Generalized approach to Gaussian and non-Gaussian CV QKD

Farsad Ahmad

Registration #: 00000330857

A thesis submitted in partial fulfillment of the requirements for the degree of

Master of Philosophy

in

Physics

completed under the supervision of

Dr. Aeysha Khalique

Department of Physics, School of Natural Sciences (SNS)
National University of Sciences and Technology (NUST)
Islamabad, Pakistan

August, 2022

FORM TH-4

National University of Sciences & Technology

MS THESIS WORK

We hereby recommend that the dissertation prepared under our supervision by: **Farsad Ahmad**, Regn No. **00000330857** Titled: **"Generalized approach to Gaussian and non-Gaussian CV QKD"** accepted in partial fulfillment of the requirements for the award of **MS** degree.

Examination Committee Members

1. Name: DR. MUHAMMAD ALI PARACHA Signature: _____

2. Name: DR. MUZZAMAL IQBAL SHAUKAT Signature: _____

Supervisor's Name: DR. AEYSHA KHALIQUE Signature: _____

_____ 24-08-22
Head of Department Date

COUNTERSINGED

Date: 26.08.2022 _____
Dean/Principal

Declaration

I certify that this research work titled "Generalized approach to Gaussian and non-Gaussian CV-QKD" is my own work. The work has not been presented elsewhere for assessment. The material that has been used from other sources it has been properly acknowledged / referred.

Farsad Ahmad

2020-NUST-MS PHY-330857

Acknowledgement

My sincere appreciation to the department of physics at NUST for not only providing an environment that promotes imagination and scientific thought but also for giving me the opportunity to work with professionals. This work would have been impossible without the supervision of Dr. Aeysha Khalique who guided me generously during all phases of my research.

Abstract

Quantum key distribution (QKD) is a growing phenomenon rapidly being adopted around the world because it adds unconditional security to our day to day communication. Recent trend in QKD has shifted towards using continuous variables (CV) to encode quantum data because of the ease in producing, manipulating, transmitting and measuring these signals. In this thesis we have developed the foundation of CV QKD with a generalized approach. By generalizing steps involved in CV QKD protocols, we have simulated several Gaussian as well as non-Gaussian protocols enabling us to quickly explore improvement opportunities in any CV QKD protocol. Resultingly we were able to find significant improvement in measurement device independent (MDI) protocol. Our method allows the generation of a positive key rate when initial squeezing is low, additionally these states offer more tolerance to thermal noise. Such states bring MDI protocol closer to commercial realization.

Contents

Thesis Outline

The thesis starts from chapter 1 by first explaining where classical cryptography fails and how QKD solves this problem. Followed by a brief explanation of the first QKD protocol and ended by listing the advantages offered by continuous variables (CV) over discrete variables (DV) QKD.

Chapter 2 lays the foundation of QKD using continuous variable Gaussian states. We start by discussing shot noise units that are used throughout this thesis, then we discuss symplectic formalism for Gaussian states and their detection methods. Finally we show the mathematical structure of some of the most basic CV states.

In chapter 3 we analyze the security of Gaussian states. This section starts by proving the reduction of entanglement schemes to prepare and measure schemes and then moves towards the mathematical description of attacks by an eavesdropper.

Chapter 4 gives the mathematical expressions for general Gaussian transformations that were used in this thesis.

In chapter 5 we show our contributions in this subject by simulating several Gaussian protocols using the formalism developed. We show how our tools are designed in a generalized fashion which makes them compatible with any Gaussian-type protocol. In chapter 6 we accommodate non-Gaussian operations in our tools to expand the reach of the code. We also simulate some useful non-Gaussian protocols to show the working.

Once we have devised these tools and verified their working, we let the computer make our guesses and test them for any improvement in existing protocols. One significant improvement that was observed is explained in chapter 7. This thesis is then concluded in chapter 8.

Chapter 1

Classical Cryptography and the need for Quantum Communication

Cryptography is the study of secrets. In the context of communication, it translates to secrecy between communicating parties. Methods of cryptography have long been a part of our history as the first cryptic message dating back to age of King Caesar Rome who made the Caesar cipher to encrypt communication with his spies.

Modern day cryptography lets us communicate privately on the internet. This has given birth to many advancements such as internet banking, sensitive military communication, private and secure data etc. The foundations of these services lie in cryptographic methods of computer science.

Communication today is secured by two methods; **symmetric key cryptography** where two communicating parties first meet and share an identical key. They can then part away from each other, use their shared keys to encrypt their messages and send them to each other. Such encryption is impossible to break if the key is significantly long. The downside of this method is that they cannot share a key without meeting in person. Using the same key over and over again dilutes the level of security it provides thus making it susceptible to deciphering by an eavesdropper if enough communication data is provided. An example of symmetric key cryptography is the use of credit cards. They hold a number and code only known by the holder and the bank which lets them process transactions securely until the card expires and new one is issued to maintain the quality of secrecy.

The second method is **public key cryptography**. As the name suggests, the primary parties do not meet face to face, rather they use public encryption methods to develop a secret key while staying at their homes. This solves the problem of meeting face to face. In these schemes, the primary

parties always start by developing a new secret key before communicating, once communication is terminated the key is disposed. The most commonly used public key encryption method is the RSA encryption and is by far the most reliable method for public encryption

Before discussing the loophole in the RSA encryption method, to be consistent with the nomenclature of information theory, we will call our primary parties Alice and Bob. Alice wants to communicate with Bob secretly while an eavesdropper (conveniently named Eve) tries to decipher their communication.

RSA encryption relies on generating a big number which is a multiple of two prime numbers (call it c) such that Alice has one of those prime numbers (a) and Bob has the other one (b). Hence the outgoing message is ciphered using c which is $a \times b$. This lets Alice and Bob be the only party who can decipher that message quickly as both of these parties have half of the factor. This form of encryption can be broken if an eavesdropper can factorize c without the knowledge of a or b. A classical computer has only one way to factorize this number; check every possibility. Of course that means if the number is big enough, computation time goes up exponentially. For example a prime factor of 768 digits can take up to 2000 years for a classical computer to factorize.

The advent of Quantum Computing imposed a threat to RSA encryption. Peter Shor proposed an algorithm that can break prime factors in polynomial time but it can only work on a quantum computer. Although we don't have a considerable sized quantum computer today that can break RSA but the possibility of it happening one day requires us to develop new methods to encrypt our data.

There are two approaches to tackle this problem, one relies on chaos-induced random numbers to encrypt signals and the other relies on quantum mechanics. These two approaches have separately been studied and are being developed to this day. While chaos-induced methods are pseudo reliable, quantum mechanics is unconditionally reliable, in this thesis we look at how quantum key distribution (QKD) solves this problem.

QKD promises the generation of a secure key between two separated parties. The idea of QKD revolves around Heisenberg's uncertainty principle; any measurement on one quadrature disturbs the measurement of it's conjugate quadrature. Alice now encodes her data in quantum states rather then encrypted classical numbers. If Eve tries to observe the quantum state, the state collapses. Eve could try to recreate the state she observed but it can never match with what was being sent due to the uncertainty principle. This makes it so that Eve has to leave her trace if she tries to tap the

Alice's random bits	0	0	1	0	1	1	1	0
Alice's sending bases	Z	X	Z	Z	X	X	Z	X
Bob's measurement basis	Z	Z	X	Z	X	X	X	X
Bob's result	0	1	1	0	1	1	0	0
Alice and Bob's key	0			0	1	1		0

Table 1.1.1: BB84 protocol without any eavesdropper

information thus exposing her. This intrinsic nature has enabled QKD as a viable alternative to our previous methods of public key cryptography.

1.1 The first QKD protocol:BB84

In 1984, Charles Bennett and Gilles Brassard developed the first QKD protocol pioneering the idea of QKD [2]. To understand the working of the protocol, let us first review the behaviour of measuring spin polarized states. If Alice prepares a spin state up in Z polarization, measuring the state in Z basis will always result in spin up. If the same state is measured in X basis, we get an equal probability of measuring up and down. There is no way for Eve to know which encoding bases were used so the encoded information is lost if measurement basis don't match. Let us now see this behaviour utilized by the BB84 protocol:

- Alice announces the mapping of her bits to Bob. For example she can decide on spin up as bit value 1 and down as bit value 0.

- Alice generates a string of random bits. She then decides to send the bit value encoded randomly in either X basis or Z basis.

- Bob, when receiving the bits, randomly chooses X or Z basis. Once all the signals are measured, the protocol moves to post processing.

- Bob publicly announces the basis he chose to measure the states. Alice tells Bob which basis to keep based on the ones that matched with her own preparation basis.

To detect the presence of any eavesdropper, Alice and Bob perform an extra step called parameter estimation. Once Bob has corrected his raw key, he announces a fraction of his key publicly. This lets Alice compare them with her bits. In case of no channel errors/eavesdropper, the announced bits should match perfectly with Alice. In the presence of error/Eve, some percentage of the announced bits will mismatch. In that case Alice and Bob perform steps to correct errors and improve privacy of their key.

Based off BB84, a general QKD scheme follows the following steps:

- **Quantum Transmission:** Alice sends a random string of qubits to Bob which are transmitted via a quantum channel. These qubits may belong to single-qubit protocols or entangled-qubit protocols.

- **Sifting:** Alice and/or Bob publicly share their preparation and measurement basis respectively through a classical channel. They disclose (then discard) a small percentage of their measurement results (where preparation and measurement basis match) to estimate channel error.

- **Error correction:** Alice further reveals additional information to Bob which Bob uses to correct his error bits.

- **Privacy Amplification:** To mitigate the information leaked during transmission and error correction, Alice and Bob compress their error corrected key into a final key. To be reliable, we must put an upper bound on the amount of information leaked and compress the error corrected key accordingly.

1.2 Practical advantages of CV QKD

BB84 is a discrete variable QKD (DV-QKD) scheme, which means that the encoded information is definitive i.e. either up or down. The primary problem that DV-QKD inherits is the complete loss of information if a qubit sustains enough error. A more recent trend is focused around continuous variables QKD (CV-QKD) where we encode information on a continuous spectrum. This type of encoding is not completely lost when environment is taken in account, but rather incurs error allowing us to balance the amount of error we can sustain. Some of the advantages that CV-QKD offers are listed below:

- CV QKD does not require expensive equipment for it's implementation. Most of the technology that is used in CV QKD is already present in the current coherent telecommunication devices. An example is the coherent light source device used to generate CV pulses. It is highly efficient as compared to heralded single photon generators.

- CV signals are detected using homodyne detectors which work on a practical efficiency of 90%, compared to single photon detectors (SPD) used in DV QKD that work at nearly 70% with near ideal conditions.

- Homodyne detectors have a measurement frequency of about 1GHz compared to the measurement frequency of SPR at about 100MHz. This translates to a very high raw key rate that can be generated by CV QKD protocols.

- Recent experiments show that CV QKD is supported by wavelength division multiplexing[1] allowing it to be integrated with already deployed optical fibres [15].

- CV QKD networks are robust, they support different configurations such as having multiple users on the same channel, different topoligies of networks and coexisting with existing telecom structures.

While CV-QKD does not perform as outstanding as DV-QKD when long distances are considered, but with current progress and repeater models alongside the practical advantages of CV-QKD, progress towards long distance CV-QKD does not seem too far.

[1]Multiplexing is a technique used in optical fibre communication which mixes multiple signals by modifying their wavelengths so that they can be sent through the same line.

Chapter 2

Continuous Variables; Gaussian Quantum Information

Any quantum system is a continuous variable system when it has an infinite dimensional Hilbert space described by an observable that has continuous eigen values for example a system of N quantum harmonic oscillators which would have a continuous spectra for number state operator if $N \to \infty$.

Fock spaces are governed by the bosonic commutation relation $[\hat{a}, \hat{a}^\dagger] = 1$ which gives:

$$\hat{a}\,|0\rangle = 0 \qquad\qquad \hat{a}\,|n\rangle = \sqrt{n}\,|n-1\rangle \quad (n \geq 1)$$

$$\hat{a}^\dagger\,|0\rangle = |1\rangle \qquad\qquad \hat{a}^\dagger\,|n\rangle = \sqrt{n+1}\,|n+1\rangle \quad (n \geq 0) \tag{2.0.1}$$

Now consider the system of N bosonic modes. Each mode is composed of a fock space that follows (2.0.1). This composite system now satisfies the commutation relation $[\hat{a}_i, \hat{a}_j] = \Omega_{ij}$ where:

$$\Omega_{ij} = \bigoplus_{\kappa=1}^{N} \omega = \begin{pmatrix} \omega & & \\ & \ddots & \\ & & \omega \end{pmatrix} \tag{2.0.2}$$

$$\omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

The above matrix generalizes the bosonic commutation relation for multiple (separable) Hilbert spaces/-

modes.

2.1 Shot Noise Units

Ladder operators are described by the relations given in (2.0.1). We cannot change their form for the sake of convenience, but, we are free to define quadrature operators w.r.t. ladder operators however we find convenient that is to say, we can rescale fundamental constants $(\hbar, c)$ to our need. This in return gives us a relation of $\hat{a}$ and $\hat{a}^\dagger$ with quadratures $\hat{q}$ and $\hat{p}$ which will give us their canonical commutation relation $[\hat{q}, \hat{p}]$ and that finally gives us the minimal uncertainty product. Our definition of $\hat{q}$ and $\hat{p}$ revolves around our requirement to set the minimal uncertainty of these operators to 1 unit i.e. $\delta\hat{q}\delta\hat{p} = 1$. By setting $\hbar = 2$ we define the quadrature operators as follows:

$$\hat{q} = (\hat{a}^\dagger + \hat{a}) \qquad\qquad \hat{p} = i(\hat{a}^\dagger - \hat{a}) \tag{2.1.1}$$

Which gives us their commutation relation:

$$\begin{aligned}
[\hat{q}, \hat{p}] &= \hat{q}\hat{p} - \hat{p}\hat{q} \\
&= i(\hat{a}^\dagger + \hat{a})(\hat{a}^\dagger - \hat{a}) - i(\hat{a}^\dagger - \hat{a})(\hat{a}^\dagger + \hat{a}) \\
&= i\Big((\hat{a}^\dagger\hat{a}^\dagger - \hat{a}^\dagger\hat{a} + \hat{a}\hat{a}^\dagger - \hat{a}\hat{a}) - (\hat{a}^\dagger\hat{a}^\dagger + \hat{a}^\dagger\hat{a} - \hat{a}\hat{a}^\dagger - \hat{a}\hat{a})\Big) \\
&= i(-2\hat{a}^\dagger\hat{a} + 2\hat{a}\hat{a}^\dagger) \\
&= i\big(-2\hat{a}^\dagger\hat{a} + 2(1 + \hat{a}^\dagger\hat{a})\big) \\
&= 2i
\end{aligned}$$

This result is slightly different from the general commutation relation of position and momentum because we demanded $\delta\hat{q}\delta\hat{p} = 1$. We will scale our values with respect to this minimum uncertainty and we call it shot noise unit (SNU).

2.2 Symplectic Formalism

Any unitary operation in this Hilbert space corresponds to a *symplectic* operation in the phase space. The symplectic formalism is an advanced topic that shows how Gaussian operations can be mapped

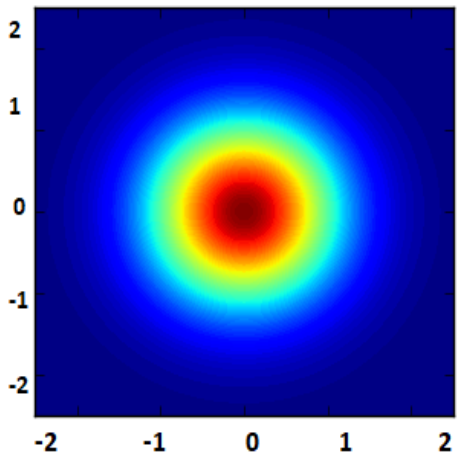


Figure 2.2.1: Wigner function of a vacuum state in phase space. The heat map gives the probability of measuring the value of position and momentum given in shot noise units. Red represents high probability while blue represents low probability.

on the phase space. We will only discuss a small part that is relevant to QKD in this thesis, for a complete description of symplectic formalism refer to [22] and for a more characteristic function approach refer to [13].

The density operator of this Hilbert space is brought to the phase space via the **Wigner characteristic function**. This is a powerful transformation because creation and annihilation operators are not physical measures, Wigner transformation allows us to get the symplectic operation in phase space corresponding to a specific unitary transformation in Hilbert space.

Observe from (2.1.1), because each Hilbert space is infinite dimensional, $\hat{q}$ and $\hat{p}$ have a continuous spectra i.e. $\hat{q}\,|q\rangle = q\,|q\rangle$ where q is a real continuous value (similarly for p) $\in \{-\infty, \infty\}$.

2.2.1 A small note on Wigner Functions

Classically, Wigner function of a phase space is a probability distribution function i.e the Wigner function tells us the probability distribution of position and momentum on the phase space. For example in case of classical light where the phase space is a continuum, the Wigner function for a perfectly prepared pulse will be a point with exact values of q and p. This is no longer true in quantum mechanics as we can not assign sharp values to position and momentum thus the Wigner function is now a $quasi$ probability distribution that takes the uncertainty of measurement in account. A graphical interpretation is given in Figure 2.2.1. Note that now for a vacuum state, values of position and momentum are not exactly zero rather they are spread out by 1 shot noise unit (lowest possible

uncertainty) as governed by Heisenberg's uncertainty principle.

