mathbb{A}\gamma) \leq \int p(\mathbb{A}\gamma)S(\mathbf{V}_{\mathfrak{E}'|\mathbb{A}\gamma})\,\mathrm{d}\mathbb{A}\,\mathrm{d}\gamma - S(\mathbf{V}_{\mathfrak{E}'|\kappa\mathbb{A}\gamma}). \tag{5.2.83}$$

5.2.5 Post-selection

At this point, we have obtained expressions for both terms of the asymptotic secret key rate under both complete and restricted eavesdropping and we may now manipulate these components in order to apply the technique of post-selection and improve the range of the protocol. Let us first re-write the mutual information integrand in the following form

$$I_{\mathrm{AB}} = \int p(\mathbb{A}\mathbb{B}\gamma)\tilde{I}_{\mathrm{AB}}(\mathbb{A},\mathbb{B},\gamma)\,\mathrm{d}\mathbb{A}\,\mathrm{d}\mathbb{B}\,\mathrm{d}\gamma\,. \tag{5.2.84}$$

where we defined the single-point mutual information

$$\tilde{I}_{\mathrm{AB}}(\mathbb{A},\mathbb{B},\gamma) = H_{\kappa|\mathbb{A}\mathbb{B}\gamma} - \sum_{\tilde{\kappa}} p(\tilde{\kappa}\,|\mathbb{A}\mathbb{B}\gamma)H_{\kappa|\,\tilde{\kappa}\,\mathbb{A}\mathbb{B}\gamma}. \tag{5.2.85}$$

Similarly, we can write the Holevo bound under complete eavesdropping as a single integrand

$$\chi = \int p(\mathbb{A}\mathbb{B}\gamma)\tilde{\chi}(\mathbb{A},\mathbb{B},\gamma)\,\mathrm{d}\mathbb{A}\,\mathrm{d}\mathbb{B}\,\mathrm{d}\gamma \tag{5.2.86}$$

with $\tilde{\chi}$ being the single-point Holevo bound given by

$$\tilde{\chi} = S(\hat{\rho}_{\mathfrak{E}'|\mathbb{A}\mathbb{B}\gamma}) - \sum_{\kappa} p(\kappa|\mathbb{A}\mathbb{B}\gamma)S(\rho_{\mathfrak{E}'|\kappa\mathbb{A}\mathbb{B}\gamma}). \tag{5.2.87}$$

In the same way, we define the following single-point Holevo bound for restricted eavesdropping, $\tilde{\chi}^{\mathrm{RE}}$ for collective attacks and the single-point mutual information between Alice and Eve, $\tilde{I}_{AE}$ for individual attacks,

$$\tilde{\chi}^{RE} \leq S(\mathbf{V}_{\mathfrak{E}'|\mathbb{A}\gamma}) - S(\mathbf{V}_{\mathfrak{E}'|\kappa\mathbb{A}\gamma}) \tag{5.2.88}$$

$$\tilde{I}_{AE} = 1 - H_2(F_-). \tag{5.2.89}$$

Using these definitions, we introduce the single-point rate, $\tilde{R} = \tilde{I}_{\mathrm{AB}} - \tilde{\chi}$ for complete eavesdropping, $\tilde{R} = \tilde{I}_{\mathrm{AB}} - \tilde{\chi}^{RE}$ for restricted eavesdropping under collective attacks and $\tilde{R} = \tilde{I}_{\mathrm{AB}} - \tilde{I}_{\mathrm{AE}}$ for restricted eavesdropping under individual attacks. We can then express the secret key rate in terms of the generic single-point rate as

$$R = \int p(\mathbb{A}\mathbb{B}\gamma)\tilde{R}(\mathbb{A},\mathbb{B},\gamma)\,\mathrm{d}\mathbb{A}\,\mathrm{d}\mathbb{B}\,\mathrm{d}\gamma\,. \tag{5.2.90}$$

For post-selection, we are interested in the region where the single-point rate is positive so that the parties can choose to only include instances of the protocol that contribute positively to the key rate. We can therefore define the post-selected key rate as

$$R_{\mathrm{PS}} = \int p(\mathbb{A}\mathbb{B}\gamma)\max\{\tilde{R}(\mathbb{A},\mathbb{B},\gamma),0\}\,\mathrm{d}\mathbb{A}\,\mathrm{d}\mathbb{B}\,\mathrm{d}\gamma\,. \tag{5.2.91}$$

The post-selected rate can also be thought of as the secret key rate over the region of the $\mathbb{A}$-$\mathbb{B}$-γ volume in which the single-point rate is positive, labeled Γ. Symbolically, this definition can be expressed as follows

$$R_{\mathrm{PS}} = \int_{\Gamma} p(\mathbb{A}\mathbb{B}\gamma)\tilde{R}(\mathbb{A},\mathbb{B},\gamma)\,\mathrm{d}\mathbb{A}\,\mathrm{d}\mathbb{B}\,\mathrm{d}\gamma\,. \tag{5.2.92}$$

5.2.6 Results

In this section, we will present a detailed analysis of our post-selected protocol. However, we must first recap the relations for the channel loss and protocol range. Firstly, the channel loss in dB is related to the transmissivity of the channel by $\tau = 10^{-\mathrm{dB}/10}$. We can also relate the transmissivity to the distance spanned by the channel, d as $\tau = 10^{-\delta d/10}$ where δ is the loss per unit distance. As we are exclusively considering fiber optic cables, a typical value of δ is 0.2 dB. There are cases in which this number is smaller, but we will take a worst-case scenario for the purposes of demonstrating the most realistic range of the protocol.

We use the excess noise to express the variances ω_A and ω_B in terms of the transmissivities of the channels. By considering each link to be a point-to-point channel we write

$$\omega_{A(B)} = 1 + \epsilon_{A(B)}\frac{\eta\tau_{A(B)}/2}{1-\eta\tau_{A(B)}/2}. \tag{5.2.93}$$

where $\epsilon_{A(B)}$ is the excess noise in the Alice-relay (Bob-relay) links.

Fig. 5.4 shows the total-distance between Alice and Bob, i.e. the sum of the lengths of both channels, as a function of the rates of all variations of the protocol in the symmetric configuration ($\tau_A = \tau_B$) and assuming a pure-loss attack ($\epsilon = \epsilon_A = \epsilon_B = 0$) with perfect detection efficiency. In all cases, we have optimized the rate over the variances σ_A and σ_B (σ_A and μ for restricted eavesdropping). For comparison, we have included the rate of the original Gaussian MDI protocol with equivalent parameters. Clearly, the range of the original protocol can be substantially increased in the case of restricted eavesdropping but a notable advantage also exists in the strongest eavesdropping scenario. It is possible that an achievable rate with complete eavesdropping may lie somewhere between the rates of the collective restricted eavesdropping rate and the complete eavesdropping rate, but the exact

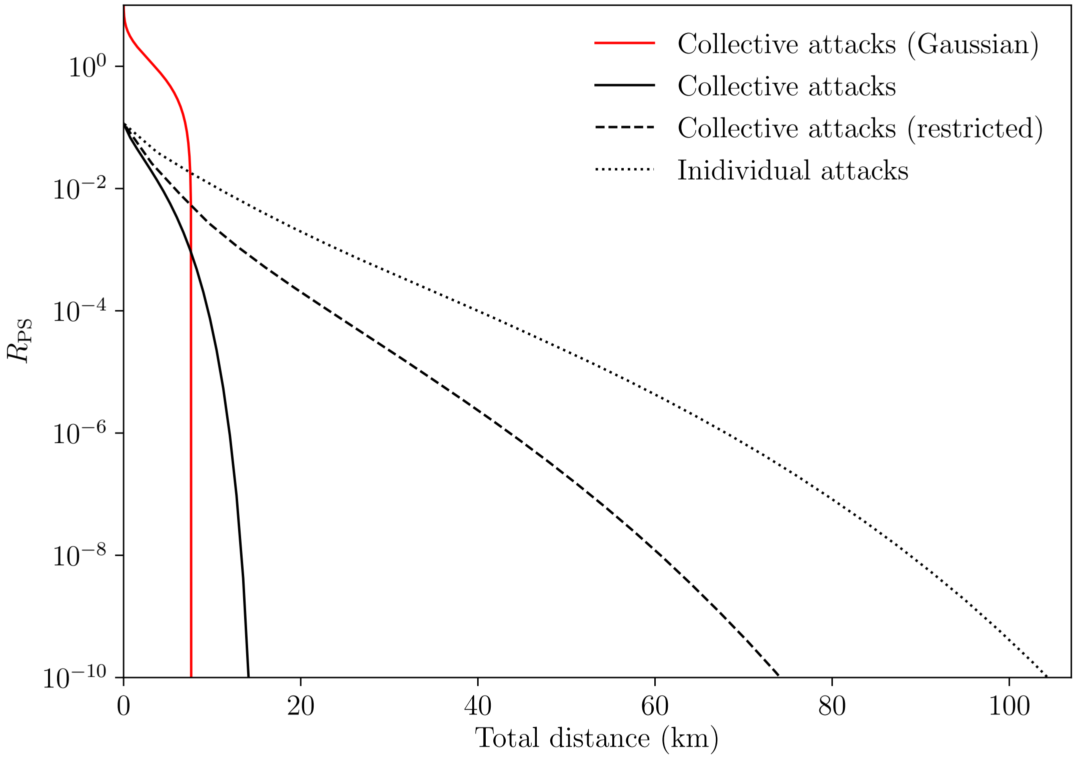

Figure 5.4: Rates of the pure-loss symmetric protocol as a function of the total distance between Alice and Bob with σ_A, σ_B and μ optimized. The red line represents the rate of the symmetric Gaussian MDI protocol.

curve remains a topic for future investigations.

In Fig. 5.5, we examine the rates of the symmetric protocol under complete eavesdropping in more detail. We include the rates under ideal parameters ($\eta = 1$, $\beta = 1$, and $\epsilon = 0$) as well as a realistic rate with excess noise $\epsilon = 0.05$, detector efficiency of 98% and reconciliation efficiency of 95%. Again, we also show the optimal rates of the Gaussian MDI protocol with identical parameters. Our protocol provides an advantage over the original MDI protocol under both ideal and realistic parameters, however, we note that the scale of the improvement reduces as we move closer to unfavorable parameters. In Fig. 5.6 we explore the asymmetric configuration of the protocol under complete eavesdropping. We see that our protocol offers the biggest advantage as the symmetry of the configuration increases. However, we still observe an advantage in the asymmetric regime up to very asymmetric configurations with less than 1 km separating Alice from the relay.