The most important symplectic operation in Gaussian QKD is the beam splitter. It is defined in Hilbert space as:

$$\hat{B}(\tau) = exp\Big(cos^{-1}(\sqrt{\tau})(\hat{a}_1^\dagger \hat{a}_2 - \hat{a}_1 \hat{a}_2^\dagger)\Big)$$

Where τ is the transmissivity of the beam splitter and the subscripts label the mode of ladder operators. The symplectic form of the beam splitter is a matrix that operates on two modes and has the following form:

$$B(\tau) = \begin{bmatrix} \sqrt{\tau} & \sqrt{1-\tau} \\ -\sqrt{1-\tau} & \sqrt{\tau} \end{bmatrix}$$

This operator will be discussed in more detail later.

2.3 Gaussian States

It has now been established that our continuous variables are the quadratures q and p originating from an infinite fock space which can have multiple modes that are initially separate. By definition, any state that can completely be characterized by its mean and variance is a Gaussian state: $\hat{\rho} = \hat{\rho}(\bar{x}, V)$. These states maintain this property under *Gaussian operations*. The reason why such states are called Gaussian is because their Wigner function is a Gaussian distribution. This is also evident from Figure 2.2.1, the probability is highest at zero and exponentially decays as we go further away from the center.

When discussed in context of quantum mechanics, Gaussian states must not violate the uncertainty principle. This follows from:

$$\langle \hat{x} \rangle = Tr(\hat{x}\ \rho) \qquad V_{ij} = \frac{1}{2}\langle \{\Delta \hat{x}_i \Delta \hat{x}_j\} \rangle \qquad \hat{x}\ \in\ \{\hat{q}, \hat{p}\} \tag{2.3.1}$$

Such that:

$$\boldsymbol{\Sigma} + i\boldsymbol{\Omega} \geq 0$$

Ω is as given in (2.0.2) and Σ represents the covariance matrix which has the following structure:

$$\Sigma = \begin{array}{c} \begin{matrix} \hat{q} & \hat{p} \end{matrix} \\ \begin{pmatrix} V(\hat{q}) & C(\hat{q},\hat{p}) \\ C(\hat{q},\hat{p}) & V(\hat{p}) \end{pmatrix} \end{array} \begin{matrix} \hat{q} \\ \hat{p} \end{matrix} \tag{2.3.2}$$

We use (2.3.1) to get $V := V_{ii}$ and $C := V_{ij}$. V represents the variance of the quadrature operator which is a real positive value always ≥ 1. We can derive the uncertainty relation directly from the diagonal entries: $V(\hat{q})V(\hat{p}) \geq 1$. The off-diagonal elements are our primary interest in QKD.

C represents the covariance between quadratures. If the covariance between two quadratures is zero, it means that they are uncorrelated and hence they are separable. Generally, covariance can be negative (implying that the two quadratures are inversely correlated) or it can be positive (implying that the two quadratures are directly correlated). Positive/Negative correlation means that if a random variable X is expected to increase in a distribution A, than it will also increase/decrease in a distribution B.

Entanglement requires non-separability and hence non-zero covariance. For a single mode Gaussian system, the quadratures are always uncorrelated because they are orthogonal so they appear with zero covariance (information of one quadrature destroys the information of it's conjugate quadrature). Correlations appear when we have a multi-mode state, a two mode state has the following form:

$$\Sigma = \begin{array}{c} \begin{matrix} \hat{q}_1 & \hat{p}_1 & \hat{q}_2 & \hat{p}_2 \end{matrix} \\ \begin{pmatrix} V(\hat{q}_1) & C(\hat{q}_1,\hat{p}_1) & C(\hat{q}_1,\hat{q}_2) & C(\hat{q}_1,\hat{p}_2) \\ C(\hat{p}_1,\hat{q}_1) & V(\hat{p}_1) & C(\hat{p}_1,\hat{q}_2) & C(\hat{p}_1,\hat{p}_2) \\ C(\hat{q}_2,\hat{q}_1) & C(\hat{q}_2,\hat{p}_1) & V(\hat{q}_2) & C(\hat{q}_2,\hat{p}_2) \\ C(\hat{p}_2,\hat{q}_1) & C(\hat{p}_2,\hat{p}_1) & C(\hat{p}_2,\hat{q}_2) & V(\hat{p}_2) \end{pmatrix} \end{array} \begin{matrix} \hat{q}_1 \\ \hat{p}_1 \\ \hat{q}_2 \\ \hat{p}_2 \end{matrix} \tag{2.3.3}$$

The term $C(\hat{q}_1,\hat{q}_2)$ is not necessarily zero. This develops a correlation between mode-1 and mode-2 such that any change in $\hat{q}_1$ affects the distribution of $\hat{q}_2$. We illuminates this statement when we formulate covariance matrices of different Gaussian states but first we discuss the measurement methods in CV QKD.

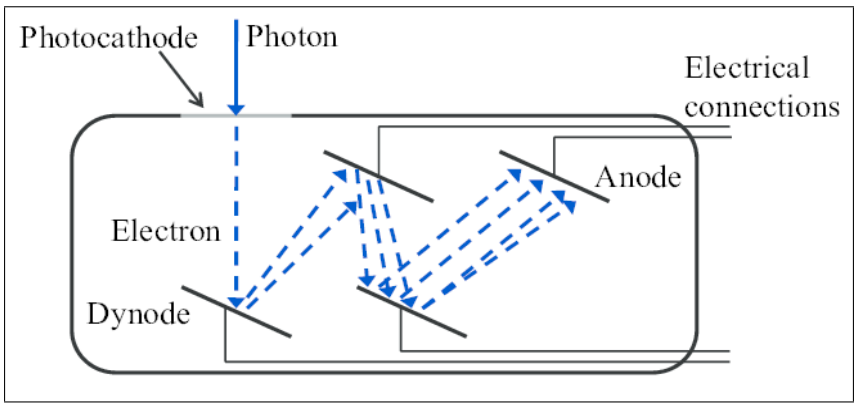


Figure 2.4.1: The single photon is converted into an electrical signal that is amplified by using multiple dynodes until the outgoing current is large enough to measure with standard electrical devices [7]

2.4 Measuring Gaussian States

We will now restrict ourselves to optical continuous variables i.e. our state is prepared by modulating the quadratures of light. Bob can retrieve this quantum information by measuring position, momentum or both quadratures of the incoming pulses of light. As discussed previously, one of the primary advantages with CV is that we can use off-the-shelf coherent telecom devices, one of such device is called a homodyne detector.

Let us start by first understanding single photon detectors. Detecting one single photon directly can be challenging so a clever method was devised that uses an indirect approach to detect a photon. Observe from Figure 2.4.1, when a single photon strikes a photocathode, it ejects a single electron. Again, measuring a single electron would be equally challenging so this signal is amplified by projecting this electron on a dynode. The dynode intakes one electron and ejects two to three electrons, this process is repeated a few times until there is enough current to measure.

If more than one photons strike the initial photocathode, it ejects more than one electron which multiply exponentially so the final signal has much more current than what a single photon can produce. This method gives protection against multi-photon signals.

The down side of this detector is that the photocathode may not eject an electron every time, even when it does the electron may not always land on the dynode. This heavily affects the efficiency of a single photon detector.

Now let's look at a homodyne detector in Figure 2.4.2. The homodyne detector mixes the incom-

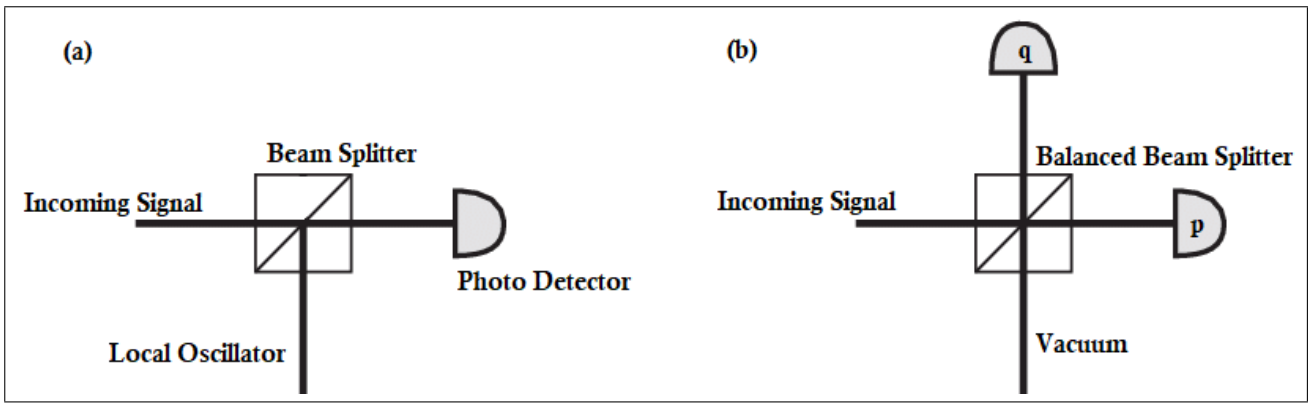


Figure 2.4.2: (a) Schematic setup of a homodyne detector (b) Schematic setup of a dual-homodyne/heterodyne detector. The label q and p in (b) refers to an individual homodyne detector, as depicted in (a), measuring that respective quadrature.

ing quantum signal with a classical signal generated by a *local oscillator*[1]. The phase of the local oscillator can be adjusted depending on the choice of quadrature that needs to be measured. This method amplifies the incoming signal making it easy to measure using a simple photo detector.

To understand the mathematics of this process, we first introduce semi-classical/coherent states of light. These states exhibit classical as well as quantum behaviour. By definition, the eigen states of annihilation operator are called coherent states:

$$\hat{a}\,|\alpha_i\rangle = \alpha_i\,|\alpha_i\rangle \qquad\qquad \langle\alpha_i|\,\hat{a}^\dagger = \langle\alpha_i|\,\alpha^*$$

From (2.1.1), $\hat{a}$ is defined as $\frac{1}{2}(\hat{q} + i\hat{p})$ which gives $\alpha = q + ip = |\alpha|e^{i\theta}$. α represents the classical half of coherent states because it is not an operator. If we now take a quantum coherent signal and mix it with this purely classical signal using a beam splitter, we get the following:

$$B\begin{pmatrix}\hat{a}\\ \alpha\end{pmatrix} = \begin{pmatrix}\frac{1}{\sqrt{2}}(\hat{a}+\alpha)\\ \frac{1}{\sqrt{2}}(-\hat{a}+\alpha)\end{pmatrix} = \begin{pmatrix}\zeta_1\\ \zeta_2\end{pmatrix}$$

Where B is a balanced (50:50) beam splitter given in matrix form as:

$$B = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ -1 & 1\end{pmatrix}$$

[1]Local oscillator refers to a classical signal sent alongside the quantum signal. It carries no information about the quadratures values of the quantum signal but only carries information about the phase of the sent quantum signal. Local oscillator is also referred as a phase reference signal. Bob has to separate the local oscillator signal from the quantum signal before using it.

The number-difference operator for the above output of the beam splitter becomes:

$$\begin{aligned}\Delta\hat{n} &= \zeta_1^\dagger\zeta_1 - \zeta_2^\dagger\zeta_2 \\ &= \frac{1}{2}(\hat{a}^\dagger\hat{a} + \alpha^*\alpha + \alpha\hat{a}^\dagger + \alpha^*\hat{a})(\hat{a}^\dagger\hat{a} + \alpha^*\alpha - \alpha\hat{a}^\dagger - \alpha^*\hat{a}) \\ &= \alpha\hat{a}^\dagger + \alpha^*\hat{a}\end{aligned} \tag{2.4.1}$$

Substituting $\alpha = |\alpha|e^{i\theta}$:

$$\begin{aligned}\Delta\hat{n} &= |\alpha|\big(\hat{a}^\dagger e^{i\theta} + \hat{a}e^{-i\theta}\big) \\ &= \frac{|\alpha|}{2}\big((\hat{q} - i\hat{p})e^{i\theta} + (\hat{q} + i\hat{p})e^{-i\theta}\big) \\ &= \frac{|\alpha|}{2}\big(\hat{q}(e^{i\theta} + e^{-i\theta}) + i\hat{p}(-e^{i\theta} + e^{-i\theta})\big) \\ &= |\alpha|\big(\hat{q}\text{cos}(\theta) + i\hat{p}\text{sin}(\theta)\big)\end{aligned} \tag{2.4.2}$$

Recall that θ is the phase of the classical signal w.r.t the incoming signal. In case of homodyne detectors, it is the phase of the local oscillator. We can then control this phase to amplify the quadrature we want to measure. $\theta = 0$ measure position while $\theta = \frac{\pi}{2}$ measure momentum. Note that we have this relation for the number difference operator, the number difference operator is proportional to photodetector current so we only measure a current when we amplify the right quadrature amplification.

We can also perform a heterodyne detection (also called dual-homodyne detection) by first splitting the incoming signal into two equal signals via a balanced beam splitter then sending one half to a homodyne detector with $\theta = 0$ and the other half to a homodyne detector with $\theta = \frac{\pi}{2}$.

The advantage of heterodyne detection is that it measures both quadratures. This is useful when estimating channel parameters as it reduces the information Eve holds. On the other hand, it introduces more noise because the amplitude of the signal falls when we split it into two signals. Since the measuring signals have an intrinsic noise of 1 SNU because of the uncertainty principle, this translates to twice the intrinsic noise when measuring both quadratures.

In most CV QKD protocols, it is assumed that Alice sends a reference phase (local oscillator signal) alongside her quantum signal which is used by Bob as a classical signal to amplify the measurement quadrature. It has been shown that Eve is capable of tampering this reference phase exploiting a security loophole [23, 25]. Although it is required by unconditional security to give protection against such attacks but these reference phase attacks are not in the scope of this thesis primarily because pro-

tection against these attacks does not directly depend on the QKD scheme but the technological setup that is being used.

2.4.1 Partial Measurements

In a QKD protocol, it is possible that a step requires measurement on part of the complete system which can affect the residual system. In Gaussian quantum information processing, we work with the covariance matrix so a partial measurement on this covariance matrix affects the whole system as given below [27]:

$$\begin{aligned} &\textbf{Partial Homodyne Transformation:} && \mathbf{V} = \mathbf{A} - \mathbf{C}\big(\mathbf{\Pi}_{\{q,p\}}\mathbf{B}\mathbf{\Pi}_{\{q,p\}}\big)^{-1}\mathbf{C}^T \\ &\textbf{Partial Heterodyne Transformation:} && \mathbf{V} = \mathbf{A} - \mathbf{C}\big(\mathbf{B} + \mathbf{I}\big)^{-1}\mathbf{C}^T \end{aligned} \tag{2.4.3}$$

Given that:

$$\mathbf{V} = \begin{bmatrix} \mathbf{A}_{n\times n} & \mathbf{C}_{n\times 2} \\ \mathbf{C}_{2\times n} & \mathbf{B}_{2\times 2} \end{bmatrix} \qquad \mathbf{\Pi}_q = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \qquad \mathbf{\Pi}_p = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \qquad \mathbf{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$\mathbf{V}$ represents the covariance matrix that undergoes partial transformation, $\mathbf{\Pi}$ is a projective matrix that depends on the choice of quadrature measured, $\mathbf{I}$ is the identity matrix. The term $\big(\mathbf{\Pi}_{\{q,p\}}\mathbf{B}\mathbf{\Pi}_{\{q,p\}}\big)^{-1}$ is not an inverse but rather a pseudo inverse also called Moore-Penrose inverse.

The dimension of $\mathbf{B}$ is always 2x2. This is because each partial measurement is performed on one mode which is made up of the variances of q, p and their covariance. It is important to note that if a protocol performs multiple partial measurements, we do it sequentially because one partial measurement can affect the result of the other.

2.5 Covariance Matrices of different Gaussian States

In this section we will derive most of the fundamental covariance matrices used in CV QKD protocols. Almost all other matrices are derived by modifying a small part of these matrices.

2.5.1 Vacuum State

Vacuum states are defined as fock states with zero photons ($\bar{n} = 0$). This makes vacuum states the lowest allowed Gaussian state. The density matrix of such a state is given as $\rho = |0\rangle \langle 0|$. We can now use (2.3.1) to get the expectation values:

$$\langle \hat{q} \rangle = Tr(\hat{q}\rho) = Tr\big((\hat{a} + \hat{a}^\dagger)\rho\big) = Tr\big(\hat{a} |0\rangle \langle 0| + \hat{a}^\dagger |0\rangle \langle 0|\big) = Tr(|1\rangle \langle 0|) = \sum_j \langle j|1\rangle \langle 0|j\rangle = 0$$

$$\langle \hat{p} \rangle = Tr(\hat{p}\rho) = Tr\big(i(\hat{a}^\dagger - \hat{a})\rho\big) = Tr\big(i\hat{a}^\dagger |0\rangle \langle 0| - i\hat{a} |0\rangle \langle 0|\big) = Tr(i |1\rangle \langle 0|) = i\sum_j \langle j|1\rangle \langle 0|j\rangle = 0$$

Evaluating the variance using $\hat{a}^\dagger\hat{a} + 1 = \hat{a}\hat{a}^\dagger$ and $\hat{n} = \hat{a}^\dagger\hat{a}$:

$$V_{11} = \frac{1}{2}\langle \Delta\hat{q}\Delta\hat{q} \rangle = \frac{1}{2}\langle \hat{q}\hat{q} + \hat{q}\hat{q} \rangle = \langle \hat{q}^2 \rangle = \langle 0| (\hat{a} + \hat{a}^\dagger)^2 |0\rangle \tag{2.5.1}$$

$$= \langle 0| \hat{a}\hat{a} |0\rangle + \langle 0| \hat{a}^\dagger\hat{a}^\dagger |0\rangle + 2 \langle 0| \hat{n} |0\rangle + \langle 0|0\rangle = 1 \tag{2.5.2}$$

$$V_{22} = \frac{1}{2}\langle \Delta\hat{p}\Delta\hat{p} \rangle = \frac{1}{2}\langle \hat{p}\hat{p} + \hat{p}\hat{p} \rangle = \langle \hat{p}^2 \rangle = \langle 0| (i\hat{a}^\dagger - i\hat{a})^2 |0\rangle \tag{2.5.3}$$

$$= - \langle 0| \hat{a}^\dagger\hat{a}^\dagger |0\rangle - \langle 0| \hat{a}\hat{a} |0\rangle + 2 \langle 0| \hat{n} |0\rangle + \langle 0|0\rangle = 1 \tag{2.5.4}$$

$$V_{21} = V_{12} = \frac{1}{2}\langle \Delta\hat{q}\Delta\hat{p} \rangle = \frac{1}{2}\langle \hat{q}\hat{p} + \hat{p}\hat{q} \rangle = \frac{1}{2} \langle 0| (\hat{a} + \hat{a}^\dagger)(i\hat{a}^\dagger - i\hat{a}) + (i\hat{a}^\dagger - i\hat{a})(\hat{a} + \hat{a}^\dagger) |0\rangle \tag{2.5.5}$$

$$= \frac{1}{2} \langle 0| - 2i\hat{a}\hat{a} + 2i\hat{a}^\dagger\hat{a}^\dagger |0\rangle = 0$$

With these values, we can write the covariance matrix:

$$\mathbf{\Gamma_{vacuum}} = \begin{bmatrix} V_{11} & V_{12} \\ V_{21} & V_{22} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad Mean = (0, 0) \tag{2.5.6}$$

So the covariance matrix for a vacuum state is the identity matrix. Later we will see that modes that suffer channel loss approach the identity matrix hence representing a lost signal.