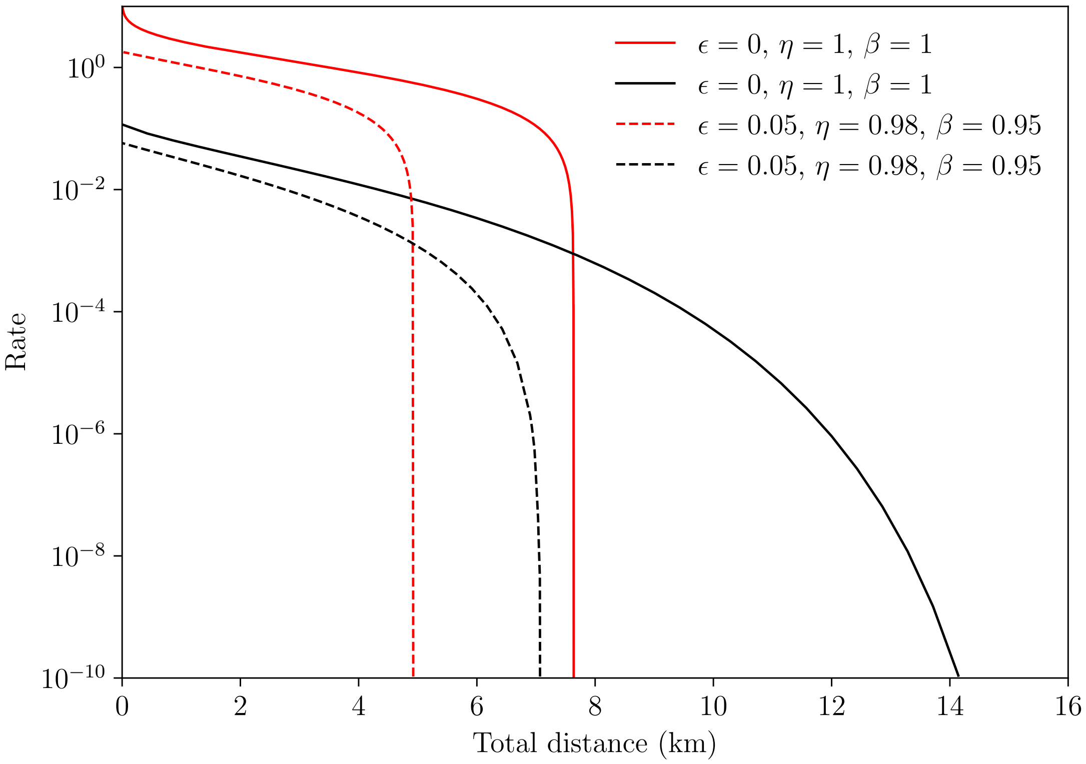

Figure 5.5: Rates of the symmetric protocol function of the total distance between Alice and Bob with σ_A and σ_B optimized (black lines). For comparison, we include the original Gaussian MDI protocol with optimal parameters (red lines). The solid lines correspond to the pure-loss protocols with ideal parameters $\eta = 1$ and $\beta = 1$, while the dashed lines correspond to a realistic scenario in which $\epsilon = 0.05$, $\eta = 0.98$ and $\beta = 0.95$.

To explore the effect of the realistic parameters in more detail, we consider in Fig. 5.7, for individual and collective attacks with restricted eavesdropping, the rates with $\epsilon = 0.05$, $\eta = 0.8$ and $\beta = 0.95$ that are typical experimental parameters [90], in the symmetric configuration. For each rate, we have incorporated η by scaling the transmissivities on each link. This has a considerable effect on the rate but a distance exceeding 60 km with collective attacks is still possible. We show in Fig. 5.8 the optimal values of the free parameters for the symmetric protocol with restricted eavesdropping under individual (top) and collective (bottom) attacks with the same parameters as those used for the rates in Fig. 5.7 between 10 and 20 km. The optimal values of μ are displayed with red lines while black lines correspond to optimal values of σ_A in units of the quantum vacuum variance, also known as

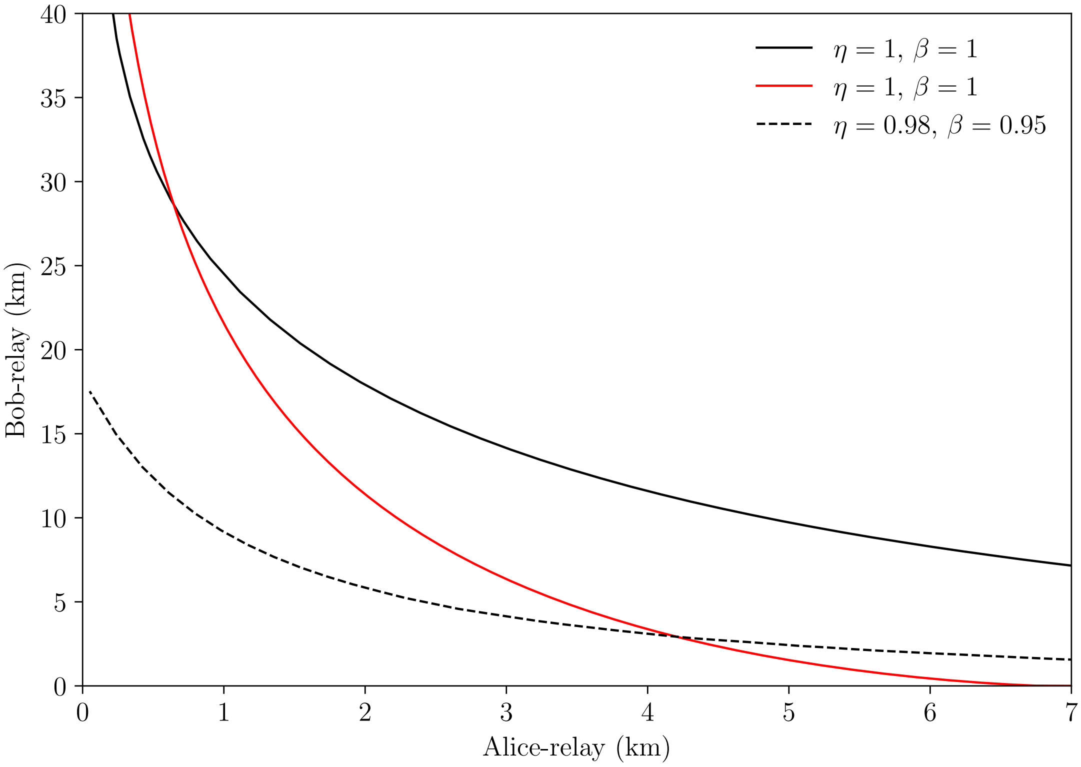

Figure 5.6: Comparison of the maximum Bob-relay distance as a function of the Alice-relay distance under complete eavesdropping. The black lines represent our protocol with the solid line corresponding to the pure-loss case with ideal parameters $\eta = 1$ and $\beta = 1$ and the dashed line corresponding to case with $\epsilon = 0.05$ and imperfect parameters $\eta = 0.98$ and $\beta = 0.95$. For comparison, the red line represents the pure-loss Gaussian MDI protocol with ideal parameters.

shot-noise units (SNU). We note that the optimal parameters are small relative to the original Gaussian MDI protocol in which the optimal value of μ tends to infinity for perfect reconciliation efficiency.

5.3 Conclusions

In this chapter, we have introduced a long-distance CV-MDI-QKD protocol with a general mathematical formulation with collective attacks that may include excess noise and experimental inefficiencies. We have demonstrated that our protocol exceeds the range of the original Gaussian CV-MDI-QKD protocol in both symmetric and asymmetric configurations. This improvement exists in the strongest eavesdrop-

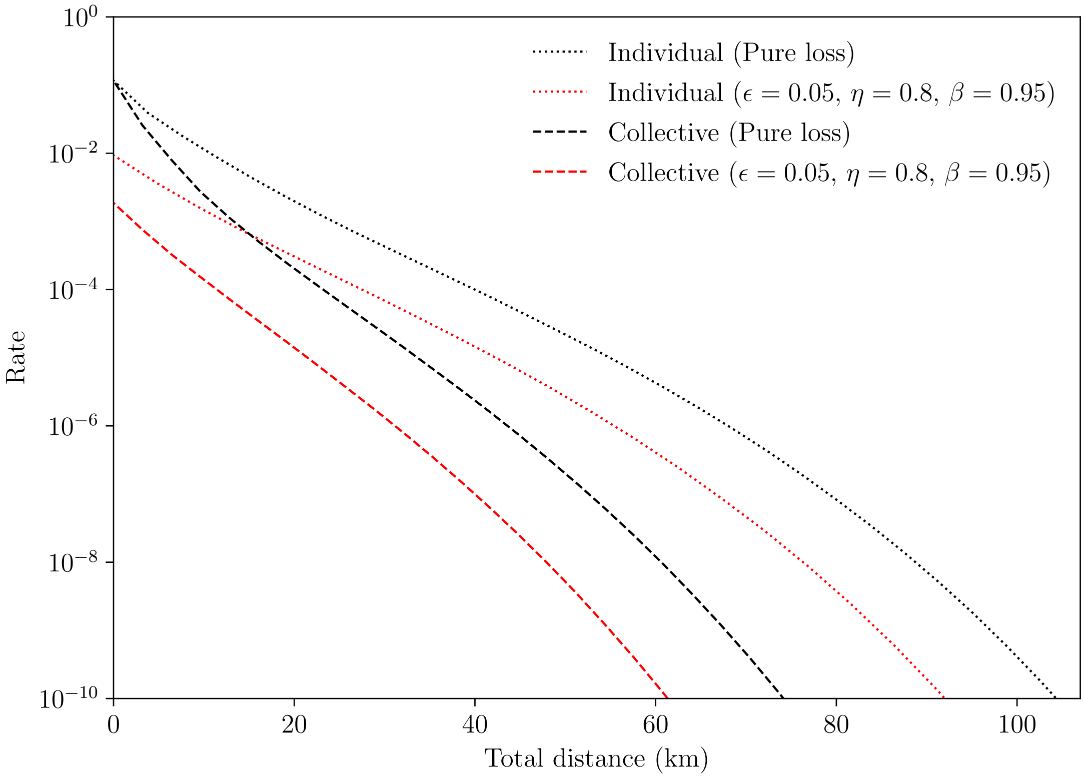

Figure 5.7: Rates of the symmetric protocol with restricted eavesdropping as a function of the total distance between Alice and Bob with σ_A and μ optimized. The black lines correspond to the pure-loss case with perfect detection and reconciliation while the red lines represent the rate with parameters $\epsilon = 0.05$, $\eta = 0.8$, and $\beta = 0.95$.

ping scenario and is substantially increased to distances exceeding 50 km if restricted eavesdropping is considered with either individual or collective attacks. In future work, it would be beneficial to explore the possibility of a fully-secure rate between these extremes if Bob is able to communicate all of the necessary information to Alice without broadcasting the absolute value of his measurement in each use of the protocol.

Our protocol is robust against excess noise as well as detection and reconciliation inefficiencies and it is, therefore, a significant step towards a realistic experimental implementation. We have demonstrated that CV-MDI QKD need not be restricted to short distances. In fact, our protocol provides a theoretical foundation for MDI-QKD at distances previously only achievable with discrete variable

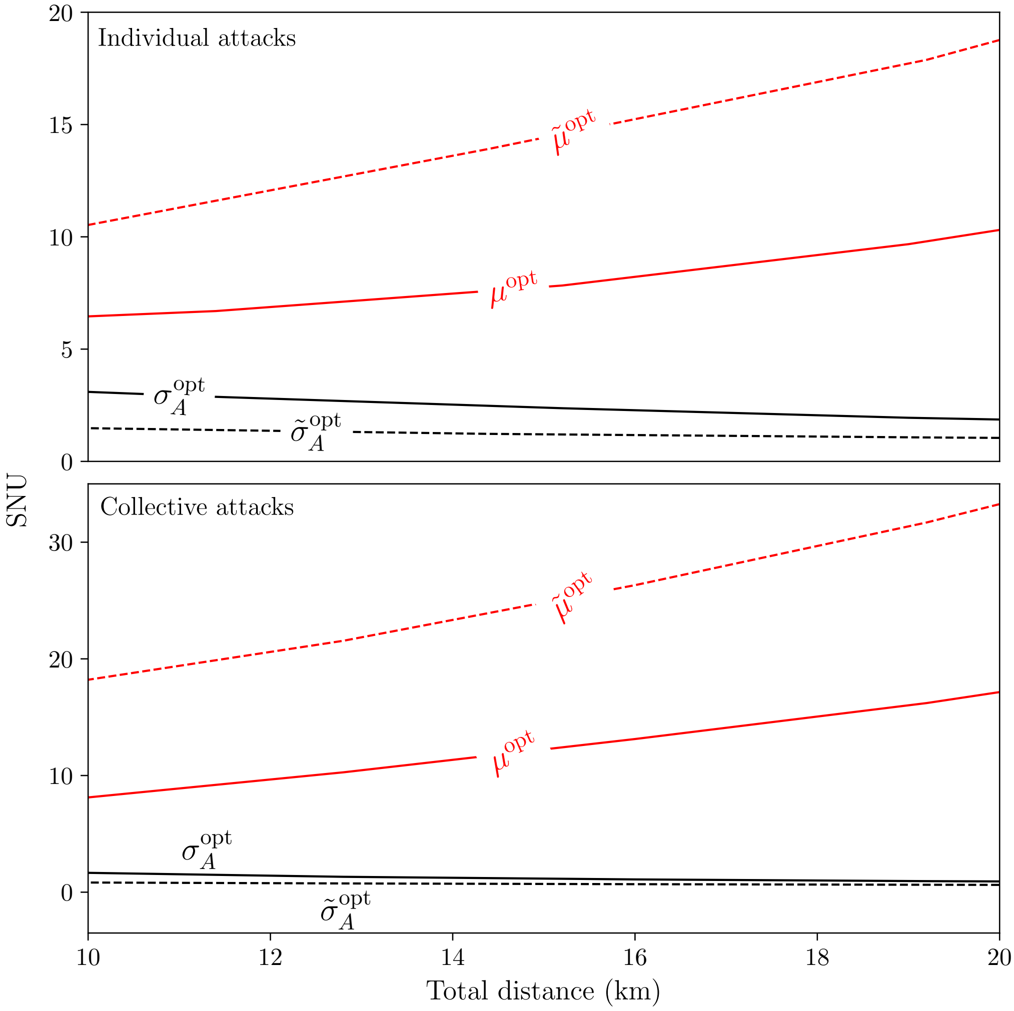

Figure 5.8: Optimal values of μ (red lines) and σ_A (black lines) in short-noise units (SNU) for the symmetric protocol with restricted eavesdropping under individual (top panel) and collective (bottom panel) attacks. The solid lines represent the optimal parameters for the pure-loss case with ideal detection efficiency and the dashed lines represent the optimal values under parameters $\epsilon = 0.05$, $\eta = 0.8$ and $\beta = 0.95$.

protocols, achievable with inexpensive and easily implementable equipment.

Despite the rate-distance improvements offered by our protocol, increasing the range further remains a difficult task. One interesting extension of the CV-MDI technology is a generalization to a multipartite configuration in which many users communicate with a central relay controlled by an eavesdropper, enabling quantum conferencing or quantum secret sharing between the parties [91]. Recently, this architecture has been proposed as a building block for a scalable modular quantum network that may provide a path towards long-distance CV-MDI QKD [92]. An interesting avenue for future work would be to implement post-selection into the multivariate CV-MDI architecture to extend its range in anticipation of larger network implementations in the future.

Chapter 6

Analysis of quantum versus classical networking in butterfly-based networks

In this chapter, we will reach the end of our journey from points to nodes. Our focus will be directed at one of the major hurdles ahead in the path towards widespread quantum networking, which is the lack of clarity regarding the performance of quantum networks built on top of or using classical network infrastructure. We will consider the well-known butterfly network and the problem of network coding, which is trivially implemented with the benefits of classical networking, but somewhat more complex in its quantum counterpart.

The characteristic feature of the butterfly network as shown in Fig. 6.1 is the bottleneck point at the node R_1. Let us consider a communication problem between the senders A_1 and A_2 and the receivers B_1 and B_2. We can assume that each sender wishes to send a single message to both receivers, known as a single-message multicast. We will also assume a flooding protocol is in place, which means each channel in the network can be used exactly once. Upon first glance, it would appear that it isn't possible for both parties to successfully perform multicasts due to the bottleneck at R_1 where data can be sent to R_2 from *either* A_1 or A_2. In 2002, a solution to this problem was proposed by R. Ahlswede et al. in the form of network coding [29]. As outlined in Fig. 6.1, network coding in the butterfly network consists

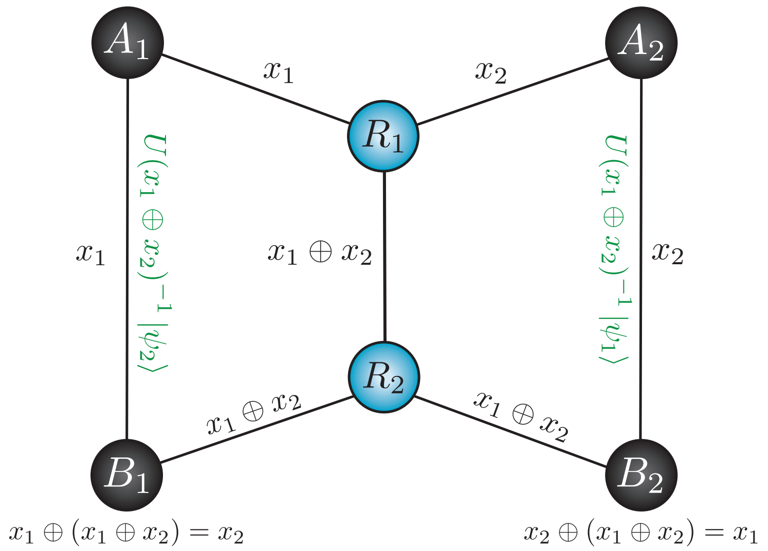
A_1
A_2
R_1
R_2
B_1
B_2
x_1
x_2
x_1
$x_1 \oplus x_2$
x_2
$U(x_1 \oplus x_2)^{-1} |\psi_2\rangle$
$U(x_1 \oplus x_2)^{-1} |\psi_1\rangle$
$x_1 \oplus x_2$
$x_1 \oplus x_2$
$x_1 \oplus (x_1 \oplus x_2) = x_2$
$x_2 \oplus (x_1 \oplus x_2) = x_1$

Figure 6.1: A schematic of the butterfly network with two senders, A_1 and A_2, a bottleneck channel with bottleneck nodes R_1 and R_2, and two receivers, B_1 and B_2. The bits transmitted according to the Ahlswede classical network coding protocol are labelled on each channel. Network coding is achieved using modulo-2 addition for encoding at R_1 and for decoding B_1 and B_2 after duplication of the encoded bit at R_2. Also highlighted in green are the states sent via the side channels in a scheme for QNC introduced by M. Hayashi based on teleportation using the resource of prior entanglement shared between the two senders.

of encoding data using a modulo-2 addition operation at the bottleneck node R_1 before sending the encoded bit through the bottleneck channel to R_2 where it is duplicated and sent to each receiver. Receiver $B_{1(2)}$ decodes the data received from R_2 using modulo-2 addition with data received from their directly-connected sender $A_{1(2)}$. This simple strategy proved groundbreaking in network theory and the field of network coding is still of great importance in modern research.

Given the success of network coding in classical networks, an important question we must ask: is can this success be replicated in the quantum setting? More specifically, can the bits in classical network coding be replaced with qubits to achieve quantum network coding (QNC) with the same high data rate per use of the network? It is apparent that quantum network coding cannot be achieved in parallel with its classical counterpart due to the no-cloning theorem [93]. Hayashi et al. [94]

confirmed that no quantum process achieves perfect QNC (i.e. with unit fidelity) while demonstrating that approximate quantum network coding can be achieved for qubits using a "universal quantum copying machine" [95] with a fidelity greater than 1/2 but no more than 0.983. In addition, Ref. [96] provided an information-theoretic proof that quantum network coding does not provide a larger information flow than routing in the butterfly network.

Clearly then, perfect QNC demands some out-of-the-box thinking. A possible solution is to assume the presence of additional resources available to nodes in the network. One protocol proposed in 2007 by M. Hayashi et al. [97] makes use of prior entanglement between the two senders in the butterfly network to achieve QNC with a strategy based on quantum teleportation. This protocol is also depicted in Fig. 6.1 with the states required to be sent via the side channels highlighted in green. Senders A_1 and A_2 share two pairs of maximally entangled Bell states. The first pair has two sites, $A_{1,1}$, $A_{2,1}$ and second pair has two sites, $A_{1,2}$ and $A_{2,2}$. The state prepared by sender A_i is denoted $|\psi_i\rangle$. The protocol can be summarised in four steps as follows:

1. Sender A_i performs a Bell measurement on the joint system $A_i \otimes A_{i,i}$ and obtains data x_i. The state of the remaining site $A_{i,i\oplus 1}$ is
$$U(x_{i\oplus 1})^{-1} |\psi_{i\oplus 1}\rangle , \tag{6.0.1}$$
where $U(x)$ is the teleportation unitary associated with the outcome x of the Bell detection.

2. A_i performs the unitary operation $U(x_i)^{-1}$ on the remaining site $A_{i,i\oplus 1}$, hence the state of the system $A_{i,i\oplus 1}$ becomes
$$U(x_i)^{-1}U(x_{i\oplus 1})^{-1} |\psi_{i\oplus 1}\rangle = c(x_i, x_{i\oplus 1})U(x_1 \oplus x_2)^{-1} |\psi_{i\oplus 1}\rangle \tag{6.0.2}$$
where $c(x_i, x_{i\oplus 1})$ is a constant with $|c(x_i, x_{i\oplus 1})| = 1$. A_i sends the system $A_{i,i\oplus 1}$ to B_i via the channel that directly connects the two nodes. A_i also sends the classical information x_i to R_1.

3. R_1 sends the classical information $x_1 \oplus x_2$ to R_2, where it is duplicated and sent to B_1 and B_2 as in the classical case.

4. B_i performs the unitary operation $U(x_1 \oplus x_2)$ to the received state $U(x_1 \oplus x_2)^{-1} |\psi_i\rangle$. The original state is then recovered as

$$U(x_1 \oplus x_2)U(x_1 \oplus x_2)^{-1} |\psi_i\rangle = |\psi_i\rangle . \tag{6.0.3}$$

This relatively straightforward protocol demonstrates a perfect QNC scheme possible due to the presence of prior entanglement between senders. This protocol has recently been verified experimentally [98] and several other studies make use of prior entanglement in the butterfly network to achieve the same goal [99–101]. Alternatively, Ref. [102] has shown that transfer of quantum states by quantum network coding is possible in the absence of prior entanglement by enabling free classical communication between nodes and several other investigations have considered a free-classical-communication regime [103–105]. While these schemes provide answers to the question of perfect QNC, the requirement of prior entanglement and/or classical communication between nodes makes them suboptimal solutions in many applications and highlights the non-trivial limitations of extending network coding to the quantum regime.

In the context of QNC in realistic networks, one must consider the general case in which multicasts from senders to receivers are only partially achieved. This is particularly important if we replace the perfect quantum channels considered thus far with noisy channels in which successful transmission is not guaranteed. We may, therefore, associate an average rate to each sender which accounts for the fact that sometimes only a subset of the receivers is reached. This rate describes the average number of bits per receiver that are transmitted in each network multicast. In this chapter, we will perform a detailed analysis of the rates of the butterfly network constructed with identity, depolarizing, and erasure channels. We will deviate from the existing literature in that our objective will be to quantify the rates in a quantum communication setting in which quantum systems are physically sent through quantum channels, rather than a quantum information processing setting in which quantum states are simply transferred or reconstructed. By applying the techniques introduced in Sec. 2.6, namely LOCC simulation and teleportation stretching, we can upper-bound the highest quantum communication rates achievable in a multicast assisted by adaptive local operations and two-way classical communication involving all the nodes of the network. We then compare these bounds with the corresponding rates that can be achieved for multicasts of classical information from senders to receivers, establishing parameter regimes where classical outperforms quantum communication.

The techniques introduced in Sec. 2.6 allow us to extend our analysis to a class of networks that are constructed with butterfly network blocks, for which we find that the performance gap between the classical and quantum regimes is more pronounced. To our knowledge, these network structures have not been considered previously in the literature. Our results allow us to illuminate the non-trivial limitations that certain network architectures have for transmitting quantum information.