2.5.2 Displaced Coherent State

As formulated above, coherent states are the eigen states of annihilation operator. Using $\alpha = q + ip$, we can derive their covariance matrix:

$$V_q \geq \langle\alpha|\hat{q}^2|\alpha\rangle - \langle\alpha|\hat{q}|\alpha\rangle^2 \qquad V_p \geq \langle\alpha|\hat{p}^2|\alpha\rangle - \langle\alpha|\hat{p}|\alpha\rangle^2$$

$$V_q \geq \langle\alpha|(\hat{a} + \hat{a}^\dagger)^2|\alpha\rangle - \langle\alpha|\hat{a} + \hat{a}^\dagger|\alpha\rangle^2 \qquad V_p \geq \langle\alpha|(i\hat{a}^\dagger - i\hat{a})^2|\alpha\rangle - \langle\alpha|i\hat{a}^\dagger - i\hat{a}|\alpha\rangle^2$$

$$V_q \geq (\alpha^2 + (\alpha^*)^2 + \qquad V_p \geq (i^2\alpha^2 + i^2(\alpha^*)^2 -$$

$$\alpha^*\alpha + 1 + \alpha^*\alpha) + (\alpha + \alpha^*)^2 \qquad i^2\alpha^*\alpha - i^2 - i^2\alpha^*\alpha) + (i\alpha - i\alpha^*)^2$$

$$V_q \geq 1 \qquad V_p \geq 1$$

So the variances of the quadratures are equal to 1 for the case of minimum uncertainty i.e. $\delta_q\delta_p = 1$. We will later observe the effect of intrinsic noise greater than 1.

A displaced coherent state can be prepared by applying the displacement operator on vacuum sate. Since the variance of coherent states is 1 for minimum quantum noise, a displaced coherent state will have a variance of 1 but with a non zero mean value. These states are also called displaced vacuum states.

$$\hat{D}(\alpha)\,|0\rangle = |\alpha\rangle$$

$$\mathbf{V} = \hat{D}(\alpha)\,|0\rangle\,\langle 0|\,\hat{D}(\alpha)^\dagger$$

Where $\hat{D}(\alpha) = exp(\alpha\hat{a}^\dagger - \alpha^*\hat{a})$ is called the coherent displacement operator.

$$\mathbf{\Gamma_{coherent-displaced}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad\qquad Mean = (q, p)$$

Note that the variance of both quadratures is same because coherent states are not squeezed so both quadratures carry the same preparation variance.

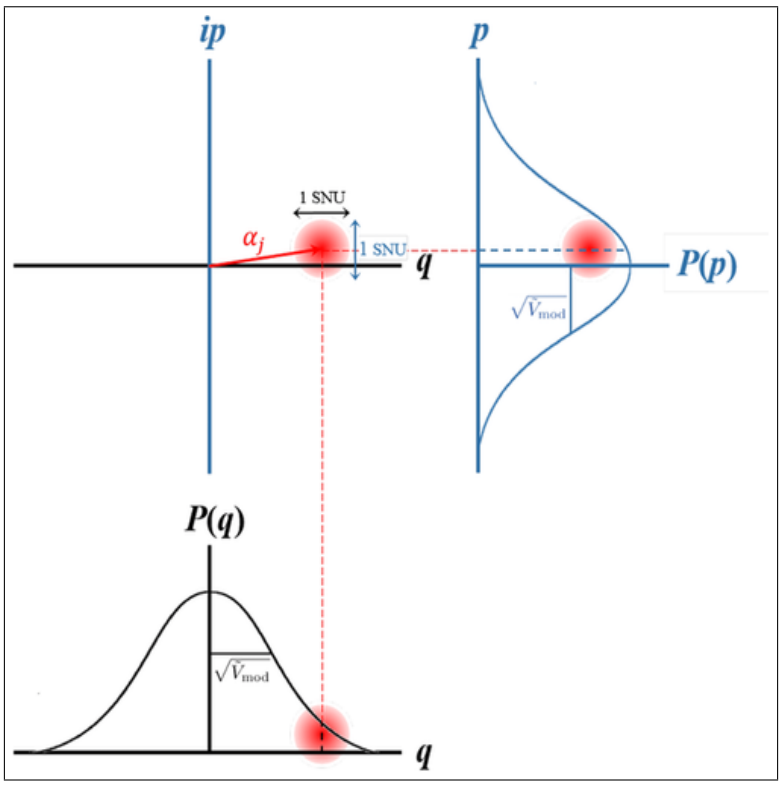


Figure 2.5.1: Phase space representation of Gaussian modulated coherent state $|\alpha_j\rangle$ with a variance of 1 shot noise unit and a non-zero mean value [16]

2.5.3 Thermal States

Thermal states are identical to vacuum states, the only different is that vacuum states carry the lowest allowed noise as their variance, thermal states have a variance greater than zero. Covariance matrix of such a state is complex when represented in terms of creation and annihilation operators, so a much simplified approach is when we represent the variance as a value called preparation variance (also called modulation variance) representing the variance of the quadrature that has been prepared: $V(\hat{q}, \hat{p}) = V_{mod}$.

This modulation variance is distributed into two factors, the state variance V and the intrinsic noise V_o so we get $V_{mod} = V + V_o$. Note that we are formulating these equations for the variance of quadrature operators and not quadrature values: $V(\hat{q}) \neq V(q)$.

$$\mathbf{\Gamma_{thermal}} = \begin{pmatrix} V & 0 \\ 0 & V \end{pmatrix} \qquad\qquad Mean = (0, 0)$$

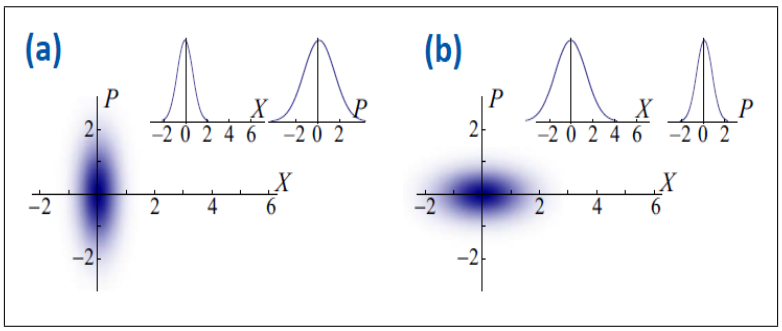


Figure 2.5.2: Phase space representation of (a) Position squeezed light and (b) Momentum squeezed light [17]

2.5.4 One and Two mode Squeezed Vacuum States

Squeezed states are states produced when the variance of one of the quadrature exceeds the allowed quantum limit of 1 SNU. This can be intuitively understood by the uncertainty relation directly. looking at $\Delta\hat{q}\Delta\hat{p} \geq 1$ if we make a precise measurement of the position of a quantum system, the momentum will be disturbed proportionally.

In context of continuous variables, we can prepare one of the quadratures of light in such a way that the variance of that quadrature is below vacuum variance while the conjugate quadrature variance increases. Observe from Fig. 2.5.2, the condition on squeezing is that the uncertainty product between $\hat{q}$ and $\hat{p}$ can never be less then 1.

The most commonly used method is spontaneous parametric down conversion (SPDC) that uses non-linear optics to squeeze light. In this method, a photon of a powerful laser field is injected into a second order non-linear crystal. It spontaneously reduces to a pair of photons with lower energy. This method can be degenerate, in which case it generates a single mode squeezed vacuum state, or it can be non-degenerate where it produces a two mode squeezed vacuum state.

Mathematically, a squeezed state is generated by applying a squeezing operator on the state. For a single mode, the squeezing operator takes the following form in Hilbert space:

$$\hat{S}(r) = exp\Big(\frac{r}{2}(\hat{a}^2 - \hat{a}^{\dagger 2})\Big)$$

Where r is the squeezing parameter related to the variance via a factor λ:

$$V = \frac{1+\lambda^2}{1-\lambda^2} \qquad\qquad r = \tanh^{-1}(\lambda) \tag{2.5.7}$$

As discussed previously, the quadratures of the state on which we apply the squeezing operator follow the symplectic map i.e. $\{\hat{q}, \hat{p}\} \rightarrow \hat{\mathbf{S}}(r)\{\hat{q}, \hat{p}\}$ which gives us the following symplectic operator:

$$\mathbf{S}(r) = \begin{pmatrix} e^{-r} & 0 \\ 0 & e^{r} \end{pmatrix}$$

If we apply this squeezing operator on vacuum, we get the following covariance matrix called a Single-mode squeezed vacuum state:

$$\mathbf{\Gamma_{SMSV}} = \begin{pmatrix} e^{-2r} & 0 \\ 0 & e^{2r} \end{pmatrix} \qquad\qquad Mean = (0, 0)$$

For a two-mode squeezed vacuum state we apply the two-mode squeezing operator defined as:

$$\hat{\mathbf{S}}_{\mathbf{2}}(r) = exp\Big(\frac{r}{2}(\hat{a}\hat{b} - \hat{a}^{\dagger}\hat{b}^{\dagger})\Big)$$

Where $\hat{a}^{\dagger}$ is the creation operator in Hilbert space $\mathscr{H}_A$ and $\hat{b}^{\dagger}$ is the creation operator in Hilbert space $\mathscr{H}_B$. When applied to a two mode vacuum (vacuum in each individual Hilbert space), the operation forms the two-mode squeezed vacuum (TMSV) state which has the same general structure given in (2.3.3):

$$\begin{aligned} |\psi\rangle_{TMSV} &= \hat{\mathbf{S}}_{\mathbf{2}}(r)\,|0_A 0_B\rangle \\ &= \sqrt{1-\lambda^2}\; e^{\lambda \hat{a}^{\dagger}\hat{b}^{\dagger}}\,|0_A 0_B\rangle \end{aligned}$$

Since the state is not displaced from the vacuum but only squeezed, the mean of such a state is zero. The covariance matrix can be formed by using equation (2.3.1). The detailed calculation is given in Appendix A:

$$\mathbf{\Gamma_{TMSV}} = \begin{pmatrix} V & 0 & \sqrt{V^2-1} & 0 \\ 0 & V & 0 & -\sqrt{V^2-1} \\ \sqrt{V^2-1} & 0 & V & 0 \\ 0 & -\sqrt{V^2-1} & 0 & V \end{pmatrix} \qquad Mean = (0, 0) \qquad (2.5.8)$$

We will often use the compact form of Γ_{TMSV}:

$$\Sigma = \begin{pmatrix} V\,\mathbb{1} & \sqrt{V^2-1}\,\sigma_z \\ \sqrt{V^2-1}\,\sigma_z & V\,\mathbb{1} \end{pmatrix} \qquad \mathbb{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{2.5.9}$$

TMSV state is the continuous variable representation of an EPR state (the maximally entangled state). This will be discussed in detail when talk about entanglement schemes in CV QKD.

2.5.5 Modeling Gaussian Quantum Channel

Before we start our discussion on CV protocols for QKD, we need to model the channel in which our states travel. The main requirement is that the channel maintains the Gaussian nature of our states i.e. the channel operation is Gaussian. There are two types of Gaussian channels, **pure-loss/bosonic-loss channels** and **thermal loss channels**. Pure loss channels are the channels where we don't consider thermal noises, these channel are easy to model where we simply apply a beam splitter loss on the signal state. This can be done by mixing the incoming signal with a vacuum input which delineates our model for bosonic loss states (shown in Figure 2.5.3). Let us implement this model on a TMSV state:

$$\Sigma' = \hat{B}(\tau_c)\Sigma\hat{B}^T(\tau_c)$$

$$\Sigma = \begin{pmatrix} V\,\mathbb{1} & \sqrt{V^2-1}\,\sigma_z & 0 \\ \sqrt{V^2-1}\,\sigma_z & V\,\mathbb{1} & 0 \\ 0 & 0 & \mathbb{1} \end{pmatrix}$$

$$\hat{B}(\tau_c) = \begin{pmatrix} \mathbb{1} & 0 & 0 \\ 0 & \sqrt{\tau_c}\,\mathbb{1} & \sqrt{1-\tau_c}\,\mathbb{1} \\ 0 & -\sqrt{1-\tau_c}\,\mathbb{1} & \sqrt{\tau_c}\,\mathbb{1} \end{pmatrix}$$

After applying these operations, we are left with:

$$\Sigma' = \begin{pmatrix} V & \sqrt{\tau_c(V^2-1)} & -\sqrt{(1-\tau_c)(V^2-1)} \\ \sqrt{\tau_c(V^2-1)} & (\tau_c V + 1 - \tau_c) & \sqrt{\tau_c(1-\tau_c)}(1-V) \\ -\sqrt{(1-\tau_c)(V^2-1)} & \sqrt{\tau_c(1-\tau_c)}(1-V) & (1-\tau_c)V + \tau_c \end{pmatrix}$$

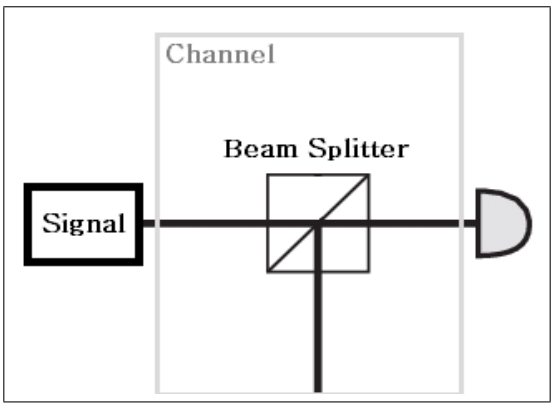


Figure 2.5.3: Schematics of a Gaussian pure loss channel. The outgoing mode from Alice splits with a vacuum mode. Part of the signal is lost and the remaining signal goes to Bob. The process depicts a lossy Gaussian channel.

Note that all entries have a $\mathbb{1}_{2\times 2}$ matrix that we have omitted for simplicity, the dimension of $\Sigma^{'}$ is currently 6x6.

The 3^{rd} row and column is the ancillary system (the environment) that is disposed, so we remove that part and we are left with the matrix shared by Alice and Bob:

$$\Sigma^{'} = \begin{pmatrix} V\,\mathbb{1} & \sqrt{\tau_c(V^2-1)}\,\sigma_z \\ \sqrt{\tau_c(V^2-1)}\,\sigma_z & (\tau_c V + 1 - \tau_c)\,\mathbb{1} \end{pmatrix} \tag{2.5.10}$$

The most interesting take from this covariance matrix is in the long distance regime, where $\tau_c \to 0$, Bob's mode $\propto \tau_c(V-1)+1$ approaches 1. This directly translates to an approaching vacuum mode which further translates to lost signal/no photons received.

If instead of a vacuum input at the channel beam splitter, we input a thermal state with variance $W \equiv 1 + \frac{\xi}{1-\tau_c}$ defined in a standard way [2], we can model the thermal loss channel. We do the same process above but now we use this thermal state:

$$\Sigma^{'} = \begin{pmatrix} V\,\mathbb{1} & \sqrt{\tau_c(V^2-1)}\,\sigma_z \\ \sqrt{\tau_c(V^2-1)}\,\sigma_z & (\tau_c V - \tau_c + 1 + \xi)\,\mathbb{1} \end{pmatrix} \tag{2.5.11}$$

Note the new factor ξ, it represents loss accumulated by preparing devices, detecting devices, bad calibrations and electronic noises from converting the signal to digital signal. For unconditional security of any protocol, we say that all forms of loss are credited to Eve's information gain.

[2]This definition of environmental variance accommodates channel as well as extra losses primarily generated by inefficient detectors, inefficient sources and electronic noise. Refer to [16] for an in-depth explanation.

We are mostly interested in distance rather than transmissivity so we use the following formula to convert transmissivity of the channel to length of the channel:

$$L = 10^{\frac{-\alpha\tau_c}{10}} \tag{2.5.12}$$

α is the attenuation of loss incurred by the quantum signal as it travels through the Gaussian channel which is measured in decibels per kilometer (db/km). To put an upper bound on a protocol's performance, we assume a Gaussian wave prepared at a wavelength of $\approx 1550nm$ which, for best quality optical fibers, can reduce loss attenuation as low as 0.20 db/km so for our simulations we will fix $\alpha = 0.20$. These type of channels are referred in literature as **fixed attenuation channels** contrary to **fading channels** which are used to model free-space QKD, we will only consider fixed attenuation channels in this thesis.