6.1 Rates of a single butterfly block

Let us now proceed with our analysis of the butterfly network starting with the computation of the rates of a single butterfly block. Firstly, we must recall the bound introduced in Sec. 2.6.4 for the capacity of a network of an ensemble of senders $\{A_i\}$ and receivers $\{B_i\}$,

$$\mathcal{B}(\mathcal{N}) := \min_{C:\{A_i\}|\{B_j\}} \sum_{(x,y)\in\tilde{C}} E_R(\hat{\sigma}_{\mathcal{E}_{xy}}), \tag{6.1.4}$$

where $C : \{A_i\}|\{B_j\}$ represents a network cut that separates the ensemble of senders from the ensemble of receivers. In analogy to the classical networking case, we are interested in single-message multiple multicasts, where, in each use of the network, each sender aims to send the same bit to each receiver. The quantum state that describes this framework most accurately is the GHZ-like multipartite logical qubit $\alpha|\bar{0}\rangle + \beta|\bar{1}\rangle$ which is encoded into as many physical qubits as there are receivers, i.e. $|\bar{0}\rangle = |0...0\rangle$ and $|\bar{1}\rangle = |1...1\rangle$. In this context, the total number of logical qubits that are correctly received by the destination set is equal to the total number of physical qubits correctly received by each receiver, which means that we need to divide the bound in Eq. (6.1.4) by the number of receivers r. Therefore our figure of merit is the total number of qubits per use and receiver, which is less than or equal to the quantum bound

$$R_Q(\mathcal{N}) := r^{-1} \min_{C:\{A_i\}|\{B_j\}} \sum_{(x,y)\in\tilde{C}} E_R(\hat{\sigma}_{\mathcal{E}_{xy}}). \tag{6.1.5}$$

By examining Fig. 6.1, we can immediately see that the minimum cut that separates the senders from the receivers in the butterfly network is horizontally through the middle of the network, disconnecting the edges (A_1, B_1), (R_1, R_2), and (A_2, B_2). Using Eq. (6.1.5), we obtain an upper bound of three physical qubits to be divided by $r = 2$ receivers or 1.5 qubits per use and receiver. By contrast, we know from network coding theory that, in the classical case, we can obtain two classical bits per use and receiver; hence we have a difference of 0.5 bits per use and receiver between the quantum and classical networks in this case.

A more interesting application of our general bound is in the examination of the butterfly network constructed with noisy channels. Let us start by considering the depolarizing channel whose action in d dimensions on an arbitrary density matrix $\hat{\rho}$ can be expressed as

$$\mathcal{P}_{\text{depol}}(\hat{\rho}) = (1-p)\hat{\rho} + p\frac{\mathbf{I}}{d}, \tag{6.1.6}$$

where $\mathbf{I}$ is the identity matrix. The output of the channel is the maximally mixed state $\mathbf{I}/d$ with probability p, known as the depolarizing probability, or the input state $\hat{\rho}$ with probability $1-p$. In the case of qubits, the action of the depolarizing channel can be thought of as shrinking the Bloch sphere [8]. At the time of writing, the exact two-way quantum capacity of the depolarizing channel is unknown, however, Ref. [20] obtained an upper bound of

$$Q_2(p) \leq E_R(\hat{\sigma}_{\mathcal{P}_{\text{depol}}}) = 1 - H_2\left(1 - \frac{3p}{4}\right) \tag{6.1.7}$$

for $p \leq 2/3$ with $Q_2 = 0$ otherwise, where $H_2(p) = -p\log_2 p - (1-p)\log_2(1-p)$ is the binary Shannon entropy. Applying the bound with the same network cut, we can write the rate per use and receiver of a butterfly network $\mathcal{B}_{\text{dep}}$ connected by depolarizing channels with equal probability p, of

$$R_Q(\mathcal{B}_{\text{dep}}) = \frac{3}{2}\left[1 - H_2\left(1 - \frac{3p}{4}\right)\right]. \tag{6.1.8}$$

The unassisted classical capacity of the quantum depolarizing channel is given by [106]

$$C(p) = 1 - H_2\left(1 - \frac{p}{2}\right). \tag{6.1.9}$$

This result can be better understood by propagating an encoded classical bit through the channel. For the input $|0\rangle\langle 0|$, we obtain

$$\begin{aligned}\mathcal{P}(|0\rangle\langle 0|) &= (1-p)|0\rangle\langle 0| + \frac{p}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)\\ &= \left(1 - \frac{p}{2}\right)|0\rangle\langle 0| + \frac{p}{2}|1\rangle\langle 1|,\end{aligned} \tag{6.1.10}$$

and similarly for $|1\rangle\langle 1|$ we have

$$\mathcal{P}(|1\rangle\langle 1|) = \left(1 - \frac{p}{2}\right)|1\rangle\langle 1| + \frac{p}{2}|0\rangle\langle 0|. \tag{6.1.11}$$

Examination of equations (6.1.10) and (6.1.11) reveals that the channel behaves as a classical binary symmetric channel (BSC) with bit flip probability $p/2$. We can use this equivalency to establish the rates of the butterfly network constructed with identical depolarizing channels.

To compute an achievable rate for the classical single-message multiple multicast over a depolarizing butterfly network, we deconstruct the network into two channels $A_1, A_2 \to B_1$ and $A_1, A_2 \to B_2$. Calculating the total rate of the combined channels gives an achievable rate for the network. The general procedure for this process is to create the transition probability matrix using the logic of the butterfly network, followed by an optimization over a distribution on the input symbol. The upper panel of Fig. 6.2 shows both the quantum bound R_Q (qubits per per use and receiver) and the achievable rate R_C for sending classical information (bits per use and receiver). The quantum bound is exceeded by the classical rate over the entire range of p with the maximum difference being 0.5 bits per receiver (which corresponds to the ideal example of identity channels discussed above).

Let us now move on to erasure channels. From classical information theory, we know that the capacity of the binary erasure channel with erasure probability ϵ is given by $C(\epsilon) = 1 - \epsilon$. This formula has also been shown to be equal to the classical capacity of the quantum erasure channel [107]. The same work found the quantum capacity to be $Q(\epsilon) = \max\{0, 1 - 2\epsilon\}$ and also $C(\epsilon) = Q_2(\epsilon) = 1 - \epsilon$. The erasure

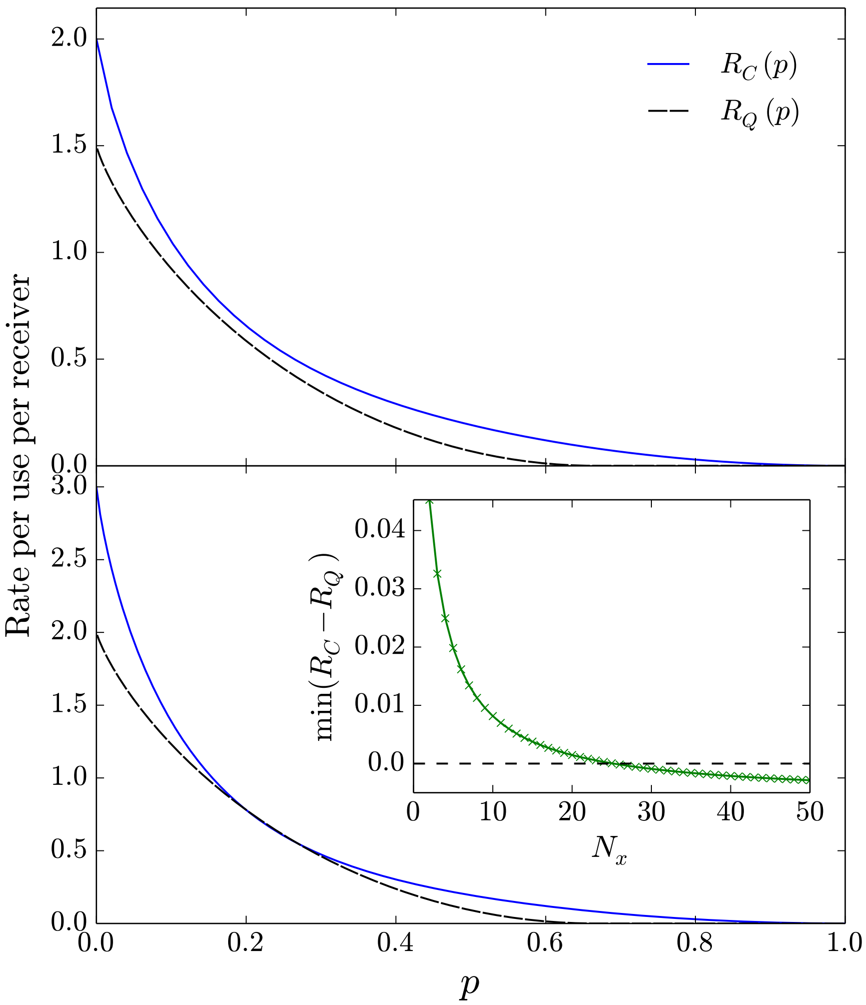

Figure 6.2: Rates (bits/qubits) per use and receiver as a function of the depolarizing probability p considering a single butterfly block (upper panel) and the limit of $N_x \to \infty$ blocks in parallel (lower panel). We plot the achievable classical rate R_C (solid blue line) and the quantum bound R_Q (dashed black line). Inset: the minimum difference between the classical rate and the quantum bound as a function of N_x (where the minimization is taken over the probabilities).

channel is unique in that the number of correctly transmitted bits is known with certainty so that the capacity is equivalent to the average number of transmitted bits. For any network, it is straightforward to calculate the achievable classical rate. For a single butterfly network block $\mathcal{B}_{\text{era}}$ connected by erasure channels with the same probability, we obtain the classical rate (per use and receiver)

$$R_C(\mathcal{B}_{\text{era}}) = (1-\epsilon) + (1-\epsilon)^5, \tag{6.1.12}$$

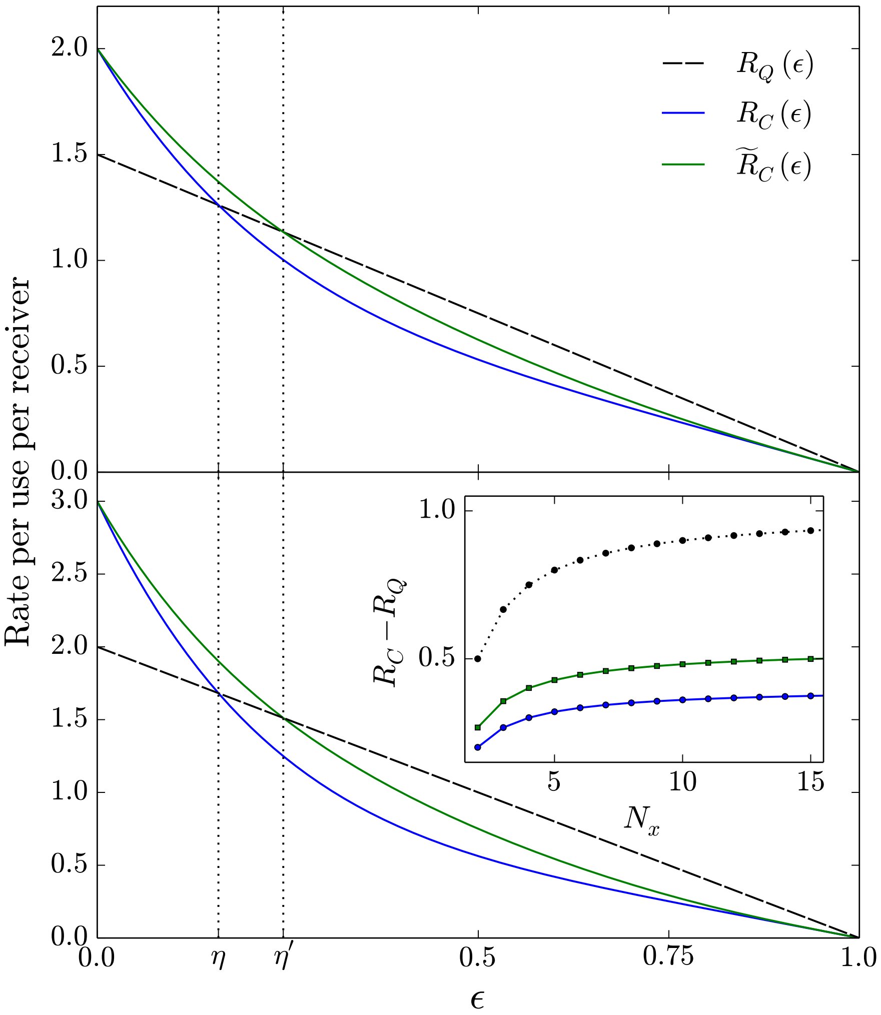

Figure 6.3: Rates (bits/qubits) per use and receiver as a function of the erasure probability ϵ, considering a single butterfly block (upper panel) and the limit of $N_x \to \infty$ blocks in parallel (lower panel). We plot the quantum bound R_Q (dashed black line), the achievable classical rate, R_C (solid blue line), and the inter-node-assisted achievable classical rate $\tilde{R}_C$ (solid green line). The values η and η' are the critical points at which R_C and $\tilde{R}_C$, respectively cross the quantum bound R_Q. Inset: Difference between $\tilde{R}_C$ and R_Q as a function of N_x for values of erasure probability equal to 0 (black line), and $\eta'/2$ (green line), and the difference between R_C and R_Q as a function of N_x for erasure probability equal to $\eta/2$ (blue line).

where the first term arises from the contribution of the side channels and the second comes from network coding at the bottleneck node.