Chapter 3

Practicality of a protocol

In context of continuous variables, we require that the ensemble of quantum states we use in our protocols can be reduced to a thermal state. This is because thermal states carry the same variance for both quadratures hence making them indistinguishable for an eavesdropper.

3.1 Understanding Prepare and Measure Schemes

When the case of quantum key distribution is studied, the simplest implementation is a prepare and measure scheme; Alice prepares a locally generated classical data, encodes that classical information on a quantum state and sends it to Bob who makes a measurement hence collapsing the state. Any eavesdropping on the quantum state is protected by Heisenberg's uncertainty principle. Following are two protocols designed on a prepare and measure scheme.

3.1.1 Single Mode Squeezed State Protocol

A protocol that uses infinitely squeezed states can be reduced to the BB84 protocol. Since infinite squeezing is not practically achievable, we have to design protocols that work with finite squeezing. This protocol was first proposed in [3] and it is as follows:

- Alice generates a random (Gaussian distributed) variable κ which is centered on zero and have a variance V_κ. She also generates a random bit $b \in \{0, 1\}$
- She then prepares a single mode squeezed vacuum state and displaces it according to κ hence preparing a position/momentum squeezed state based on the result of b, with a modulation

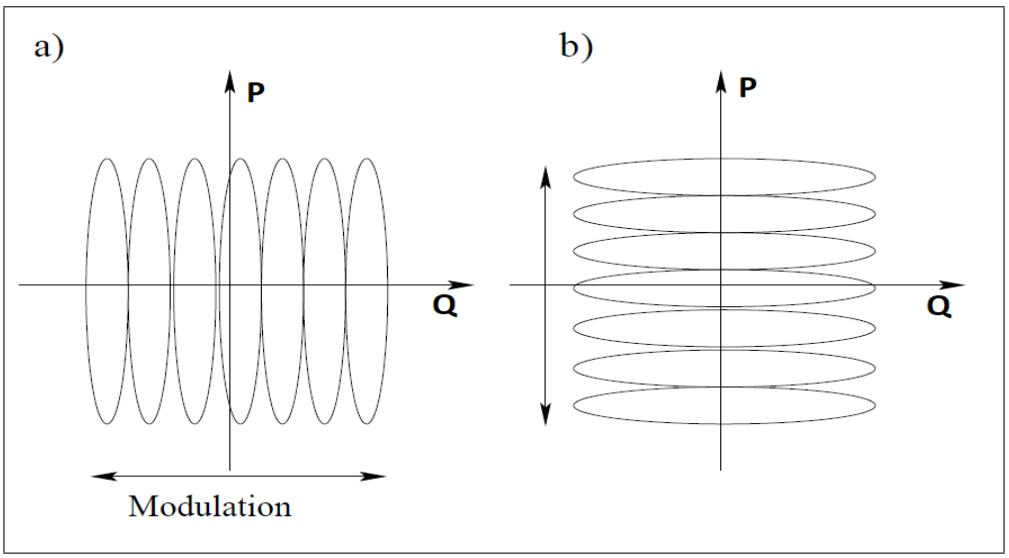


Figure 3.1.1: Phase space representation of a single mode (a) position squeezed vacuum state and (b) momentum squeezed vacuum state after applying a modulation

variance of V_κ (Figure 3.1.1)

- The state is then transmitted to Bob via a quantum channel who measures the state based on a locally generated random variable $\tilde{b} \in \{0, 1\}$

- The protocol then follows a two step post-processing: (1) Alice discloses her value of b for each pulse via an authenticated classical channel[1] (2) Bob keeps only the ones where $b = \tilde{b}$

Say Alice prepared a q-squeezed state, if she imposes the following condition on her state:

$$e^{-2r} + V_\kappa = e^{2r}$$

the output state becomes a thermal state indistinguishable from a state made with a mixture of p-squeezed states:

$$\mathbf{\Gamma}_\kappa = \begin{pmatrix} e^{-2r} + V_\kappa & 0 \\ 0 & e^{2r} \end{pmatrix} = \begin{pmatrix} e^{-2r} & 0 \\ 0 & e^{2r} + V_\kappa \end{pmatrix} = \begin{pmatrix} V & 0 \\ 0 & V \end{pmatrix}.$$

[1] Authenticated classical channel refers to a classical channel that is accessible to everyone. Anyone can read the data flowing through it but no one can rewrite it.

3.1.2 Coherent State Protocol

Coherent state protocols are the most practical protocols in continuous variable QKD. The idea is that we can reduce an ensemble average of Gaussian coherent states to a thermal state. The protocol follows as below:

- Alice generates two random (independent Gaussian distributed) variable (κ_q, κ_p) with a variance V_κ
- She then prepares a coherent state centered on (κ_q, κ_p) and sends it to Bob
- Bob performs a Homodyne measurement on (q, p) based on a locally generated random bit $(0, 1)$.
- Once Bob receives all of the pulses, he discloses the value of his random bit for each pulse and Alice keeps (κ_q, κ_p) based on the measurement of Bob.

The last part of the protocol involves sifting the key and amplifying privacy by using hashing algorithms. If Alice sets her modulation variance as $V_\kappa = V - 1$, it allows her to reduce her coherent state to a thermal state:

$$\mathbf{\Gamma}_\kappa = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} V_\kappa + 1 & 0 \\ 0 & V_\kappa + 1 \end{pmatrix} = \begin{pmatrix} V & 0 \\ 0 & V \end{pmatrix}.$$

3.2 Understanding Entanglement Based Schemes

In an entanglement scheme, Alice does not generate any local classical data to encode, instead she uses an EPR state to share data with Bob. Since EPR/TMSV state are correlated (as seen in (2.5.8)) any operation on one mode will change the measurement outcome of the other mode. Experimentally producing TMSV states is challenging but most protocols employ entanglement scheme. The reason is because we can virtually reduce an entanglement scheme to a prepare and measure scheme. The advantage of entanglement scheme is its much simplified security analysis for the type of attacks involved in CV QKD. We discuss this entanglement based QKD scheme that uses TMSV state as the entanglement resource below. It is a summary of the original protocol from [10]:

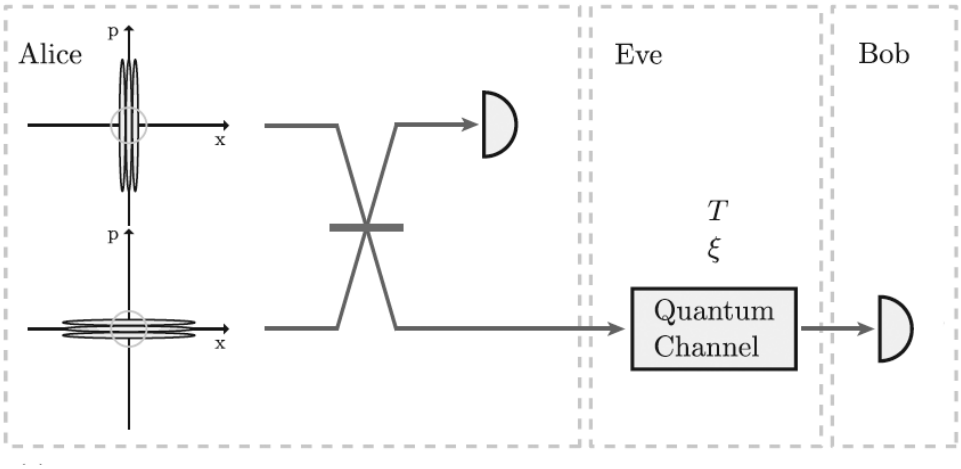


Figure 3.2.1: Setup of a prepare and measure protocol using two-mode squeezed vacuum state as a resource. Alice generates a TMSV state by mixing a position squeezed and momentum squeezed vacuum state on a balanced beam splitter

- Alice prepares a two-mode squeezed vacuum state with variance V as seen in Figure 3.2.1. She keeps one half of the signal and sends the other half to Bob.
- Alice can now measure either one quadrature (homodyne) or both quadratures (heterodyne) of her signal. In each case, the outcome affects the protocol as follows:
  - If Alice **homodynes** her mode, she can measure either position or momentum. Lets assume she measures position, by measuring it she effectively projects the other beam to a q-squeezed beam centered around $(q_A, 0)$. q_A being the measurement outcome of Alice. Similarly, if she measures momentum, the outgoing beam centers around $(0, p_A)$.
  - If Alice **heterodynes** her mode, the outgoing beam reduces to a coherent state centered around (q_A, p_A)
- Regardless of Alice's choice, the protocol than proceeds as before. Bob makes his measurement followed by parameter estimation and error correction.

When Alice decides to measure one quadrature, the outgoing system reduces to a single mode squeezed state where the measured quadrature now has a squeezing equal to $\frac{1}{V}$ (below the standard quantum limit). The residual system now follows the single mode squeezed protocol discussed in section 3.1.1. This is to say that we can reduce the outgoing system to a thermal state as well. The proof for the reduction to coherent state protocol when Alice uses a heterodyne detector is given in

the next section.

The advantage of this scheme is evident. Irrespective of Bob's decision, Alice's decision of measurement completely changed the post processing of Bob's state. In both cases, we can see that the system has reduced to a prepare and measure protocol.

3.2.1 Reduction of EB scheme to coherent PM scheme

The general approach is to design an entanglement based protocol and reduce it to a prepare and measure scheme mathematically, this allows us to test the security of the designed protocol in entanglement scheme while experimentally running the protocol in a prepare and measure scheme.

It can be mathematically shown all entanglement protocols are reducible to prepare and measure protocols [14]. The equivalence of the two schemes for the case of direct transmission is given below. For simplicity, we assume the lowest vacuum noise $V_o = 1$:

$$\Sigma_{PM} = \begin{pmatrix} V_{mod} & 0 & V_{mod} & 0 \\ 0 & V_{mod} & 0 & V_{mod} \\ V_{mod} & 0 & V_{mod}+1 & 0 \\ 0 & V_{mod} & 0 & V_{mod}+1 \end{pmatrix} = \begin{pmatrix} V-1 & 0 & V-1 & 0 \\ 0 & V-1 & 0 & V-1 \\ V-1 & 0 & V & 0 \\ 0 & V-1 & 0 & V \end{pmatrix} \tag{3.2.1}$$

$$\Sigma_{EB} = \begin{pmatrix} V & 0 & \sqrt{V^2-1} & 0 \\ 0 & V & 0 & -\sqrt{V^2-1} \\ \sqrt{V^2-1} & 0 & V & 0 \\ 0 & -\sqrt{V^2-1} & 0 & V \end{pmatrix}$$

Alice starts with an entangled state (Σ_{EB}), sends one mode to Bob while keeping the other mode and applies a balanced beam splitter. This transforms the covariance matrix as follows:

$$\Sigma_{EB} \longrightarrow \hat{U}_{BS}\Big|_{\tau=\frac{1}{2}} \Sigma_{EB}\, \hat{U}_{BS}^{\dagger}\Big|_{\tau=\frac{1}{2}}$$

Where the beam splitter operator $\hat{U}(\tau)$ for Alice's modes is given as follows:

$$\hat{U}_{BS} = \begin{pmatrix} \sqrt{\tau} & \sqrt{1-\tau} & 0 & 0 \\ -\sqrt{1-\tau} & \sqrt{\tau} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Then her covariance matrix becomes:

$$\Sigma_{EB} = \begin{pmatrix} \frac{V+1}{2} & 0 & \sqrt{\frac{1}{2}(V^2-1)} & 0 \\ 0 & \frac{V+1}{2} & 0 & -\sqrt{\frac{1}{2}(V^2-1)} \\ \sqrt{\frac{1}{2}(V^2-1)} & 0 & V & 0 \\ 0 & -\sqrt{\frac{1}{2}(V^2-1)} & 0 & V \end{pmatrix} \tag{3.2.2}$$

Alice then rescales her quadrature operators as follows (directly comparing (3.2.1) and (3.2.2)):

$$\sqrt{\frac{V+1}{2}}\hat{q}^A_{EB} = \sqrt{V-1}\hat{q}^A_{PM}$$

$$\hat{q}^A_{EB} = \sqrt{\frac{V+1}{2(V-1)}}\hat{q}^A_{PM}$$

$$-\sqrt{\frac{V+1}{2}}\hat{p}^A_{EB} = \sqrt{V-1}\hat{p}^A_{PM}$$

$$\hat{p}^A_{EB} = -\sqrt{\frac{V+1}{2(V-1)}}\hat{p}^A_{PM}$$

Alice performs a quadrature rescale as given above before performing a heterodyne measurement. This lets her entanglement based covariance matrix reduce to a coherent prepare and measure covariance matrix.

We will later see the advantage of this equivalence. Some protocols, such as the measurement device independent protocol, can be reduced to a prepare and measure protocol even though they have a very different experimental setup. This allows us to establish the protocol in the entanglement frame to assess its security which is mathematically trivial.

3.3 Eavesdropper's Information

Realistically, a quantum state when sent through a quantum channel inevitably suffers loss which translates to decoherence. This loss/decoherence can be mitigated by applying methods of purification and error corrections which allows the transmission of quantum information reliably. The amount of information lost in a protocol is equal to the amount of information gained by the eavesdropper. The real challenge is to put an upper bound on the information lost not only because of the channel, but also during error correction and privacy amplification. We will form the mathematical framework needed to evaluate this upper bound in this section.

To understand this lost information, we need to understand the notion of 'unconditional' security. It is the requirement of shared information between our primary parties to be protected by the laws of physics hence making it impossible to be intercepted. Unconditional security requires very strong assumptions on what an eavesdropper is capable of so we distribute an eavesdropper's attack strategy into three type (increasing in power given to Eve): individual, collective and coherent attacks.

3.3.1 Individual, Collective and Coherent Attacks

In any of these general attacks, first Eve replaces the whole quantum channel with a completely lossless channel, then she prepares an ancillary system $|E\rangle \langle E|$ which she attaches with Alice's state effectively 'tagging' the signal. Even then performs a unitary operation on the composite system leaving her ancillary system in the following form:

$$\rho = Tr_A\Big(\hat{U}^\dagger \rho_A \otimes |E\rangle \langle E| \hat{U}\Big) \tag{3.3.1}$$

Finally, Eve performs a positive operator values measurement $\mathcal{M} = \{M_j\}$ on the ancillary system which gives her the result j with probability $Tr(M_j\rho)$. For an exchange of n-qubits, this probability becomes a probability density which dictates the upper bound on Eve's information.
For our CV-QKD protocols, the unitary operation in (3.3.1) will be a beam-splitter with a transmissivity set equal to the transmissivity of the channel. This maximizes the amount of information Eve can get through the channel while staying undetected.

The difference between each attack is in the form of Eve's density matrix and her probability distribution. The reason why Individual attacks are considered the weakest is because Eve's density

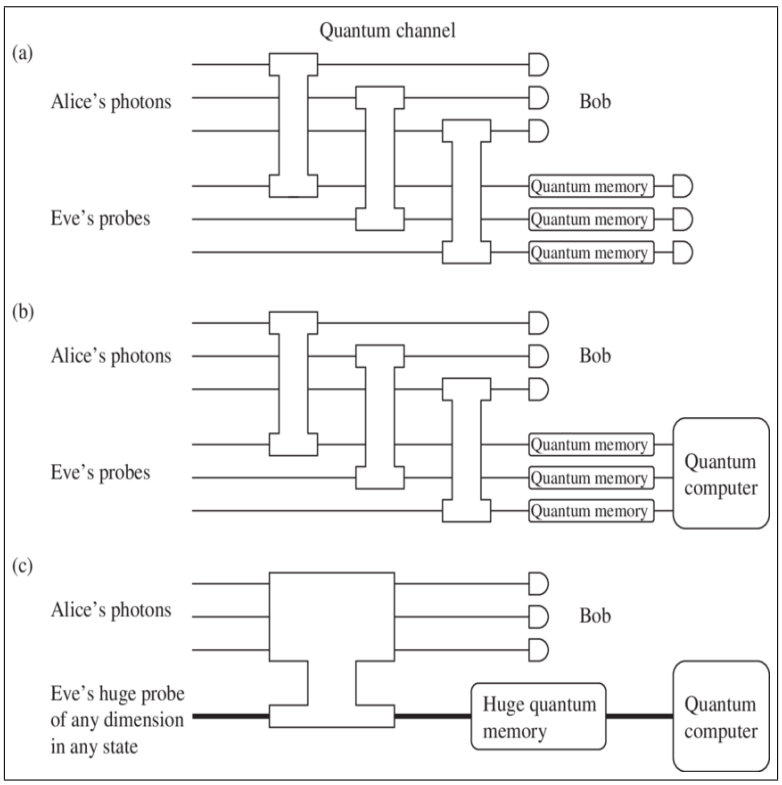


Figure 3.3.1: (a) Individual attack (b) Collective attack (c) Coherent attack [5]

matrix is already separate from the signal state. She stores the tagged states in a quantum memory until measurement basis are announced and then measures them independently. Such an attack cannot extract information from error correction or privacy amplification because Eve cannot develop any correlation between the tagged states as they are separate from each other.

Collective and coherent attacks nullify this advantage Alice and Bob had. In collective attacks, while Eve tags each signal separately, she can process all signals in a quantum computer simultaneously. This allows her to take advantage of correlations introduced during error correction and privacy amplification. Because each signal is tagged individually, Eve cannot develop a correlation between them until after processing them through a quantum computer.

Coherent attacks resolve that as well. Because now Eve has a huge ancillary system that tags all signals, Eve can now develop correlations before measuring and processing them in the quantum computer. This is, by far, the strongest form of eavesdropping.

It is clear from Table 3.3.1 that separating Eve's state from Alice and Bob's shared state in case of general collective and coherent attacks will be a challenge. If we cannot separate her state, we cannot put an upper bound on her information. Fortunately, the solution to this problem takes a fundamental approach from information theory which, for continuous variables, reduces this problem to simple

	Ancilla state	Prob. dist.
Individual	$\rho^i = \mathrm{Tr}_A \left(U^\dagger(\rho_A^i \otimes \lvert E\rangle \ \langle E\rvert)U\right)$	$P_{\mathcal{M}^1}^{\rho^1} \cdots P_{\mathcal{M}^1}^{\rho^n}$
Collective	$\rho^i = \mathrm{Tr}_A \left(U^\dagger(\rho_A^i \otimes \lvert E\rangle \ \langle E\rvert)U\right)$	$P_{\mathcal{M}^n}^{\rho^1 \otimes \cdots \otimes \rho^n}$
Coherent	$\rho = \mathrm{Tr}_A \left(U_G^\dagger((\rho_A^1 \otimes \cdots \otimes \rho_A^n) \otimes \lvert E\rangle \ \langle E\rvert)U_G\right)$	$P_{\mathcal{M}^n}^{\rho}$

Table 3.3.1: The state of Eve's density matrix before measurement and their respective probability distribution

mathematics.

3.4 Shannon's Entropy and Holevo's bound

We now introduce a quantity called *secret key rate* (K). It is the ensemble average of secure bits generated during the protocol by each pulse sent from Alice to Bob.

$$K \geq \beta I(A:B) - I(A:E) \tag{3.4.1}$$

Where $I(A:B)$ is the information shared by Alice and Bob and $I(A:E)$ is the information shared by Alice and Eve. $\beta \in [0,1]$ is called the efficiency of data reconciliation. It is a classical post-processing method where Alice or Bob disclose part of their data to recover the rest. For unconditional security we want our protocols to be secure under coherent attacks. A solution was introduced by Devetak and Winter [4]. Devetak and Winter proved the lower bound on (3.4.1) that is valid for collective attacks in the asymptotic regime [2].

While coherent attacks are still a challenge for most protocols, the current approach to resolve this problem is by using quantum de Finetti theorem which reduces the infinite block size of collective attacks to a limited size valid for coherent attacks. There are postselection techniques as well that reduce the security from coherent to collective at the cost of reduced key rate. Although the security analysis of each protocol is still an open topic, most of the practical protocols have already been proven to withstand coherent attacks.

Let us now discuss the expanse of (3.4.1) without any assumptions on which attack is carried by

[2] Asymptotic regime means that the number of pulses sent by Alice are not limited. In a practical CV-QKD setup, these pulses, also referred to as block size, are at the order of 10^7 pulses per second mostly restricted to this order by computational processing speed

Eve. Alice-Bob and Eve's system can be gives as:

$$\rho_{AB} = Tr_E(\rho_{ABE}) = \sum_{\alpha} \lambda_\alpha \left|\alpha\right\rangle_{AB} \left\langle\alpha\right|_{AB}$$

$$\rho_E = Tr_{AB}(\rho_{ABE}) = \sum_{\alpha} \lambda_\alpha^{'} \left|\alpha\right\rangle_{E} \left\langle\alpha\right|_{E}$$

For Eve to get the most information without being detected, Eve must hold a purification of Alice-Bob system i.e. only Eve can separate their system out of Alice-Bob's system. Because of Schmidt representation used in the above equation, purification implies that $\lambda_\alpha^{'} = \lambda_\alpha$ and Eve's Von Neumann entropy coincides with Alice and Bob's shared state.

The Von Neumann entropy of a mixed state can be written as:

$$S = -\sum_{\alpha} \lambda_\alpha \log(\lambda_\alpha)$$

Following the assumption of purification:

$$S_E = S_{AB} = -\sum_{\alpha} \lambda_\alpha \log(\lambda_\alpha)$$

We can now compute Holevo's information [3]:

$$I(A:E) = S_E - S_{E|A} \tag{3.4.2}$$

$$I(B:E) = S_E - S_{E|B} \tag{3.4.3}$$

The term $S_{E|A}$ represents the information of Eve once Alice has performed a projective measurement and similarly $S_{E|B}$ represents the information when Bob has performed a projective measurement. In our case, these projective measurements are Homodyne or Heterodyne measurements discussed later.

We can see that when proceeding to error correction, one of the parties (Alice or Bob) must disclose their part of information. This is why we have two different relations for Eve's information. It follows that Alice and Bob may decide either to use **Direct Reconciliation** (3.4.2) where Alice sends her bit information to Bob who corrects his information accord to Alice's data, or **Reverse**

[3] Holevo's information is an upper bound on the classical information that can be extracted from an ensemble of quantum states.

Reconciliation (3.4.3) where Bob sends his bit information to Alice who corrects her information accordingly. Reverse reconciliation has shown to perform better than direct reconciliation in high loss channel/long distances [11] so we restrict ourselves to reverse reconciliation.

The scope of this thesis is primarily focused on getting the key rate under collective attacks for different protocols (in the asymptotic regime) with a general approach. The objective is to formulate the covariance matrix for any protocol which will be used to extract the key rate.

3.4.1 Quantum Key Rate

The symplectic formalism is extremely compatible with Von Neumann entropy simplifying a big chunk of our calculations. Lets first evaluate the term S_E in (3.4.3):

$$\begin{aligned} S_E &= -\sum_{\alpha} \lambda_\alpha \log(\lambda_\alpha) \\ &= -Tr_{AB}\big(\rho_{ABE} \log(\rho_{ABE})\big) \end{aligned}$$

The Von Neumann entropy of a Gaussian state ρ can be written in terms of it's symplectic eigen values as [12]:

$$S = \sum_{\kappa=1}^{n} G(v_\kappa)$$

To get the eigen values v we will use the following relation:

$$v = |i\mathbf{\Omega}\mathbf{\Sigma}_{AB}| \geq 1 \tag{3.4.4}$$

Σ_{AB} is the covariance matrix shared by Alice and Bob and:

$$G(x) = \Big(\frac{x+1}{2}\Big)\log_2\Big(\frac{x+1}{2}\Big) - \Big(\frac{x-1}{2}\Big)\log_2\Big(\frac{x-1}{2}\Big)$$

$$\mathbf{\Omega}_{n=2} = \bigoplus_{\kappa=1}^{2} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$$

$\oplus$ represents the direct sum of matrices. It depends on the dimension of the covariance matrix. Since our covariance matrix will always reduce to a 4x4 matrix (1 mode of Alice and mode of Bob) as we

will always develop protocols for a bipartite state so we will take Ω up to $n = 2$.

In most of CV-QKD protocols, the final covariance matrix is in the following standard form:

$$\Sigma_{AB} = \begin{pmatrix} a\mathbb{1} & c\sigma_z \\ c\sigma_z & b\mathbb{1} \end{pmatrix} \qquad \mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{3.4.5}$$

If the covariance matrix is not in the standard form, we can always bring it to the standard form by local squeezing and displacement operations as explained in [6].

If we use this standard form covariance matrix in (3.4.5), we get the following two eigen values when we use (3.4.4):

$$v_{\pm} = \sqrt{\frac{\Delta}{2} \pm \sqrt{\Delta^2 - 4\,\det(\Sigma_{AB})}} \qquad \Delta = a^2 + b^2 - 2c^2 \tag{3.4.6}$$

Using these eigen values, we can evaluate Eve's information before measurement: $S_E = G(v_+) + G(v_-)$.

The second factor $S_{E|B}$ depends on the type of measurement Bob performs. Assuming again that Alice-Bob covariance matrix is in the standard form, we get the following symplectic eigen value for the two possible measurements at Bob's end:

$$\begin{aligned} \textbf{Homodyne Measurement by Bob:} \quad & v = \sqrt{a\Big(a - \Big(\frac{c^2}{b}\Big)\Big)} \\ \textbf{Heterodyne Measurement by Bob:} \quad & v = a - \Big(\frac{c^2}{b+1}\Big) \end{aligned} \tag{3.4.7}$$

Which gives us $S_{E|B} = G(v)$. Using these values in (3.4.3) we get:

$$I(B:E) = G(v_+) + G(v_-) - G(v) \tag{3.4.8}$$

Alice and Bob's mutual information is relatively trivial as all of the values are already present inside the covariance matrix:

$$\textbf{Homodyne Measurement by Bob:} \quad I(A:B)_{hom} = \frac{1}{2}\log_2\Big(V(\hat{x}_B)\Big) - \frac{1}{2}\log_2\Big(V_1(\hat{x}_{B|A})\Big)$$

$$\textbf{Heterodyne Measurement by Bob:} \quad I(A:B)_{het} = \log_2\Big(V(\hat{x}_B)+1\Big) - \log_2\Big(V_2(\hat{x}_{B|A})\Big)$$

$$\begin{aligned} V_1(\hat{x}_{B|A}) &= V(\hat{x}_B) - \frac{|\langle \hat{x}_B \hat{x}_A \rangle|}{V(\hat{x}_A)} \\ V_2(\hat{x}_{B|A}+1) &= V(\hat{x}_B) - \frac{|\langle \hat{x}_B \hat{x}_A \rangle|}{V(\hat{x}_A)+1} \end{aligned} \tag{3.4.9}$$

Where $\hat{x} = \{\hat{q}, \hat{p}\}$ are quadrature values for the respective subscript and $V(\hat{x})$ is the variance of that quadrature.

3.4.2 Summarizing the approach for all protocols

We will start by building the covariance matrix of the system Σ, implement the respective Gaussian operations on the covariance matrix and trace out any ancillary system leaving behind a covariance matrix of Alice and Bob Σ_{AB}. We will then check whether the covariance matrix is in the standard form or not. If it is not in the standard form, we bring it to the standard form.

Once we have the final covariance matrix, we evaluate $I(A:B)$ and $I(B:E)$ by using (3.4.9) and (3.4.8) and extract the key rate using:

$$K = \beta I(A:B) - I(B:E) \tag{3.4.10}$$

Chapter 4

Generalized Operations

To work with any dimensional Hilbert spaces, we need to formulate any-dimensional symplectic operations. The generalized operators used in this thesis are given in the following section.

4.1 Beam Splitter

Beam splitter for the input mode i and j in an n-mode system:

$$\hat{B}(\tau) = \begin{pmatrix} 1 & \dots & & & & & \\ \vdots & \ddots & & & & & \\ & & \sqrt{\tau}_i\mathbf{I} & \dots & \sqrt{1-\tau}_{ij}\mathbf{I} & & \\ & & \vdots & & \vdots & & \\ & & -\sqrt{1-\tau}_{ji}\mathbf{I} & \dots & \sqrt{\tau}_j\mathbf{I} & & \\ & & & & & \ddots & \vdots \\ & & & & & \dots & 1 \end{pmatrix} \tag{4.1.1}$$

I is the 2x2 identity matrix. The off diagonal elements, except at $B(\tau)_{ij}$ and $B(\tau)_{ji}$ are zero.

4.2 N-Mode TMSV State

At the start of all entanglement based Gaussian type protocols, we start by generating a big TMSV state that is composed of all the states involved. This would be Alice's state, Bob's state (if any) and

Eve's attack state. The structure of TMSV state generated is as follows:

$$\Sigma_{ABE} = \bigoplus_{i=0}^{n} \sigma_i = \begin{bmatrix} \sigma_0 & & \\ & \ddots & \\ & & \sigma_n \end{bmatrix} \tag{4.2.1}$$

$$\sigma_i = \begin{pmatrix} V_i & 0 & \sqrt{V_i^2-1} & 0 \\ 0 & V_i & 0 & -\sqrt{V_i^2-1} \\ \sqrt{V_i^2-1} & 0 & V_i & 0 \\ 0 & -\sqrt{V_i^2-1} & 0 & V_i \end{pmatrix} = \begin{pmatrix} V_i\,\mathbb{1} & \sqrt{V_i^2-1}\,\sigma_z \\ \sqrt{V_i^2-1}\,\sigma_z & V_i\,\mathbb{1} \end{pmatrix}$$

$$\mathbb{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad\qquad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

n is the total number of TMSV states used in the system.

4.3 Standardization

We will deal with the following standardization whenever needed:

$$\begin{pmatrix} a_1 & 0 & c & 0 \\ 0 & a_2 & 0 & c' \\ c & 0 & b_1 & 0 \\ 0 & c' & 0 & b_2 \end{pmatrix} \xrightarrow{Standardize} \begin{pmatrix} a & 0 & c & 0 \\ 0 & a & 0 & c' \\ c & 0 & b & 0 \\ 0 & c' & 0 & b \end{pmatrix}.$$

Such a transformation can be done by applying squeezing operations on mode 1 and 2 separately. Let us derive the required amount of squeezing for a_1 and a_2 first, we can then use the same relation for b_1 and b_2:

$$\begin{pmatrix} e^{-r} & 0 \\ 0 & e^{r} \end{pmatrix} \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} \begin{pmatrix} e^{-r} & 0 \\ 0 & e^{r} \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

$$\begin{pmatrix} e^{-2r}a_1 & 0 \\ 0 & e^{2r}a_2 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

$$e^{-2r}a_1 = a \qquad\qquad e^{2r}a_2 = a \tag{4.3.1}$$

$$e^{-2r}a_1 = e^{2r}a_2$$

$$e^{-4r} = \frac{a_2}{a_1}$$

$$r = -\frac{1}{4}\ln\left(\frac{a_2}{a_1}\right)$$

we can now form the two mode standardizing matrix as follows:

$$\mathbf{S} = \begin{pmatrix} e^{-\zeta_1} & 0 & 0 & 0 \\ 0 & e^{\zeta_1} & 0 & 0 \\ 0 & 0 & e^{-\zeta_2} & 0 \\ 0 & 0 & 0 & e^{\zeta_2} \end{pmatrix}$$

$$\zeta_1 = -\frac{1}{4}\ln\left(\frac{a_2}{a_1}\right) \qquad\qquad \zeta_2 = -\frac{1}{4}\ln\left(\frac{b_2}{b_1}\right) \tag{4.3.2}$$

Such that we can get:

$$\mathbf{S}\Sigma\mathbf{S}^T = \Sigma_{standard}$$

Chapter 5

Generalized approach to Gaussian CV-QKD protocols

As we have established the equivalence between entanglement schemes and prepare-measure schemes, we will now use TMSV states as the initial resource in every protocol unless said otherwise. Also, we will strictly discuss Gaussian protocols under Gaussian operations only.

5.0.1 Resources

We have simulated our code on Goggle Colab[1] using python. This section uses the following libraries specifically:

Sympy: Used for symbolic computation/algebra. This library has heavily been used to generate our covariance matrix, multiply matrices with variables and compute the key rate.

Matplotlib: This library has been used for 2-D plots.

Numpy: After the form of the matrix is established and we have substituted numerical values, we use Numpy for further calculations because of their computational speed advantage. We also use Numpy's eigen value calculator during the evaluation of the key rate.

A complete code of all functions used is given in Appendix B.

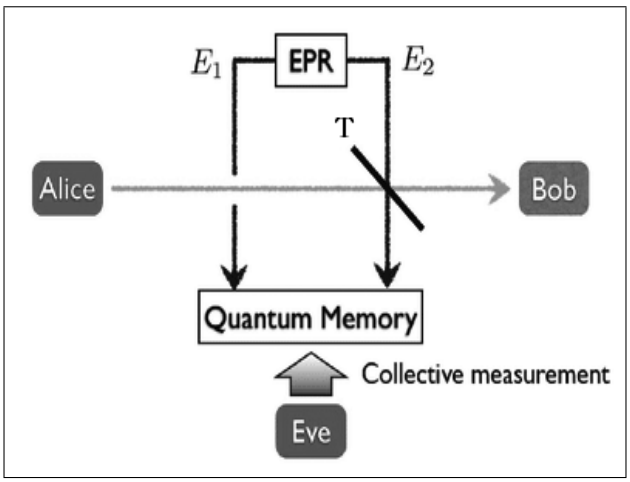


Figure 5.1.1: Eve's entangling cloner attack on Alice's traveling mode. E_1 and E_2 are Eve's EPR modes. She mixes one mode with the signal and keeps the other one unchanged performing a collective measurement at the end.

5.1 Entangling Cloner Attack

This attack is the foundation of generalized collective attacks. As we discussed before, the general attack procedure for Eve is to attach her locally created ancillary system with Alice-Bob pulse to gain information on the signal. This attack gives a mathematical description of what parameters Eve must set to stay hidden while maximizing her information. The schematic is given in Figure 5.1.1, the procedure is identical to (2.5.11) with the only difference being a TMSV input instead of a vacuum input. The protocol is as follows:

- Alice generates a TMSV state. Keeps one mode and sends the other mode to Bob.

- Eve replaces the quantum channel with a completely lossless channel. Eve then creates her TMSV state with a different variance and mixes one mode with Alice's state via a beam splitter with transmissivity τ_e. She then sends both of her modes to a quantum memory for later processing.