Allowing side one-way classical communication between nodes in the network allows for the optimization of the transmission routes, increasing the rate. For example, if we detect a failure in a channel connected to the bottleneck node, (A_i, R_1), we send any correct data received at R_1 directly to R_2 and subsequently to both receivers. We then have additional communication paths from A_j to B_i and B_j. The inter-node-assisted rate (per use and receiver) is given by

$$\tilde{R}_C(\mathcal{B}_{\text{era}}) = (1-\epsilon) + (1-\epsilon)^5 + \epsilon(1+\epsilon)(1-\epsilon)^3. \tag{6.1.13}$$

The upper panel of Fig. 6.3 shows each of the rates for a single butterfly block. For both R_C and $\tilde{R}_C$, we observe a region where the quantum bound R_Q is exceeded. We label the crossing points $\eta = 0.159$ and $\eta' = 0.244$ for R_C and $\tilde{R}_C$, respectively. The advantage of inter-node classical communications is significant and extends the performance difference between the classical and quantum butterfly network in this configuration.

6.2 Building networks with butterfly blocks

We will now expand our analysis to larger networks constructed with butterfly network blocks as shown in Fig. 6.4. We consider adding blocks in parallel in Sec. 6.2.1, in series in Sec. 6.2.2 and in both series and parallel in Sec. 6.2.3.

6.2.1 Butterfly blocks connected in parallel

By connecting N_x butterfly network blocks in parallel, i.e. in a single row, we create a larger network $\mathcal{N}_{\text{par}}$ with $r = N_x + 1$ senders/receivers. Happily, we can easily extend the previous reasoning to evaluate the maximum number of multipartite logical qubits that can be transmitted from senders to receivers in a flooding protocol per use of the network. The optimal network cut in this case is the one that passes through the horizontal center of the network such that $2r - 1$ channels are disconnected. For the depolarizing case, therefore, we obtain the general quantum bound

$$R_Q = \frac{2r-1}{r}\left[1 - H_2\left(\frac{3p}{4}\right)\right], \tag{6.2.14}$$

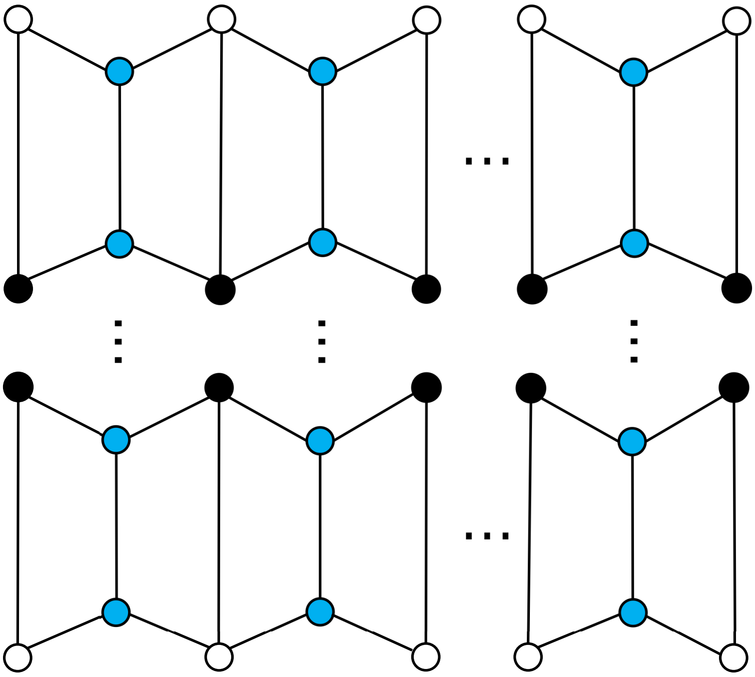

Figure 6.4: Diagram of the construction of larger networks from butterfly network blocks in parallel (horizontal) and series (vertical).

while for the erasure case, we can write

$$R_Q = \frac{2r-1}{r}(1-\epsilon). \tag{6.2.15}$$

The achievable classical rate of the depolarizing network can be found by expanding the methods used in the case of a single butterfly block. The network can be deconstructed into two channels of the form $A_i, A_{i+1} \rightarrow B_i$ at the ends, and $(N_x - 1)$ channels of the form $A_i, A_{i+1}, A_{i+2} \rightarrow B_{i+1}$ in the middle. We find the overall rate numerically from the combination of the capacities of all channels, from which we can compute the rate per user and receiver, R_C. The lower panel of Fig. 6.2 shows the rates of the depolarizing case in the limit of large r for the entire range of probabilities. The asymptotic rates are approximately identical at 0.2 but the classical case outperforms the quantum bound everywhere else in the range.

For a network of identical erasure channels, this process of finding the classical rates is far more straightforward and we can directly write the following unassisted rate per user and receiver

$$R_C = (1-\epsilon) + 2\frac{(r-1)}{r}(1-\epsilon)^5. \tag{6.2.16}$$

Here the first term on the right-hand side is due to the fact that all receivers may receive a single bit from their directly connected sender, while the second term accounts for the fact that all receivers, except those at the edges of the network, B_1 and B_r, may receive two bits from successful network coding on the adjacent intermediate nodes. In the case of free inter-node classical communication, the rate can be adapted by considering the additional 'backup' communication routes in each block in addition to the unassisted rate in Eq. (6.2.16), giving an overall rate per user and receiver of

$$\tilde{R}_C = (1-\epsilon) + \frac{2(r-1)}{r}\big[(1-\epsilon)^5 + \epsilon(1+\epsilon)(1-\epsilon)^3\big]. \tag{6.2.17}$$

Using these bounds, we see immediately for the erasure network that the difference between the average number of bits/qubits grows monotonically as we increase the number of butterfly blocks. Taking the limit of large r, we obtain

$$\lim_{r\to\infty} R_Q = 2(1-\epsilon) \tag{6.2.18}$$

$$\lim_{r\to\infty} R_C = (1-\epsilon) + 2(1-\epsilon)^5 \tag{6.2.19}$$

$$\lim_{r\to\infty} \tilde{R}_C = (1-\epsilon) + 2(1-\epsilon)^5 + 2\epsilon(1+\epsilon)(1-\epsilon)^3. \tag{6.2.20}$$

The lower panel of Fig. 6.3 shows the asymptotic rates for the erasure case. We find that η and η' are independent of N_x. At small values of the erasure probability ϵ, the gap between the rates converges to one bit per use per receiver as the channels become free of noise.

6.2.2 Butterfly blocks connected in series

We now consider the rates of a network $\mathcal{N}_{\text{ser}}$ consisting of N_y butterfly network blocks connected in series i.e. in a ladder formation. The number of receivers is always the same ($r = 2$), and the number of intermediate nodes and channels now varies. The addition of extra blocks has the effect of reducing the rates, as it becomes harder to reach a receiver without incurring errors. The quantum capacity of the network $\mathcal{N}_{\text{ser}}$ is independent of N_y as the optimal cut is any that passes through the center of any of the butterfly blocks, which always disconnects three quantum channels.

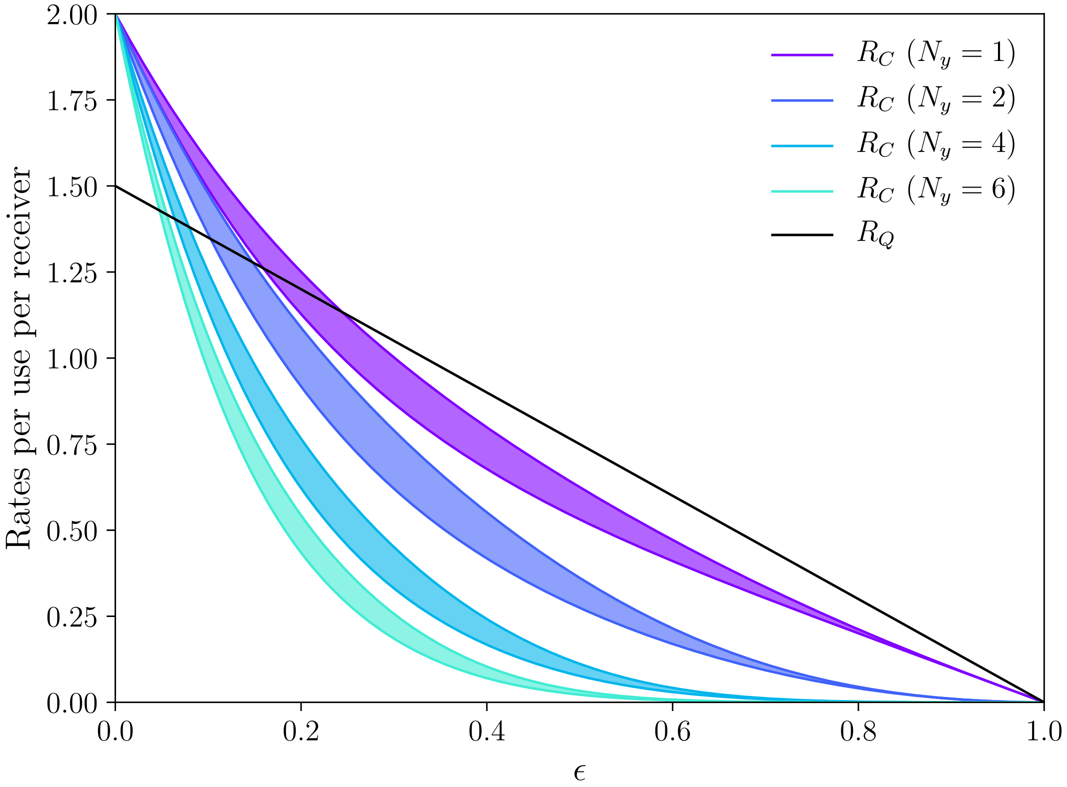

Figure 6.5: Classical rate (lower lines) and inter-node CC assisted classical rate (upper lines) per receiver for a $1 \times N_y$ butterfly block network constructed with erasure channels. Comparison with the quantum bound (solid black line).

For the depolarizing case, adding blocks in a ladder structure is equivalent to adding only extra side channels above a single block as the information arriving at the intermediate nodes cannot be checked for errors. In the erasure case, however, extra bottlenecks can be used effectively, even if there are no additional communications. If we allow the nodes to duplicate data, we can use the bottleneck channels as effective backup channels in case of errors and perform network coding *only* in the final bottleneck before the receivers.