- Bob receives Alice's noisy signal and performs either a homodyne or a heterodyne measurement. Once all signals are processed, the protocol moves to post processing

[1] https://colab.research.google.com

Mathematically, we apply a beam splitter of transmissivity T to the initial covariance matrix and remove Eve's modes from the system resulting in a noisy covariance matrix shared by Alice and Bob:

$$\Sigma_{AB} \longrightarrow \left(\mathbb{1}_A \otimes B(T)_{BE_1} \otimes \mathbb{1}_{E_2}\right) \Sigma_{ABE_1E_2} \left(\mathbb{1}_A \otimes B(T)_{BE_1} \otimes \mathbb{1}_{E_2}\right)^T \longrightarrow \Sigma'_{AB}$$

Whereas:

$$\left(\mathbb{1}_A \otimes B(T)_{BE_1} \otimes \mathbb{1}_{E_2}\right) = \begin{pmatrix} \mathbb{1} & 0 & 0 & 0 \\ 0 & \sqrt{T}\,\mathbb{1} & \sqrt{1-T}\,\mathbb{1} & 0 \\ 0 & -\sqrt{1-T}\,\mathbb{1} & \sqrt{T}\,\mathbb{1} & 0 \\ 0 & 0 & 0 & \mathbb{1} \end{pmatrix}$$

$$\Sigma_{ABE_1E_2} = \begin{pmatrix} V\,\mathbb{1} & \sqrt{V^2-1}\,\sigma_z & 0 & 0 \\ \sqrt{V^2-1}\,\sigma_z & V\,\mathbb{1} & 0 & 0 \\ 0 & 0 & W\,\mathbb{1} & \sqrt{W^2-1}\,\sigma_z \\ 0 & 0 & \sqrt{W^2-1}\,\sigma_z & W\,\mathbb{1} \end{pmatrix}$$

V is the variance of Alice's prepared TMSV state while W is the variance of Eve's TMSV state. When we apply these operations and remove Eve's half, we are left with the following covariance matrix shared by Alice and Bob:

$$\Sigma'_{AB} = \begin{pmatrix} V\,\mathbb{1} & \sqrt{T(V^2-1)}\,\sigma_z \\ \sqrt{T(V^2-1)}\,\sigma_z & (TV+W-TW)\,\mathbb{1} \end{pmatrix} \tag{5.1.1}$$

If we directly compare this form with (2.5.11), we can see that if Eve decides to set her variance $W = 1 + \frac{\xi}{1-\tau_c}$ and the transmissivity of here beam splitter $T = \tau_c$, Eve mimics total loss between Alice and Bob. This allows Eve to stay hidden as Alice and Bob will not observe loss over the upper limit they calculated through the distance between them. As previously established, All of this loss translates to information gained by Eve.

With (5.1.1) we are now able to calculate $I(A:B)$ and $I(B:E)$ using (3.4.8) and (3.4.9) and subsequently the key rate using (3.4.10). The code blocks are explained below:

```
primary_pairs_dim = 1
```

```
attack_pairs_dim = 1
cm = CM_TMSV(primary_pairs_dim, attack_pairs_dim)
```

We start by first defining the total number of TMSV states involved in the system. For this protocol, we have 1 TMSV state generated by Alice to share with Bob and 1 generated by Eve to implement her attack. The function **CM_TMSV** follows (4.2.1) to make the covariance matrix of this system.

```
cm = beam_splitter(3,7,t,cm)
cm = mode_M_separator(1,4,1,4,cm)
```

The next step is to apply Eve's beam splitter on Alice's mode traveling through the channel. The function **beam_splitter**, following (4.1.1), applies this operation mixing 2^{nd} mode of Alice and Eve with a transmissivity t. The second function simply picks out a part of the whole covariance matrix. Since we are only interested in Alice and Bob's state, we dispose Eve's modes and only keep the first four rows and columns.

```
err = 0.01
l = 0.8
w = 1 + (err)/(1-t)
v = (1+l**2)/(1-l**2)
cm = cm.subs({"V_1":v,"W_1":w})
```

We can now start defining constants. In this block, we have assumed $\xi = 0.01$ and $\lambda = 0.8$. With these values, we use the relation derived for Eve's variance defined w and Alice's preparation valiance defined v and substitute both of them in the covariance matrix.

```
n = 500
L = np.linspace(0,250,n)
key = []
for i in range(n):
  t0 = 10**(-0.02*L[i])
  M_ab = cm.subs({"T":t0})
  key.append(het_key_rate(M_ab,recon = 0.95))
```

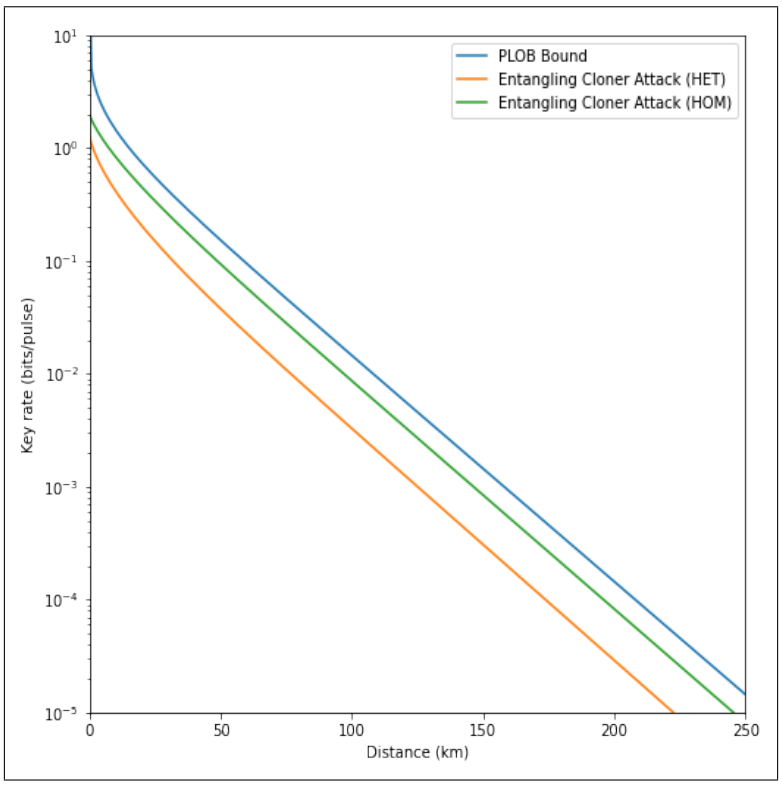


Figure 5.1.2: Key rate for the Entangling Cloner Attack in a direct transmission scheme under homodyne (HOM) and heterodyne (HET) detection by Bob. $\beta = 0.95$, $\xi = 0.01$, $\lambda = 0.8$

```
plt.plot(L,key)
plt.show()
```

Our covariance matrix is now ready. The only variable left is t which is the transmissivity of the beam splitter used by Eve. Since this transmissivity translates to channel loss, we will use the length-transmissivity relation to convert t into L. We run the values for n steps iterating L from 0 to 250 km. The function defined as **het_key_rate** uses the covariance matrix of Alice and Bob to generate the key rate with a reconciliation efficiency of 0.95. Once the loop ends, the values are plotted on a 2D graph.

We re-run the same code and replace heterodyne with a homodyne detector and plot these results alongside the PLOB bound[2] for comparison. The results clearly suggest that direct transmission of TMSV state will generate a better key rate if Bob uses homodyne detection. This fact is partially because we are evaluating the key rate in the asymptotic regime, in the non-asymptotic regime Bob has to discard roughly 50% of his pulses to match Alice's choice mode which reduces the key rate by

[2]PLOB bound [21] is the maximum possible key rate that can be generated in a quantum channel without using repeaters

a half.

5.2 Approaching Classical Limit [28, 29]

If Alice prepares a thermal state and transmits it to Bob, when Bob makes a measurement on this state the result will always suffer 1 SNU of quantum noise as governed by the uncertainty relation. In this paper, the authors study the security of a direct transmission protocol when this intrinsic noise is greater than 1. Practically, this error appears due to the preparation device imperfection. Bob can always calibrate his measurement device at the start of the protocol to exact the value of this preparation noise. To account for this loss, we have to modify $V(\hat{x}_{B|A})$ from (3.4.9) slightly:

$$V(\hat{x}_{B|A}) = \left(V(\hat{x}_B) - \frac{|\langle \hat{x}_B \hat{x}_A \rangle|}{V(\hat{x}_A)}\right) \Longrightarrow \left(V(\hat{x}_B) - \frac{|\langle \hat{x}_B \hat{x}_S \rangle|}{V(\hat{x}_A)}\right) \tag{5.2.1}$$

$\hat{x}_S$ is Bob's approximation of Alice's signal, not signal + noise. The procedure for the calculation of key rate is the same as in Entangling Cloner Attack but we simulate with different parameter values. It can be seen that approaching a high value of V_o requires an almost perfect channel to generate a positive key rate. Higher values of V_o imply that we are approaching the classical regime and hence our formalism designed for quantum system becomes redundant.

```
primary_pairs_dim = 1
attack_pairs_dim = 1
cm = CM_TMSV(primary_pairs_dim, attack_pairs_dim)
cm = beam_splitter(3,7,t,cm)
cm = mode_M_separator(1,4,1,4,cm)
```

Above code generates a TMSV covariance matrix by Alice attached with an ancillary Eve TMSV. The last two lines mix the ancillary state with Alice's state and then removes it.

```
err = 0
recon = 1
l = 0.99999
w = (err)/(1-t) + 1
cm = cm.subs({"W_1":w})
thermal_noise = [1,2,3,5]
```

```
for j in range(4):
  key = []
  v0 = thermal_noise[j]
  v = (1+l**2)/(1-l**2) + v0
  for i in range(n):
    v0 = thermal_noise[j]
    t0 = channel_t[i]
    p = cm.subs({"V_1":v,"T":t0})
    key.append(het_key_rate(p,recon,signal=v0))
```

Finally we define the values of all constants which include channel loss ξ, reconciliation efficiency β, Alice's squeezing λ and Eve's variance W. Than we use these values to plot the heterodyne/homodyne key rate by iterating over channel transmittance and thermal noise. Note that we are sending an additional argument 'signal' in the key rate evaluation function which by default is set to 1.

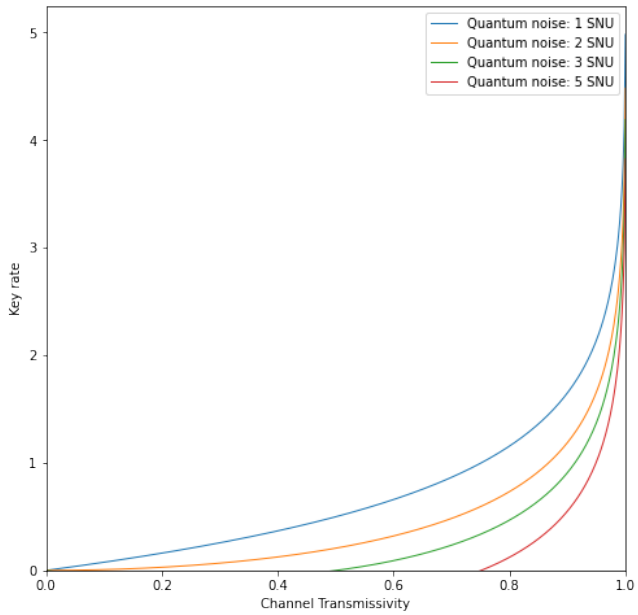


Figure 5.2.1: Key rate for different values of thermal noise at Bob's measurement apparatus under homodyne measurement

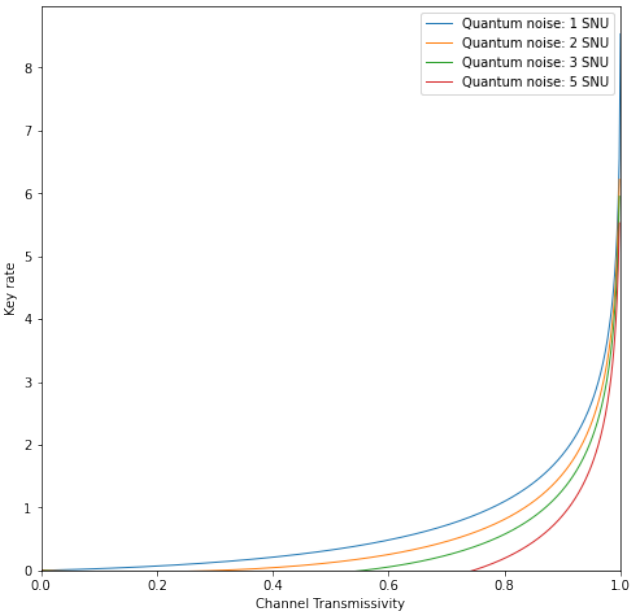


Figure 5.2.2: Key rate for different values of thermal noise at Bob's measurement apparatus under heterodyne measurement

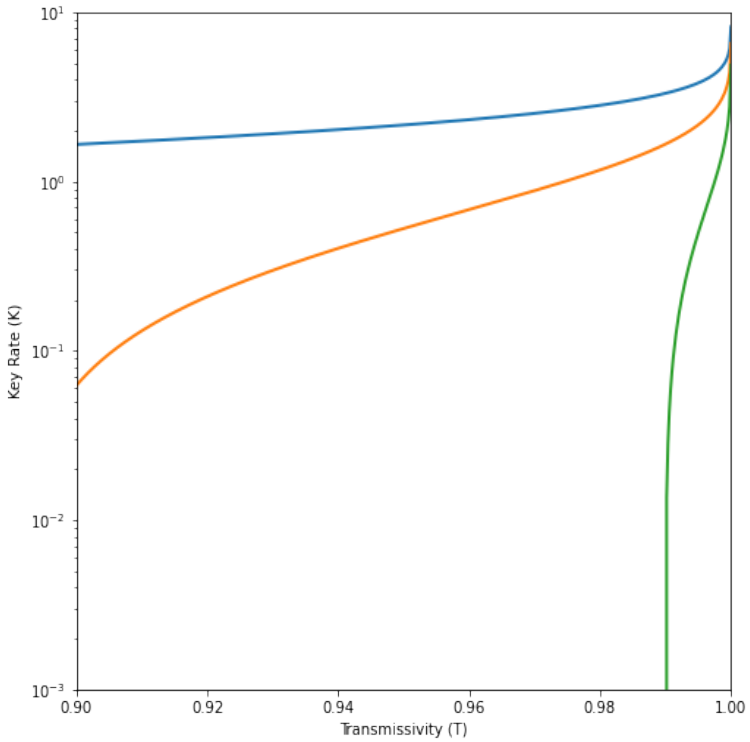


Figure 5.2.3: Homodyne measurement by Bob using ideal parameters but with a significantly large thermal noise. $V_o = 1$ (blue), $V_o = 10$ (orange) and $V_o = 100$ (green)

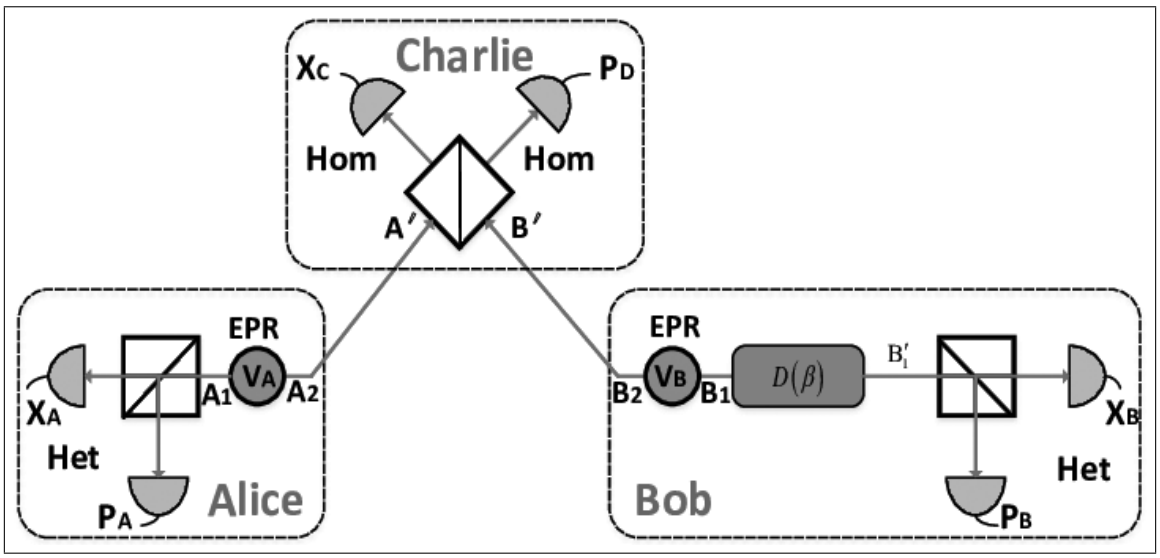


Figure 5.3.1: Setup of an MDI protocol with heterodyne detection. Alice and Bob separately generate their EPR states with variances V_A and V_B. They send one half of their signal to Charlie who interferes the signal at a balanced beam splitter before performing a projective homodyne measurement of conjugate quadratures. Bob rescales his mode followed by heterodyne measurement by Alice and Bob. Charlie is assumed to be under Eve's influence and Eve is aware of the whole system except the heterodyne measurement results at Alice and Bob

5.3 Measurement-device independent protocol [33]

The measurement device independent (MDI) protocol is a monumental step in realizing practical quantum communication. This is because under the assumption of coherent attacks, Eve can attack the measurement devices used by Bob forcing Bob to underestimate information leakage which overestimates the key rate and imposes a security threat. Although with perfect devices, it is not possible for Eve to performs such attacks but practical setups always have some amount of error.

To tackle this, we take the measurement devices and give it to a third party called Charlie. Charlie will handle the measurements of noisy states and announce of their results publicly. This then removes the requirement to protect Bob against measurement device attacks.

Observe from Figure 5.3.1, Alice and Bob have prepared an independent mode, there exists no correlation between their modes. Each half of the mode sent to Charlie suffers channel loss. When Charlie receives the signal and interacts them on a 50:50 beam splitter, the outgoing modes entangle. When Charlie homodynes the two modes and announces their result, the other half of the system which was sitting in Alice and Bob's lab becomes entangled. The process at Charlie's station is also called entanglement swapping.