For simplicity, we will explicitly consider only two blocks in series. In the upper block, we send data via the side channels to the intermediate nodes. Additionally, a bit from A_1 to the intermediate node on A_1's side of the network, which we briefly label I_1, via the channel $R_1 \to R_2$. Now I_1 has a greater probability of receiving the correct bit, and, because there are no additional operations, no communication between nodes is required. We can calculate the probability that a correct bit is received as

$$\lambda = 1 - p(\text{fail}) = 1 - \epsilon[1 - (1-\epsilon)^3], \tag{6.2.21}$$

where $p(\text{fail})$ is the probability that the bit is not received correctly. The classical rate (per use and receiver) is therefore given by

$$R_C = \frac{(1-\epsilon)\lambda + (1-\epsilon)^2}{2} + (1-\epsilon)^6\lambda. \tag{6.2.22}$$

This strategy can be extended to any number of blocks in series, where a backup channel can be applied once per block. Sender/intermediate nodes on either side of the network can use the bottleneck route, however, for more than two blocks the rate is maximized when the routes are always used by nodes on the same side of the network. The previous classical rate can, therefore, be generalized as

$$R_C = \frac{(1-\epsilon)\lambda^{N_y-1} + (1-\epsilon)^{N_y}}{2} + (1-\epsilon)^5(1-\epsilon)^{N_y-1}\lambda^{N_y-1}. \tag{6.2.23}$$

If we allow inter-node communication, the classical rate of a $1 \times N_y$ erasure network is obtained by considering all of the possible paths from sender to receiver, while prioritizing the backup route in upper blocks and accounting for possible channel failures. The classical rates for the $1 \times N_y$ network are shown in Fig. 6.5 and compared with the quantum bound R_Q which does not depend on N_y. The value of the crossing point η' decreases rapidly as N_y increases, but there is still a significant gap between the upper bound on the quantum rate and the achievable classical rate.

6.2.3 Butterfly blocks connected in series and parallel

Finally, we come to the most complex case in which we consider a general $N_x \times N_y$ grid of butterfly network blocks. This means that we have $r = N_x + 1$ receivers. Again, we calculate the classical rates of the erasure network, accounting for how the additional bottlenecks may be exploited. By allowing each sender (excluding the one at the right edge of the network) to use the backup route to its right in $(N_y - 1)$ upper blocks, we obtain the following unassisted classical rate (per use and receiver) for a general grid

$$R_C = \frac{1}{N_x+1}\{N_x(1-\epsilon)\lambda^{N_y-1} + (1-\epsilon)^{N_y} + 2(N_x-1)(1-\epsilon)^5\lambda^{2(N_x-1)} + 2(1-\epsilon)^5(1-\epsilon)^{N_y-1}\lambda^{N_y-1}\}. \tag{6.2.24}$$

For the inter-node assisted rate, we repeat the strategy of the series-only case and obtain values of η' for different configurations. The top panel of Fig. 6.6 shows the relative increase in the critical point η' with respect to the series-only case. The increase is significant and increases with the number of blocks we have in series. The lower panel shows η' as a function of N_y. The point η' decreases rapidly as we increase the number of blocks between the sender and the receiver, however, the results show that we always have a finite range over which the classical rate exceeds the quantum bound. These results demonstrate that by adding more blocks in parallel we can increase η' up to a convergence point, increasing by more than 60% in some cases.

6.3 Conclusions

Our analysis of the butterfly network has revealed an important discrepancy between quantum and classical communication rates under single-message multiple multicasts. We have demonstrated that this discrepancy can be monotonically increased by adding butterfly blocks in parallel, up to an asymptotic value of one bit/qubit per use and receiver for networks constructed using ideal channels.

By exploiting inter-node classical communication in erasure networks, we have shown that the discrepancy is increased more rapidly due to the increased number of routing paths that can be employed to facilitate the communication of classical data. Additionally, in this case, we observe a notable discrepancy even when we add blocks in series and the number of butterfly blocks separating senders from receivers is large. By adding further blocks in series and parallel, we can increase the value of the critical point, at which the classical rate exceeds the quantum bound, by more than 60%.

Our results demonstrate that duplicating certain existing classical network struc-

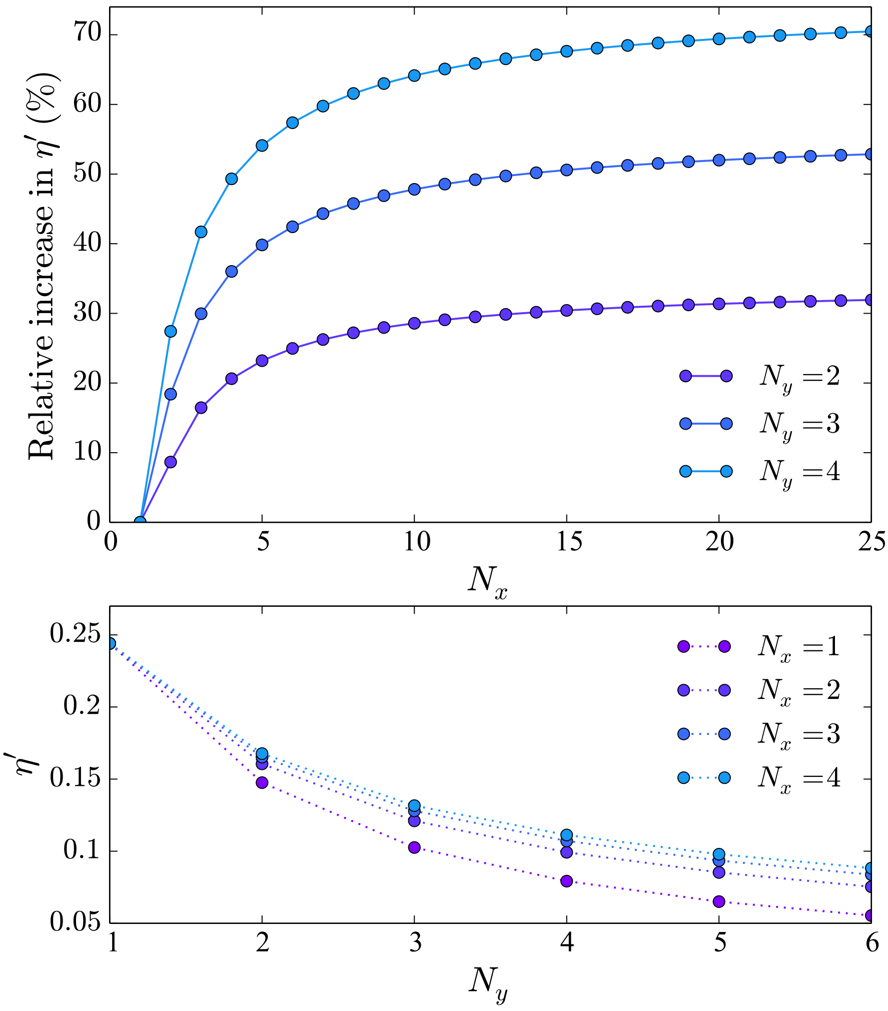

Figure 6.6: Upper panel: relative increase in the critical point η' as compared to the $N_x = 1$ case for various values of N_y. Lower panel: variation of η' with N_y for various values of N_x.

tures containing butterfly blocks in order to build quantum counterparts can result in significantly reduced performance. It may be possible to exploit this performance discrepancy to create a system in which quantum communication cannot beat a classical equivalent. In this sense, our results provide a theoretical guide with which to engineer such a system.

Chapter 7

Conclusions and future directions

In this thesis, we have addressed two of the most prominent issues facing the field of quantum information theory: the need for a long-distance QKD protocol that alleviates the security risks quantum supremacy poses to classical cryptography, and the need for a more complete understanding of the performance of quantum networking on classical network infrastructure.

We have introduced two original continuous-variable quantum key distribution protocols that employ the technique of post-selection. We have demonstrated that our protocols achieve a range that exceeds that of the equivalent protocols in the literature for both QKD at terahertz frequencies and CV-MDI QKD with coherent states. Our results add value to the field of CV QKD as a means of provably secure communications that can, in theory, be brought to fruition in a very short timescale due to the simplicity of the hardware implementation. In the particular case of MDI QKD, our protocol can be implemented with coherent states of light that can easily be generated in the laboratory. By providing a regime that increases the range of CV-MDI QKD, we have started to bridge the gap between the continuous- and discrete-variable regimes.

With the introduction of our one-way protocol at terahertz frequencies, we have provided a significant improvement in the achievable range under atmospheric conditions compared with the current state-of-the-art protocol with direct reconciliation. This improvement allows for the possibility of CV-QKD within a larger variety of short-range high-frequency communication scenarios and it builds a strong case for

CV-QKD as the primary method of secure communications at terahertz frequencies in the atmosphere.

We hope that in the near future, proof-of-concept experiments demonstrating our CV-QKD protocols in a realistic setting will emerge. This is a reasonable expectation particularly in the case of our MDI protocol due to the simplicity of the states involved. Despite the merits of using coherent states in our MDI protocol, another avenue for future work is to extend the mathematical framework to allow for thermal states as information carriers. Finally, for both protocols, we would like to perform a finite-size analysis to obtain more realistic estimates for the secret key rate of possible future implementations in the field.

Our analysis of the butterfly network has outlined a little-known difficulty that must be considered in future quantum network infrastructure. We have shown that this network structure is particularly detrimental to quantum networking which performs badly when compared with its classical counterpart. Moreover, we have shown that a network structure that contains multiple butterfly blocks may experience an even larger discrepancy between the two regimes.

Our quantification of the performance discrepancies between quantum and classical networking in the most general networks constructed with butterfly blocks provides a useful reference when designing quantum network infrastructure with particular regard to situations that should be avoided. Our particular analysis of networks constructed with realistic noisy channels, namely the erasure and depolarizing channel, add strength to this reference as they reveal the performance in a more realistic scenario. In the future, we hope to investigate the inferiority of quantum networking in the butterfly network in the hope that it may be exploited in quantum devices.

Appendix A

Entropy approximation of a non-Gaussian state

To avoid complex treatment of non-Gaussian states in the Fock basis, we will introduce an approximation for the entropy of a particular type of non-Gaussian state that is composed of the average of two Gaussian states with the same CM and different mean values. We use the CM and mean values of the constituent states to write a formula for the CM of the total state, then, by treating it as Gaussian, we use this CM to estimate its entropy. This approximation is most accurate for states with small higher-order moments, but the Gaussian assumption ensures that it is an upper bound on the entropy of any state of this form. This fact makes the approximation particularly useful in quantum key distribution when calculating the total entropy of an eavesdropper's non-Gaussian state in the Holevo bound.

We will label the constituent states of the global state $\hat{\rho}$ as $\hat{\rho}_+$ and $\hat{\rho}_-$ with associated probabilities $p(+)$ and $p(-)$, respectively. The general non-Gaussian state can then be written as

$$\hat{\rho} = \sum_{\kappa=\pm} p(\kappa)\hat{\rho}_\kappa. \tag{A.0.1}$$

Let us now recall the definitions of the mean value and CM of a Gaussian state $\hat{\rho}$ by referring back to equations (2.2.44) and (2.2.45). The mean value of the quadrature operator $\hat{x}_i$ is given by

$$\bar{x}_i = \langle \hat{x}_i \rangle = \mathrm{tr}(\hat{x}_i\hat{\rho}) \tag{A.0.2}$$

and the covariance matrix of a state is given by

$$V_{ij} = \frac{1}{2}\langle\{\Delta\hat{x}_i, \Delta\hat{x}_j\}\rangle = \frac{1}{2}\operatorname{tr}\left[\{\hat{x}_i, \hat{x}_j\}\hat{\rho}\right] - \bar{x}_i\bar{x}_j. \tag{A.0.3}$$

Using Eq. (A.0.3), we can express the elements V_{ij} of the CM, $\mathbf{V}$ of a constituent state $\hat{\rho}_\kappa$ with mean value $\bar{\mathbf{x}}^\kappa$ as

$$V_{ij}^\kappa + \bar{x}_i^\kappa\bar{x}_j^\kappa = \frac{1}{2}\operatorname{tr}\left[\{\hat{x}_i, \hat{x}_j\}\hat{\rho}_\kappa\right], \tag{A.0.4}$$

and we can also write the elements V'_{ij} of the CM $\mathbf{V}'$ of the total state $\hat{\rho}$ as

$$\begin{aligned} V'_{ij} &= \frac{1}{2}\operatorname{tr}\left[\{\hat{x}_i, \hat{x}_j\}\left(\sum_{\kappa=\pm} p(\kappa)\hat{\rho}_\kappa\right)\right] - \bar{x}_i\bar{x}_j \\ &= \sum_{\kappa=\pm} p(\kappa)\frac{1}{2}\operatorname{tr}\left[\{\hat{x}_i, \hat{x}_j\}\hat{\rho}_\kappa\right] - \bar{x}_i\bar{x}_j. \end{aligned} \tag{A.0.5}$$

We then substitute into this expression the right hand side of Eq. (A.0.4) to obtain

$$\begin{aligned} V'_{ij} &= \sum_{\kappa=\pm} p(\kappa)\left(V_{ij}^\kappa + \bar{x}_i^\kappa\bar{x}_j^\kappa\right) - \bar{x}_i\bar{x}_j \\ &= V_{ij} + \sum_{\kappa=\pm} p(\kappa)\bar{x}_i^\kappa\bar{x}_j^\kappa - \bar{x}_i\bar{x}_j, \end{aligned} \tag{A.0.6}$$

where we have made use of the requirement that the CMs of the constituent states are identical. Now by writing the mean values as $\bar{x}_i = \operatorname{tr}(\hat{x}_i\hat{\rho}) = \sum_\kappa p(\kappa)\operatorname{tr}(\hat{x}_i\hat{\rho}_k)$, and substituting into Eq. (A.0.6), we obtain

$$V'_{ij} = V_{ij} + \sum_{\kappa=\pm} p(\kappa)\bar{x}_i^\kappa\bar{x}_j^\kappa - \sum_{\kappa=\pm}\sum_{\kappa'=\pm} p(\kappa)p(\kappa')\bar{x}_i^\kappa\bar{x}_j^{\kappa'} \tag{A.0.7}$$

and by factoring out one of the sums we obtain

$$\begin{aligned} V'_{ij} &= V_{ij} + \sum_{\kappa=\pm} p(\kappa)\left[\bar{x}_i^\kappa\bar{x}_j^\kappa - \sum_{\kappa'=\pm} p(\kappa')\bar{x}_i^\kappa\bar{x}_j^{\kappa'}\right] \\ &= V_{ij} + \sum_{\kappa=\pm} p(\kappa)\left[\bar{x}_i^\kappa\bar{x}_j^\kappa - p(\kappa)\bar{x}_i^\kappa\bar{x}_j^\kappa - p(-\kappa)\bar{x}_i^\kappa\bar{x}_j^{-\kappa}\right] \\ &= V_{ij} + \sum_{\kappa=\pm} p(\kappa)p(-\kappa)\bar{x}_i^\kappa\left(\bar{x}_j^\kappa - \bar{x}_j^{-\kappa}\right), \end{aligned} \tag{A.0.8}$$

where we have used $1 - p(\kappa) = p(-\kappa)$. Now note that $p(\kappa)p(-\kappa) = p(+)p(-)$ for either value of κ, and $\sum_\kappa \bar{x}_i^\kappa(\bar{x}_j^\kappa - \bar{x}_j^{-\kappa}) = (\bar{x}_j^+ - \bar{x}_j^-)\sum_\kappa \kappa\bar{x}_i^\kappa$. Therefore we obtain

$$\begin{aligned} V'_{ij} &= V_{ij}^+ + p(+)p(-)(\bar{x}_j^+ - \bar{x}_j^-)\sum_{\kappa=\pm}\kappa\bar{x}_i^\kappa \\ &= V_{ij}^+ + p(+)p(-)(\bar{x}_j^+ - \bar{x}_j^-)\left(\bar{x}_i^+ - \bar{x}_i^-\right). \end{aligned} \tag{A.0.9}$$

We can write this in compact outer product form as

$$\mathbf{V}' = \mathbf{V} + p(+)p(-)\Delta\bar{\mathbf{x}} \cdot \Delta\bar{\mathbf{x}}^{\mathsf{T}}, \tag{A.0.10}$$

where $\Delta\bar{\mathbf{x}} = \bar{\mathbf{x}}^{+} - \bar{\mathbf{x}}^{-}$.

Abbreviations

BSC Binary symmetric channel.

CC Classical communication.

CM Covariance matrix.

CV Continuous variable.

DR Direct reconciliation.

DV Discrete variable.

EPR Einstein Podolsky Rosen.

GHZ Greenberger Horne Zeilinger.

IID Independent and identically distributed.

LO Local operation.

LOCC Local operation and classical communication.

MDI Measurement-device independent.

OPA Optical parametric amplification.

PLOB Pirandola Laurenza Ottaviani Banchi.

QIT Quantum information theory.

QKD Quantum key distribution.

QNC Quantum network coding.

REE Relative entropy of entanglement.

RR Reverse reconciliation.

RSA Rivest Shamir Adleman.

SNU Shot-noise units.

TF Twin field.

TMSV Two-mode squeezed vacuum.

VNE von Neumann entropy.

Bibliography

[1] Kieran N. Wilkinson, Panagiotis Papanastasiou, Carlo Ottaviani, Tobias Gehring, and Stefano Pirandola. Long-distance continuous-variable measurement-device-independent quantum key distribution with postselection. Phys. Rev. Research, 2:033424, 2020.

[2] Kieran N Wilkinson, Thomas PW Cope, and Stefano Pirandola. Exploring the limitations of quantum networking through butterfly-based networks. Advanced Quantum Technologies, 3(3):1900103, 2020.

[3] Max Planck. On the law of distribution of energy in the normal spectrum. Annalen der physik, 4(553):1, 1901.

[4] Albert Einstein. Über einen die erzeugung und verwandlung des lichtes betreffenden heuristischen gesichtspunkt. Annalen der physik, 322(6):132–148, 1905.

[5] Hugh Everett III. " relative state" formulation of quantum mechanics. Reviews of modern physics, 29(3):454, 1957.

[6] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? Physical review, 47(10):777, 1935.

[7] Stuart J Freedman and John F Clauser. Experimental test of local hidden-variable theories. Physical Review Letters, 28(14):938, 1972.

[8] Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.

[9] Samuel L Braunstein and Arun K Pati. Quantum information with continuous variables. Springer Science & Business Media, 2012.

[10] Paul Benioff. The computer as a physical system: A microscopic quantum mechanical hamiltonian model of computers as represented by turing machines. Journal of statistical physics, 22(5):563–591, 1980.

[11] David Deutsch and Richard Jozsa. Rapid solution of problems by quantum computation. Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences, 439(1907):553–558, 1992.

[12] Don Coppersmith. An approximate fourier transform useful in quantum factoring. arXiv preprint quant-ph/0201067, 2002.

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

[14] Lov K Grover. A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, pages 212–219, 1996.

[15] Richard P Feynman. Simulating physics with computers. Int. J. Theor. Phys, 21(6/7), 1982.

[16] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2):120–126, 1978.

[17] CHBG Brassard and Charles H Bennett. Quantum cryptography: Public key distribution and coin tossing. In International conference on computers, systems and signal processing, 1984.

[18] Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón, Nicolas J Cerf, Timothy C Ralph, Jeffrey H Shapiro, and Seth Lloyd. Gaussian quantum information. Reviews of Modern Physics, 84(2):621, 2012.

[19] Samuel L Braunstein and Peter Van Loock. Quantum information with continuous variables. Reviews of modern physics, 77(2):513, 2005.

[20] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. Nature communications, 8(1):1–15, 2017.

[21] Carlo Ottaviani, Matthew J Woolley, Misha Erementchouk, John F Federici, Pinaki Mazumder, Stefano Pirandola, and Christian Weedbrook. Terahertz quantum cryptography. IEEE Journal on Selected Areas in Communications, 38(3):483–495, 2020.

[22] Ziqing Wang, Robert Malaney, and Jonathan Green. Inter-satellite quantum key distribution at terahertz frequencies. In ICC 2019-2019 IEEE International Conference on Communications (ICC), pages 1–7. IEEE, 2019.

[23] Ian F Akyildiz, Josep Miquel Jornet, and Chong Han. Terahertz band: Next frontier for wireless communications. Physical Communication, 12:16–32, 2014.

[24] Steven Cherry. Edholm's law of bandwidth. IEEE spectrum, 41(7):58–60, 2004.

[25] Samuel L Braunstein and Stefano Pirandola. Side-channel-free quantum key distribution. Physical review letters, 108(13):130502, 2012.

[26] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. Physical review letters, 108(13):130503, 2012.

[27] H Jeff Kimble. The quantum internet. Nature, 453(7198):1023–1030, 2008.

[28] Stefano Pirandola and Samuel L Braunstein. Physics: Unite to build a quantum internet. Nature, 532(7598):169–171, 2016.

[29] Rudolf Ahlswede, Ning Cai, S-YR Li, and Raymond W Yeung. Network information flow. IEEE Transactions on information theory, 46(4):1204–1216, 2000.

[30] Debashis Sen. The uncertainty relations in quantum mechanics. Current Science, pages 203–218, 2014.

[31] John Williamson. On the algebraic problem concerning the normal forms of linear dynamical systems. American journal of mathematics, 58(1):141–163, 1936.

[32] Stefano Pirandola, Gaetana Spedalieri, Samuel L Braunstein, Nicolas J Cerf, and Seth Lloyd. Optimality of gaussian discord. Physical review letters, 113(14):140405, 2014.

[33] Claude E Shannon. A mathematical theory of communication. The Bell system technical journal, 27(3):379–423, 1948.

[34] Vlatko Vedral. The role of relative entropy in quantum information theory. Reviews of Modern Physics, 74(1):197, 2002.

[35] Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim. Secure key from bound entanglement. Physical review letters, 94(16):160502, 2005.

[36] Igor Devetak. The private classical capacity and quantum capacity of a quantum channel. IEEE Transactions on Information Theory, 51(1):44–55, 2005.

[37] Charles H Bennett, David P DiVincenzo, John A Smolin, and William K Wootters. Mixed-state entanglement and quantum error correction. Physical Review A, 54(5):3824, 1996.

[38] Stefano Pirandola. End-to-end capacities of a quantum communication network. Communications Physics, 2(1):1–10, 2019.

[39] Stefano Pirandola. Bounds for multi-end communication over quantum networks. Quantum Science and Technology, 4(4):045006, 2019.

[40] Daniel M Greenberger, Michael A Horne, and Anton Zeilinger. Going beyond bell's theorem. In Bell's theorem, quantum theory and conceptions of the universe, pages 69–72. Springer, 1989.

[41] Timothy C Ralph. Continuous variable quantum cryptography. Physical Review A, 61(1):010303, 1999.

[42] Mark Hillery. Quantum cryptography with squeezed states. Physical Review A, 61(2):022309, 2000.

[43] Margaret D Reid. Quantum cryptography with a predetermined key, using continuous-variable einstein-podolsky-rosen correlations. Physical Review A, 62(6):062308, 2000.

[44] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. Physical review letters, 88(5):057902, 2002.

[45] Frédéric Grosshans and Philippe Grangier. Reverse reconciliation protocols for quantum cryptography with continuous variables. arXiv preprint quant-ph/0204127, 2002.

[46] Frédéric Grosshans, Gilles Van Assche, Jérôme Wenger, Rosa Brouri, Nicolas J Cerf, and Philippe Grangier. Quantum key distribution using gaussian-modulated coherent states. Nature, 421(6920):238–241, 2003.

[47] Frédéric Grosshans, Nicolas J Cerf, Jérôme Wenger, Rosa Tualle-Brouri, and Ph Grangier. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. arXiv preprint quant-ph/0306141, 2003.

[48] Christian Weedbrook, Andrew M Lance, Warwick P Bowen, Thomas Symul, Timothy C Ralph, and Ping Koy Lam. Quantum cryptography without switching. Physical review letters, 93(17):170504, 2004.

[49] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. Proceedings of the Royal Society A: Mathematical, Physical and engineering sciences, 461(2053):207–235, 2005.

[50] Paul Jouguet, Sébastien Kunz-Jacques, and Anthony Leverrier. Long-distance continuous-variable quantum key distribution with a gaussian modulation. Physical Review A, 84(6):062317, 2011.

[51] Stefano Pirandola, Ulrik L Andersen, Leonardo Banchi, Mario Berta, Darius Bunandar, Roger Colbeck, Dirk Englund, Tobias Gehring, Cosmo Lupo, Carlo Ottaviani, et al. Advances in quantum cryptography. Advances in Optics and Photonics, 12(4):1012–1236, 2020.