This protocol has been studied in two settings. **Symmetric**: when the distance between Alice and

Charlie is the same as the distance between Bob and Charlie. **Asymmetric**: when these distances are not equal. For the case of reverse reconciliation, we move Charlie close to Bob. This is because during the process of reconciliation, Eve tries to estimate Bob's data, if the channel in which Bob's state traveled is small, Eve has very little information on Bob's state and this makes it harder for Eve to develop correlation between Alice's signal and Bob's signal. We will show the pseudo code for symmetric setting in this section and the pseudo code for asymmetric setting for a different protocol in the next section because the modification is identical for both protocols.

One can read through the paper to see how the authors have formulated Charlie's measurement in terms of state vectors of Alice and Bob. We take a different approach to this and simply generate a covariance matrix for Alice, Bob and Eve, apply channel loss, apply Charlies beam splitter on the lossy modes and make a position and momentum partial measurement. This is a much simplified approach which is possible because all operations are Gaussian.

```
primary_pairs_dim = 2
attack_pairs_dim = 2
cm = CM_TMSV(primary_pairs_dim, attack_pairs_dim)
cm = beam_splitter(3,11,T,cm)
cm = beam_splitter(5,15,T,cm)
cm = mode_M_separator(1,8,1,8,cm)
```

We start by first generating the CM composing of 2 primary TMSV states Alice's and Bob's followed by applying Eve's beam splitters separately on the two primary modes. At the end we dispose all ancillary modes.

Note that the transmissivity of both Eve's beams splitters is set equal. This is the case of symmetric setting when the channel length Alice to Charlie and Bob to Charlie are equal. We will also take asymmetric setup when these values are not equal.

```
cm = beam_splitter(3,5,0.5,cm)
cm = partial_homodyne_q(cm)
cm = partial_homodyne_p(cm)
```

Now that channel loss has been implemented, we apply Charlie's operations by first mixing the two states on a balanced beam splitter followed by performing partial homodyne measurements on

position and momentum.

The last set of operations reduces the dimension of covariance matrix to 4x4. We then follow the same key rate evaluation method as given in section 5.1.

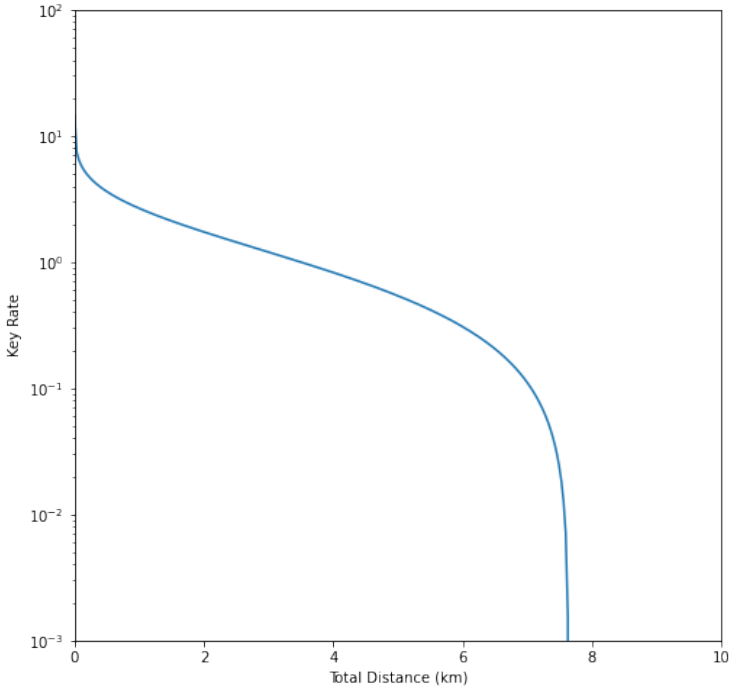


Figure 5.3.2: Key rate for CV-MDI protocol in a symmetric setting $L_{Bob-Charlie} = L_{Alice-Charlie}$

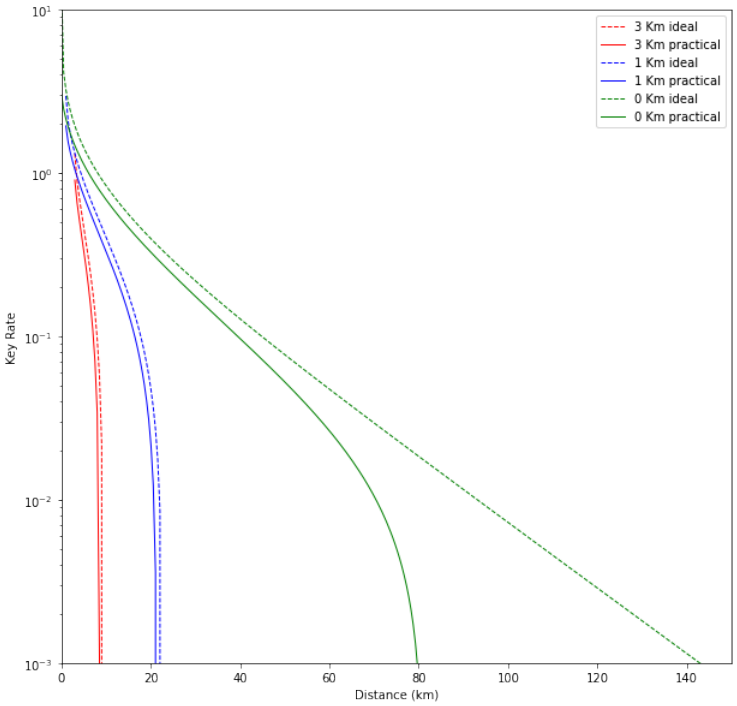


Figure 5.3.3: Key rate for CV-MDI protocol in an a asymmetric settings $L_{Bob-Charlie} = \{0, 1, 3\}$ km. The practical key rate has $\beta = 1$, $\xi = \xi_A + \xi_B = 0.004$ and $V = 40$

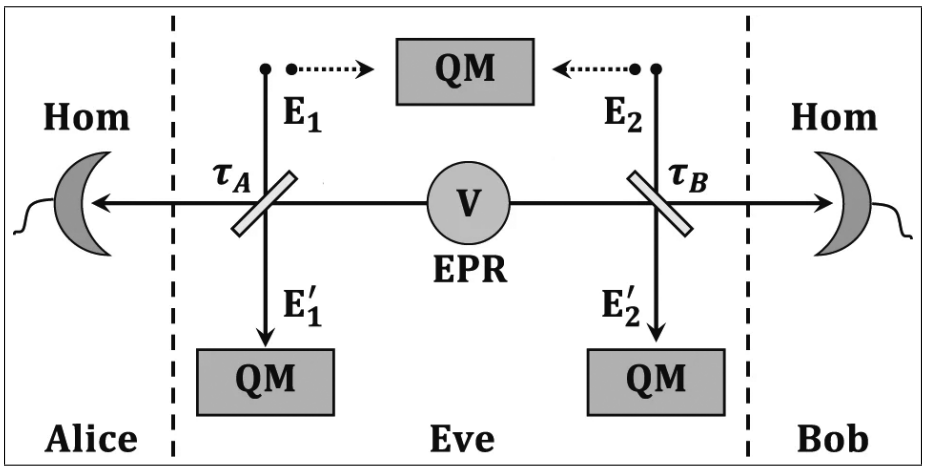


Figure 5.4.1: Setup of entanglement in the middle. An EPR state with variance V is generated by Charlie. One mode is sent to Alice and the other is sent to Bob. Eve tags the signal with her two EPR states. Once received, Alice and Bob perform a homodyne measurement on their noisy signal completing the transmission step.

5.4 Source-device independent protocol with TMSV state [32]

Much like an independent measurement device, an independent source device has also contributed in realizing practical CV QKD. This is an entanglement in the middle protocol i.e. Charlie is now responsible to generate the EPR pair and send one half to Alice and the other half to Bob while being completely under the influence of Eve.

The authors of this paper have taken the case of coherent attack on an entanglement-in-the-middle setup thus realizing it as a source device independent setup. Since the scope of this thesis is constrained to asymptotic collective attacks, we will not discuss the limited block size case for SDI.

Although we will additionally show that like the MDI protocol, an asymmetric setting also shows improvement with an independent source under general collective attacks and it is quite resilient to noise. The major difference of asymmetric SDI and asymmetric MDI protocol is that Charlie is now very close to Alice rather than Bob. This is because the state sent to Alice and Bob is identical. When Bob discloses part of his signal in the reconciliation step, it adds less information for Eve as Eve has very little information on the signal sent to Alice.

```
cm = CM_TMSV(1)
cm = attack_mode(1,cm,error,ta)
cm = attack_mode(3,cm,error,tb)
```

We generate a CM with 1 primary and use a function **attack_mode** which is a short form of entangling cloner attack. We send the function two different values of transmissivities i.e. we simulate the case when $t_a \neq t_b$ to mimic asymmetric channel losses.

```
err = 0
recon = 1
l = 0.99999
v = (1+l**2)/(1-l**2)
w1 = (ta*err)/(1-ta) + 1
w2 = (tb*err)/(1-tb) + 1

L = np.linspace(0,10,n)
for i in range(n):
   ta_o = 10**(-0.02*(l_ac))
   tb_o = 10**(-0.02*L[i])
   p = cm.subs({"ta":ta_o,"tb":tb_o})
   key.append(hom_key_rate(p,recon))
plt.plot(L,key)
plt.show()
```

Then we set the values of all constants which now includes two different values of Eve's variance corresponding to two different channel lengths, and calculate the key rate as done before.

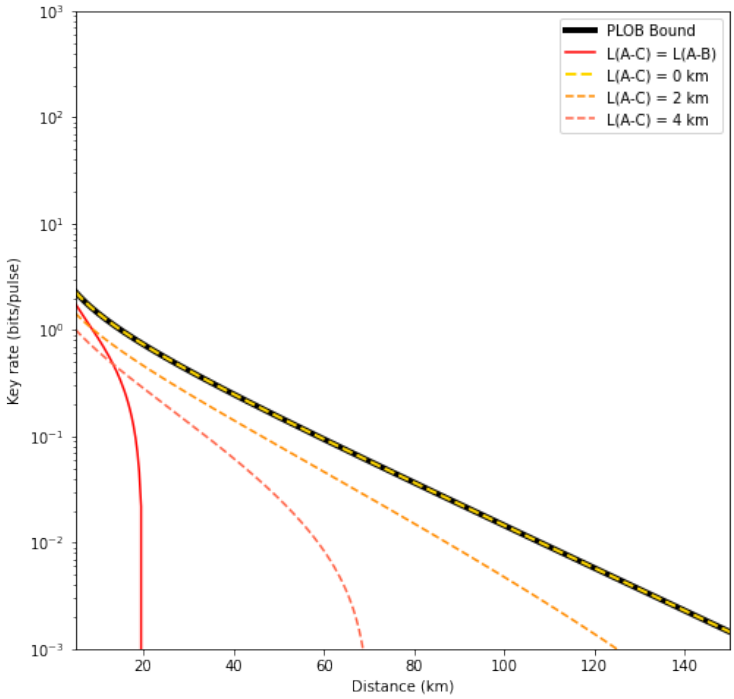


Figure 5.4.2: **Ideal** homodyne key rate under general collective attacks for entanglement in the middle. $\beta = 1, \xi = 0, V = 10^5$

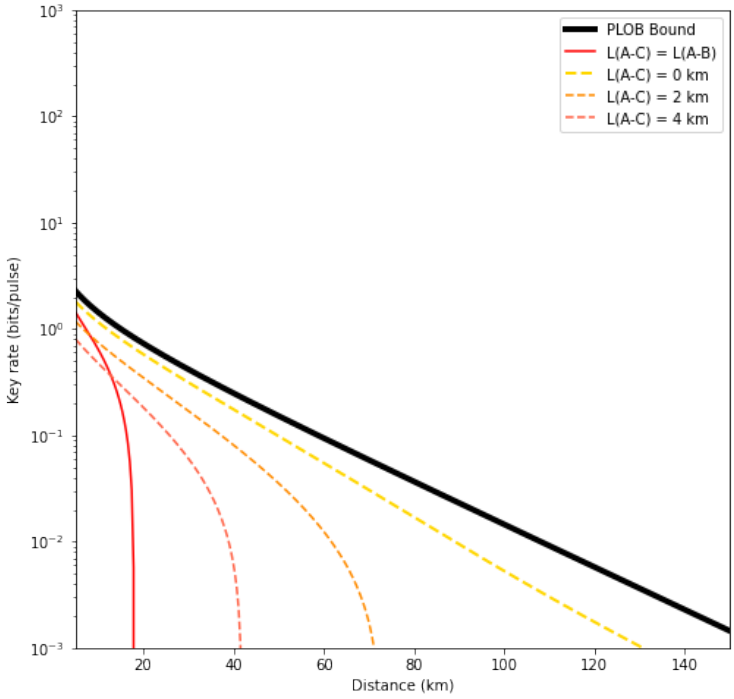


Figure 5.4.3: **Practical** homodyne key rate under general collective attacks for entanglement in the middle. $\beta = 0.97, \xi = 0.01, V = 40$

Chapter 6

Generalized approach to Non-Gaussian CV-QKD protocols

Distilling entanglement is an important purification step to enhance any QKD protocol, while we can never distill entanglement by local Gaussian operations on Gaussian states [8] we can however use non-Gaussian operations.

Non-Gaussian operations are operations that disturb the Gaussian nature of CV states. Even though the state of the system is non-Gaussian once we apply such operators, Devetak-Winter rate can still be used to bound the key rate. This is done by slightly modifying (3.4.1) as below:

$$K \geq \mathcal{P}\Big(\beta I(A:B) - I(B:E)\Big) \tag{6.0.1}$$

where $\mathcal{P}$ is the probability of success of the non-Gaussian operation performed which means that we discard all states on which the non-Gaussian operation was unsuccessful.

Non-Gaussian states have a non zero second moment which makes them analytically non-tractable i.e. we cannot analytically evaluate the upper limit of Eve's information. Fortunately, optimality of Gaussian attacks [9] makes sure that (6.0.1) is lower bounded iff we extract $I(A:B)$ and $I(B:E)$ from an equivalent Gaussian state implying that $K_{non-Gaussian} \geq K_{Gaussian}$. So our previous formalism is valid as well as lower bounded.

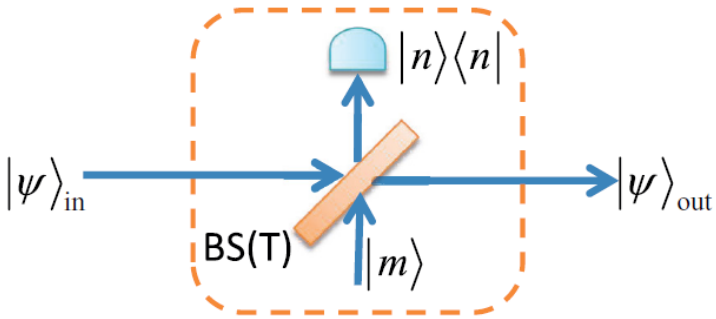


Figure 6.1.1: Setup of non-Gaussian operations. $|\psi\rangle$ will be TMSV state for us, $|n\rangle\langle n|$ is a photon number resolving detector and $|m\rangle$ is the photon state mixed at the beam splitter BS with transmissivity T. (1) Photon addition: $m > n$ (2) Photon subtraction: $m < n$ (3) Photon replacement: $m = n$ (Figure reused from [13])

6.0.1 Resources

When working with these protocols we need to start from the state vector of the system and implement operators as described by the protocol. This is because symplectic operations for non-Gaussian operators do not conserve the Gaussian nature of states so we have to take the non-Gaussian output state and approximate it to a Gaussian state.

Qutip is an open quantum system simulator built on python, we will use this library to construct state vectors and operators acting on them. The downside of using this library is that it is purely numerical and not compatible with **Sympy's** symbolic arguments. This means that we will start with constant values for all of our variables when working with **Qutip**.

Our approach is to perform all non-Gaussian operations on our state and move towards it's covariance matrix as early as possible. This is because Qutip is computationally heavy when we assume a high dimension fock space and we need a high dimension fock space to approximate our result better. The advantage of our previous formalism is it's computational speed so we will use our previous functions alongside this new library.

6.1 Non-Gaussian operations in direct transmission [1, 13]

The setup of non-Gaussian operations is shown in Figure 6.1.1, the model mixes m-photon state with $|\psi\rangle$ and projects part of it on $\Pi_n = |n\rangle\langle n|$. The projection operator Π_n clicks whenever it detect n-photons. The three possible non-Gaussian operation are (1) Photon addition: when photons are

added in the input signal ($m > n$), (2) Photon subtraction: when photons are removed from the signal ($m < n$) and (3) Photon replacement: when same number of photons are added and removed from the beam ($m = n$).

Let us now model a general non-Gaussian setup for a TMSV state. We will discuss two cases, when these operations are applied before and after channel loss.

6.1.1 Pre-Channel loss

```
from qutip import *
N = 50
a = tensor(destroy(N),qeye(N))
b = tensor(qeye(N),destroy(N))
l = 0.8
for n in range(N):
  psi = psi + sqrt(1-l**2) * (l**n) * tensor(fock(N,n),fock(N,n))
```

We start by first importing the whole quitp library as core so that we don't have to call individual functions explicitly. Then we define our ladder operators for the two Hilbert space $\mathcal{H}_A$ and $\mathcal{H}_B$ and calculate TMSV state vector by using $|\psi\rangle_{TMSV} = \sqrt{1-\lambda^2}\sum_{n=0}^{\infty}\lambda^n |n\rangle \otimes |n\rangle$. To generate a perfect TMSV state we have to take an infinite dimensional fock space, by restricting ourselves to $N = 50$ we approximate the TMSV state up to the 20^{th} decimal which is more than enough for protocols discussed in this section.

```
Pi = fock(N,n_o) * fock(N,n_o).dag()
BS = (np.arccos(t)*(a.dag()*b - a*b.dag())).expm('sparse')
psi = tensor(psi, fock(N,m_o))
psi = tensor((qeye(N), qeye(N), Pi)) * tensor(qeye(N),BS) * psi
```

The first line defines the projection operator $\Pi_n = |n\rangle\langle n|$ we have fixed these values based on which non-Gaussian operation we are performing. The second line defines the beam splitter[1] operator $e^{(\sqrt{t}(\hat{a}^\dagger\hat{b} - \hat{a}\hat{b}^\dagger))}$, the third line appends the m-photon fock state to our TMSV state $|\psi\rangle_{TMSV} \rightarrow$

[1]The argument 'sparse' given in **expm** is to indicate that most of the entries in **BS** are zeros. This give a huge boost to calculation speed.