[52] Stefano Pirandola, Raul García-Patrón, Samuel L Braunstein, and Seth Lloyd. Direct and reverse secret-key capacities of a quantum channel. Physical review letters, 102(5):050503, 2009.

[53] Frédéric Grosshans and Philippe Grangier. Quantum cloning and teleportation criteria for continuous quantum variables. Physical Review A, 64(1):010301, 2001.

[54] Stefano Pirandola, Stefano Mancini, Seth Lloyd, and Samuel L Braunstein. Continuous-variable quantum cryptography using two-way quantum communication. Nature Physics, 4(9):726–730, 2008.

[55] Ch Silberhorn, Timothy C Ralph, Norbert Lütkenhaus, and Gerd Leuchs. Continuous variable quantum cryptography: Beating the 3 db loss limit. Physical review letters, 89(16):167901, 2002.

[56] Matthias Heid and Norbert Lütkenhaus. Efficiency of coherent-state quantum cryptography in the presence of loss: Influence of realistic error correction. Physical Review A, 73(5):052316, 2006.

[57] Matthias Heid and Norbert Lütkenhaus. Security of coherent-state quantum cryptography in the presence of gaussian noise. Physical Review A, 76(2):022313, 2007.

[58] Thomas Symul, Daniel J Alton, Syed M Assad, Andrew M Lance, Christian Weedbrook, Timothy C Ralph, and Ping Koy Lam. Experimental demonstration of post-selection-based continuous-variable quantum key distribution in the presence of gaussian noise. Physical Review A, 76(3):030303, 2007.

[59] Andrew M Lance, Thomas Symul, Vikram Sharma, Christian Weedbrook, Timothy C Ralph, and Ping Koy Lam. No-switching quantum key distri-

bution using broadband modulated coherent light. Physical review letters, 95(18):180503, 2005.

[60] Guilherme Temporão, Sébastien Tanzilli, Hugo Zbinden, Nicolas Gisin, Thierry Aellen, Marcella Giovannini, and Jérome Faist. Mid-infrared single-photon counting. Optics letters, 31(8):1094–1096, 2006.

[61] Christian Weedbrook, Stefano Pirandola, Seth Lloyd, and Timothy C Ralph. Quantum cryptography approaching the classical limit. Physical review letters, 105(11):110501, 2010.

[62] Christian Weedbrook, Stefano Pirandola, and Timothy C Ralph. Continuous-variable quantum key distribution using thermal states. Physical Review A, 86(2):022318, 2012.

[63] Christian Weedbrook, Carlo Ottaviani, and Stefano Pirandola. Two-way quantum cryptography at different wavelengths. Physical Review A, 89(1):012309, 2014.

[64] Panagiotis Papanastasiou, Carlo Ottaviani, and Stefano Pirandola. Gaussian one-way thermal quantum cryptography with finite-size effects. Physical Review A, 98(3):032314, 2018.

[65] Reed W Andrews, Robert W Peterson, Tom P Purdy, Katarina Cicak, Raymond W Simmonds, Cindy A Regal, and Konrad W Lehnert. Bidirectional and efficient conversion between microwave and optical light. Nature Physics, 10(4):321–326, 2014.

[66] Maurice M Mizrahi. Generalized hermite polynomials. Journal of Computational and Applied Mathematics, 1(3):137–140, 1975.

[67] Pieter Kok and Samuel L Braunstein. Multi-dimensional hermite polynomials in quantum optics. Journal of Physics A: Mathematical and General, 34(31):6185, 2001.

[68] Kurt Bernardo Wolf. Canonical transforms. i. complex linear transforms. Journal of Mathematical Physics, 15(8):1295–1301, 1974.

[69] P Kramer, Marcos Moshinsky, and TH Seligman. Complex extensions of canonical transformations and quantum mechanics. In Group theory and its applications, pages 249–332. Elsevier, 1975.

[70] V V Dodonov, O V Man'ko, and V I Man'ko. Multidimensional Hermite polynomials and photon distribution for polymode mixed light. Physical Review A, 50(1):813, 1994.

[71] Brajesh Gupt, Josh Izaac, and Nicolás Quesada. The walrus: a library for the calculation of hafnians, hermite polynomials and gaussian boson sampling. Journal of Open Source Software, 4(44):1705, 2019.

[72] Jingye Sun, Fangjing Hu, and Stepan Lucyszyn. Predicting atmospheric attenuation under pristine conditions between 0.1 and 100 thz. IEEE Access, 4:9377–9399, 2016.

[73] Marco Lucamarini, Zhiliang L Yuan, James F Dynes, and Andrew J Shields. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. Nature, 557(7705):400–403, 2018.

[74] Kiyoshi Tamaki, Hoi-Kwong Lo, Wenyuan Wang, and Marco Lucamarini. Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound. arXiv preprint arXiv:1805.05511, 2018.

[75] M Minder, M Pittaluga, GL Roberts, M Lucamarini, JF Dynes, ZL Yuan, and AJ Shields. Experimental quantum key distribution beyond the repeaterless secret key capacity. Nature Photonics, 13(5):334–338, 2019.

[76] Xiongfeng Ma, Pei Zeng, and Hongyi Zhou. Phase-matching quantum key distribution. Physical Review X, 8(3):031043, 2018.

[77] Yang Liu, Zong-Wen Yu, Weijun Zhang, Jian-Yu Guan, Jiu-Peng Chen, Chi Zhang, Xiao-Long Hu, Hao Li, Cong Jiang, Jin Lin, et al. Experimental twin-field quantum key distribution through sending or not sending. Physical Review Letters, 123(10):100505, 2019.

[78] Cong Jiang, Zong-Wen Yu, Xiao-Long Hu, and Xiang-Bin Wang. Unconditional security of sending or not sending twin-field quantum key distribution with finite pulses. Physical Review Applied, 12(2):024061, 2019.

[79] Stefano Pirandola, Carlo Ottaviani, Gaetana Spedalieri, Christian Weedbrook, Samuel L Braunstein, Seth Lloyd, Tobias Gehring, Christian S Jacobsen, and Ulrik L Andersen. High-rate measurement-device-independent quantum cryptography. Nature Photonics, 9(6):397–402, 2015.

[80] Panagiotis Papanastasiou, Carlo Ottaviani, and Stefano Pirandola. Finite-size analysis of measurement-device-independent quantum cryptography with continuous variables. Physical Review A, 96(4):042332, 2017.

[81] Xueying Zhang, Yichen Zhang, Yijia Zhao, Xiangyu Wang, Song Yu, and Hong Guo. Finite-size analysis of continuous-variable measurement-device-independent quantum key distribution. Physical Review A, 96(4):042334, 2017.

[82] Pu Wang, Xuyang Wang, and Yongmin Li. Continuous-variable measurement-device-independent quantum key distribution using modulated squeezed states and optical amplifiers. Physical Review A, 99(4):042309, 2019.

[83] Hong-Xin Ma, Peng Huang, Dong-Yun Bai, Shi-Yu Wang, Wan-Su Bao, and Gui-Hua Zeng. Continuous-variable measurement-device-independent quantum key distribution with photon subtraction. Physical Review A, 97(4):042329, 2018.

[84] Luyu Huang, Yichen Zhang, Ziyang Chen, and Song Yu. Unidimensional continuous-variable quantum key distribution with untrusted detection under realistic conditions. Entropy, 21(11):1100, 2019.

[85] Hong-Xin Ma, Peng Huang, Dong-Yun Bai, Tao Wang, Shi-Yu Wang, Wan-Su Bao, and Gui-Hua Zeng. Long-distance continuous-variable measurement-device-independent quantum key distribution with discrete modulation. Physical Review A, 99(2):022322, 2019.

[86] Raúl García-Patrón and Nicolas J Cerf. Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution. Physical review letters, 97(19):190503, 2006.

[87] Carlo Ottaviani, Gaetana Spedalieri, Samuel L Braunstein, and Stefano Pirandola. Continuous-variable quantum cryptography with an untrusted relay: Detailed security analysis of the symmetric configuration. Physical Review A, 91(2):022320, 2015.

[88] Leonardo Banchi, Samuel L Braunstein, and Stefano Pirandola. Quantum fidelity for arbitrary gaussian states. Physical review letters, 115(26):260501, 2015.

[89] Stefano Pirandola and Seth Lloyd. Computable bounds for the discrimination of gaussian states. Physical Review A, 78(1):012331, 2008.

[90] Chao Zhou, Xiangyu Wang, Yichen Zhang, Zhiguo Zhang, Song Yu, and Hong Guo. Continuous-variable quantum key distribution with rateless reconciliation protocol. Physical Review Applied, 12(5):054013, 2019.

[91] Yadong Wu, Jian Zhou, Xinbao Gong, Ying Guo, Zhi-Ming Zhang, and Guangqiang He. Continuous-variable measurement-device-independent multipartite quantum communication. Physical Review A, 93(2):022325, 2016.

[92] Carlo Ottaviani, Cosmo Lupo, Riccardo Laurenza, and Stefano Pirandola. Modular network for high-rate quantum conferencing. Communications Physics, 2(1):1–6, 2019.

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

[94] Masahito Hayashi, Kazuo Iwama, Harumichi Nishimura, Rudy Raymond, and Shigeru Yamashita. Quantum network coding. In Annual Symposium on Theoretical Aspects of Computer Science, pages 610–621. Springer, 2007.

[95] Vladimir Bužek and Mark Hillery. Quantum copying: Beyond the no-cloning theorem. Physical Review A, 54(3):1844, 1996.

[96] Avinash Jain, Massimo Franceschetti, and David A Meyer. On quantum network coding. Journal of Mathematical Physics, 52(3):032201, 2011.

[97] Masahito Hayashi. Prior entanglement between senders enables perfect quantum network coding with modification. Physical Review A, 76(4):040301, 2007.

[98] He Lu, Zheng-Da Li, Xu-Fei Yin, Rui Zhang, Xiao-Xu Fang, Li Li, Nai-Le Liu, Feihu Xu, Yu-Ao Chen, and Jian-Wei Pan. Experimental quantum network coding. npj Quantum Information, 5(1):1–5, 2019.

[99] Takahiko Satoh, François Le Gall, and Hiroshi Imai. Quantum network coding for quantum repeaters. Physical Review A, 86(3):032331, 2012.

[100] Harumichi Nishimura. Quantum network coding-how can network coding be applied to quantum information? In 2013 International Symposium on Network Coding (NetCod), pages 1–5. IEEE, 2013.

[101] Zhen-Zhen Li, Gang Xu, Xiu-Bo Chen, Zhiguo Qu, Xin-Xin Niu, and Yi-Xian Yang. Efficient quantum state transmission via perfect quantum network coding. Science China Information Sciences, 62(1):12501, 2019.

[102] Hirotada Kobayashi, François Le Gall, Harumichi Nishimura, and Martin Rötteler. General scheme for perfect quantum network coding with free classical communication. In International Colloquium on Automata, Languages, and Programming, pages 622–633. Springer, 2009.

[103] Hirotada Kobayashi, François Le Gall, Harumichi Nishimura, and Martin Rötteler. Constructing quantum network coding schemes from classical nonlinear protocols. In 2011 IEEE International Symposium on Information Theory Proceedings, pages 109–113. IEEE, 2011.

[104] Debbie Leung, Jonathan Oppenheim, and Andreas Winter. Quantum network communication-the butterfly and beyond. IEEE Transactions on Information Theory, 56(7):3478–3490, 2010.

[105] Ming-Xing Luo, Gang Xu, Xiu-Bo Chen, Yi-Xian Yang, and Xiaojun Wang. Efficient quantum transmission in multiple-source networks. Scientific reports, 4:4571, 2014.

[106] Christopher King. The capacity of the quantum depolarizing channel. IEEE Transactions on Information Theory, 49(1):221–229, 2003.

[107] Charles H Bennett, David P DiVincenzo, and John A Smolin. Capacities of quantum erasure channels. Physical Review Letters, 78(16):3217, 1997.