$|\psi\rangle_{TMSV} \otimes |m\rangle$ and finally we apply the beam splitter followed by projection operator:

$$|\psi\rangle = \left(\mathbb{1} \otimes \mathbb{1} \otimes |1\rangle\langle 1|\right)\left(\mathbb{1} \otimes BS\right)\left(|\psi\rangle_{TMSV} \otimes |m\rangle\right)$$

```
prob = psi.norm()**2
psi =  (1/sqrt(prob)) * psi
rho = psi * psi.dag()
rho = rho.ptrace([0,1])
cm = get_CM(rho, a, b)
```

While $|\psi\rangle_{TMSV}$ itself is normalized, $|\psi\rangle$ is not. We start by first normalizing the non-Gaussian state w.r.t. the probability of success defined as **prob**. Then we generate it's normalized density matrix $\rho = |\psi\rangle\langle\psi|$. Next we take a partial trace and remove all ancillary modes by keeping only the first and second Hilbert space. Now that our density matrix is ready and all operation past this point are Gaussian, we send ρ to the function **get_CM** which converts this density matrix into covariance matrix by using (2.3.1).

```
for i in range(500):
  tc = 10**(-0.02*L[i])
  M = attack_mode(3,cm,error,tc)
  key.append(prob * hom_key_rate(M,recon))
```

Once the covariance matrix is formed the code runs a loop assuming different values of channel transmittance where an entangling cloner attack is assumed on mode 2. The function **attack_mode** is a short form of the two steps involved in entangling cloner attacks i.e. prepare Eve's TMSV with variance $W = 1 + \frac{\xi}{1-t_c}$ and mix it with the signal via a beam splitter of transmissivity t_c. Finally we calculate the heralded key rate $K^{'} = \mathcal{P}K$.

Note that we did not explicitly define the transmissivity t of the first beam splitter. This is because the value of t is optimized w.r.t. the values of λ and t_c. To do this we re-run the code from start assuming a different value of t each time. Finally we take only those values of t where the key rate is maximum.

6.1.2 Post-Channel loss

When applying non-Gaussian operations after channel loss, we have to start by first generating Alice's TMSV state alongside Eve's ancillary state and implement the entangling cloner attack, after the attack is applied we move towards the same steps discussed above. They key difference here is that we are no longer working with state vector after we apply channel loss. We will be working with density matrix which slightly changes the method of applying non-Gaussian operators.

```
N = 50
a = tensor(destroy(N),qeye(N))
b = tensor(qeye(N),destroy(N))

# Following code blocks are all in a loop iterating over 'tc'
l = 0.8
l_E = sqrt( error/(error - 2*tc + 2) )
for n in range(N):
  psi_alice += sqrt(1-l**2) * (l**n) *
                    tensor(fock(N,n),fock(N,n))
  psi_eve += sqrt(1-l_E**2) * (l_E**n) *
                    tensor(fock(N,n),fock(N,n))
```

λ_E is Eve's squeezing parameter which depends on the length of the channel. Since Eve has to set her variance to $W = 1 + \frac{\xi}{1+T_c}$ where $W = \frac{1+\lambda_E^2}{1-\lambda_E^2}$, we can solve these equations for λ_E to get $\lambda_E = \sqrt{\frac{\xi}{\xi-2T_c+2}}$.

```
psi = tensor(psi_alice,psi_eve)
psi = BS_channel * psi
rho = psi.ptrace([0,1])
rho = rho.unit()
```

Next we attach Eve's TMSV state to Alice's state and apply a beam splitter to mix their outgoing modes. We then reduce the total system by tracing out the ancillary mode.

```
rho = tensor(rho,rho_non_gaussian)
rho = BS_non_gaussian * rho * BS_non_gaussian.dag()
rho = Pi * rho * Pi.dag()
rho = rho.ptrace([0,1])
```

Finally we append the non-Gaussian state to the residual density matrix:

$$\rho = \rho_{lossy\ state} \otimes \rho_{non-Gaussian} = |\psi\rangle^{'} \langle\psi|^{'} \otimes |n\rangle \langle n|$$

and perform the same operations as defined the in the previous section. We take the case when Alice and Bob perform heterodyne measurement.

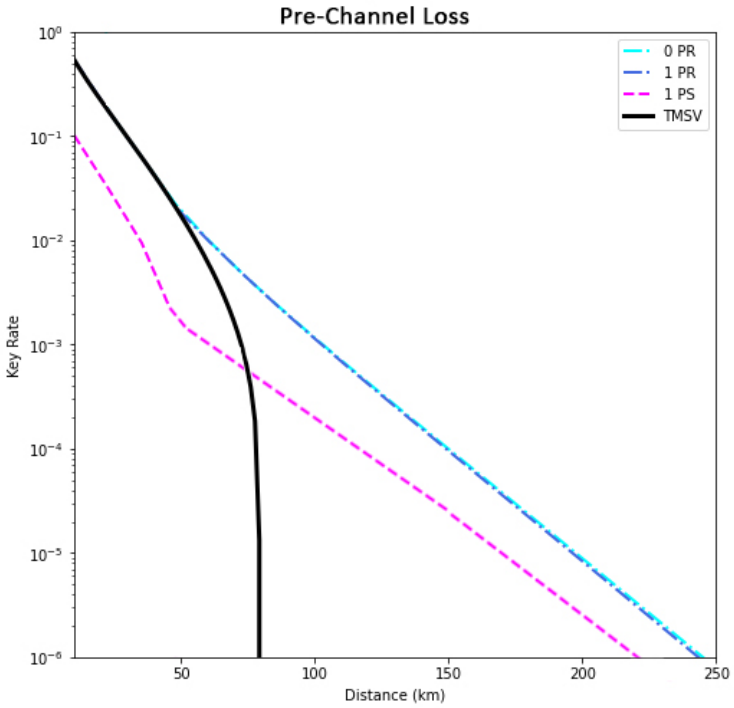


Figure 6.1.2: Key rate for non-Gaussian operations before channel loss assuming practical parameters: $\beta = 0.95$, $\xi = 0.01$ and $\lambda = 0.9512$ ($V = 20$). 0 PR = zero photon replacement (m = n = 0), 1 PR = one photon replacement (m = n = 1) and 1 PS = one photon subtraction (m = 0; n = 1)

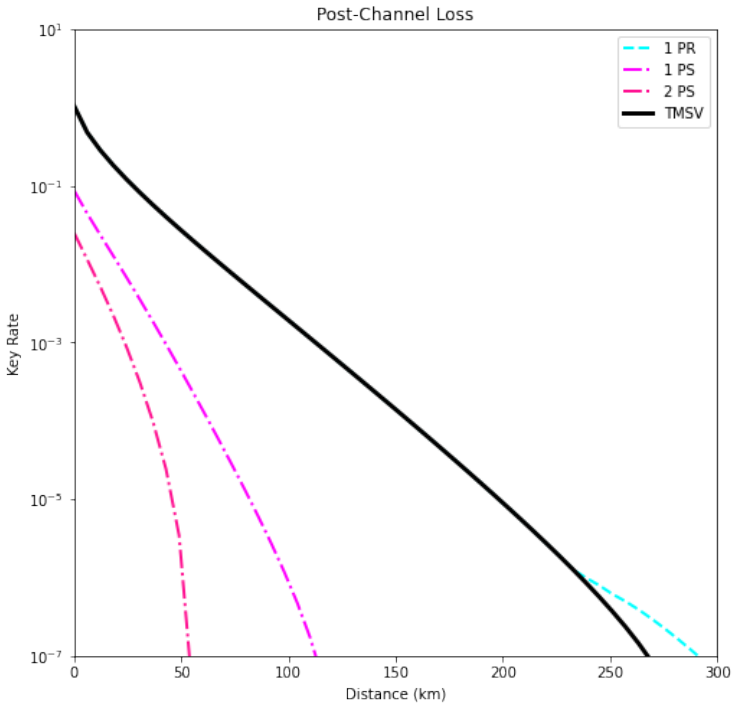


Figure 6.1.3: Key rate for non-Gaussian operations after channel loss assuming practical parameters: $\beta = 0.95$, $\xi = 0.03$ and $\lambda = 0.8$. 1 PR = one photon replacement (m = n = 1), 1 PS = one photon subtraction (m = 0; n = 1) and 2 PS = two photon subtractions (m = 0; n = 2)

6.2 Non-Gaussian operations in MDI protocol [24, 30]

Non-Gaussian operations offer improvement to measurement device independent protocol. As we have seen in the previous section, non-Gaussian operations when applied after channel loss do not offer much improvement to the protocol. This combined with the fact that MDI protocol has several Gaussian operations involved, the key rate is directly affected due to such operations and any minor noise in the system significantly reduces the distance for secure key rate. This is the reason why post-channel non-Gaussian operations haven't shown any improvement so far. We will only consider non-Gaussian operations applied before channel loss and only by Alice since Alice suffers the most channel loss in the asymmetric case.

We start by building the code as discussed in 6.1.1. Taking this approach only for Alice's state and following complete Gaussian approach for Bob's state.

```
l = 0.980196058819607    # V = 50
for n in range(N):
  psi = psi + sqrt(1-l**2) * (l**n) * tensor(fock(N,n),fock(N,n))
psi = tensor(psi, fock(N,m_o))
psi = tensor((qeye(N), qeye(N), Pi)) * tensor(qeye(N),BS) * psi
prob = psi.norm()**2
psi =  (1/sqrt(prob)) * psi
rho = psi * psi.dag()
rho = rho.ptrace([0,1])
cm = get_CM(rho, a, b)
```

This will generate Alice's covariance matrix with the included non-Gaussian operation. We reused Π_n and beam splitter as defined in the previous section.

```
M_alice = attack_mode(3,cm,error,ta)
M_bob = CM_TMSV(1,0)
M_bob = attack_mode(3,M_bob,error,tb)
M = M.diag(M_alice, M_bob)
```

The final result M is now the covariance matrix received by Charlie who then mixes them at a balanced beam splitter followed by a partial homodyne measurement as done in section 5.3.

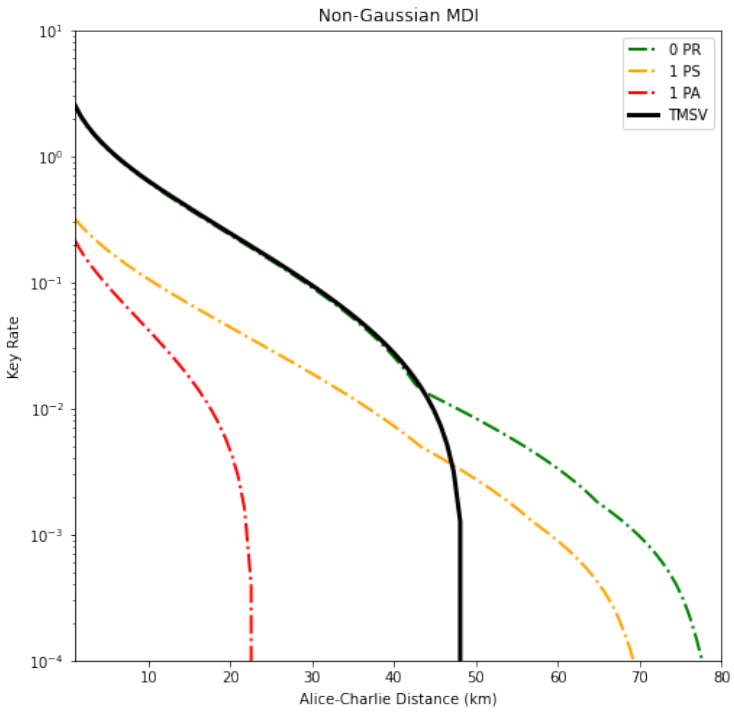


Figure 6.2.1: Key rate for asymmetric MDI under different non-Gaussian operations applied before channel loss. Parameters taken are $\beta = 0.96$, $\xi = 0.002$ and $\lambda = 0.9802$ (V = 50). 1 PA = one photon addition (m = 1; n = 0)

6.3 Cascaded non-Gaussian operations [19]

In this protocol we apply non-Gaussian operations for only one photon generating a one photon non-Gaussian state that is sent to another one photon operation and so on. This method is repeated n times, each time we use a single photon detector. The advantage here is the use of single photon detector which has a much better base efficiency than the same detector when measuring larger number of photons. For the sake of simplicity, we assume the same detector efficiency for both cases (with and without cascade). To observe the effect of a cascade we use a measure called log-negativity which is explained below.

6.3.1 Logarithmic Negativity [26]

Entangled quantum states follow the assumption that entanglement does not increase under the action of a quantum channel which can be realized by local quantum operations and classical communication (LOCC), entanglement quantities that satisfy this condition are called entanglement monotones. **Entanglement distillation** is one such operation, the goal here is to use infinitely many copies of a

quantum states to produce a high fidelity Bell state. Opposite to this is **entanglement dilution** where the goal is to produce high fidelity Bell states by using as few Bell states as possible.

The question then arises, how much entanglement can a quantum state distil? The answer lies in logarithmic negativity, this measure (which is also an entanglement monotone) puts an upper bound on the amount of entanglement that can potentially be distilled from a bipartite mixed state.

It is a useful measure in QKD because channel loss reduces entanglement by mixing the pure state with an ancillary state. Log negativity calculates the amount of this mixing, higher values mean more entanglement can be distilled from the state. The formula to calculate log negativity is as follows:

$$E_N = \log_2\left(\left\|\rho_{AB}^{\Gamma}\right\|\right) \tag{6.3.1}$$

Where $^{\Gamma}$ represents a partial transpose and $\|.\|$ represents trace norm. It is easy to calculate this because we already know how to get to the non-Gaussian density matrix.

```
rho = partial_transpose(rho, [0, 1])
rho = rho.norm()
log_negativity = log(rho,2)
```

To apply cascaded non-Gaussian operations, we simply apply the operation sequentially, normalizing the state after each operation.

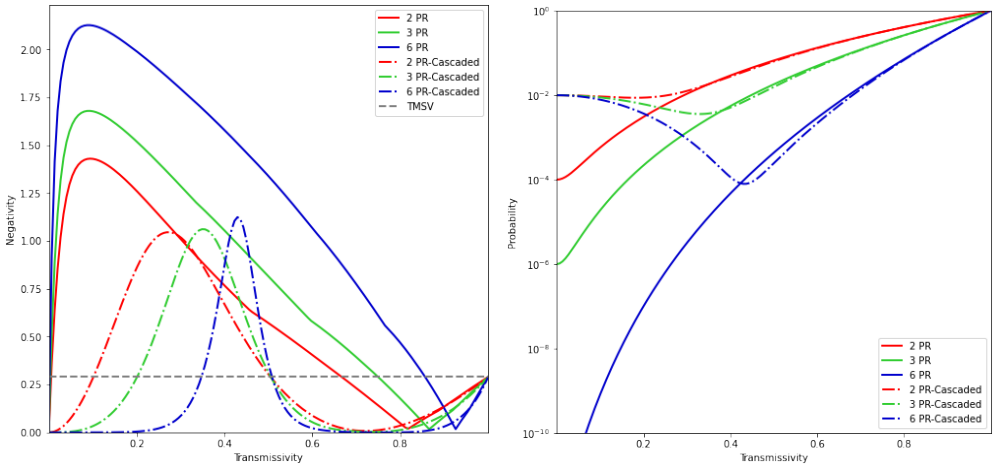


Figure 6.3.1: Photon replacement with and without cascade for $\lambda = 0.1$

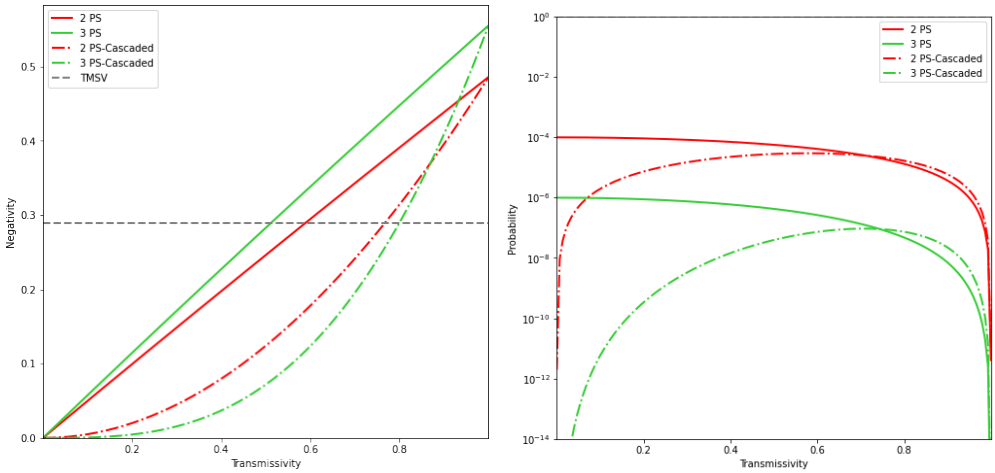


Figure 6.3.2: Photon subtraction with and without cascade for $\lambda = 0.1$

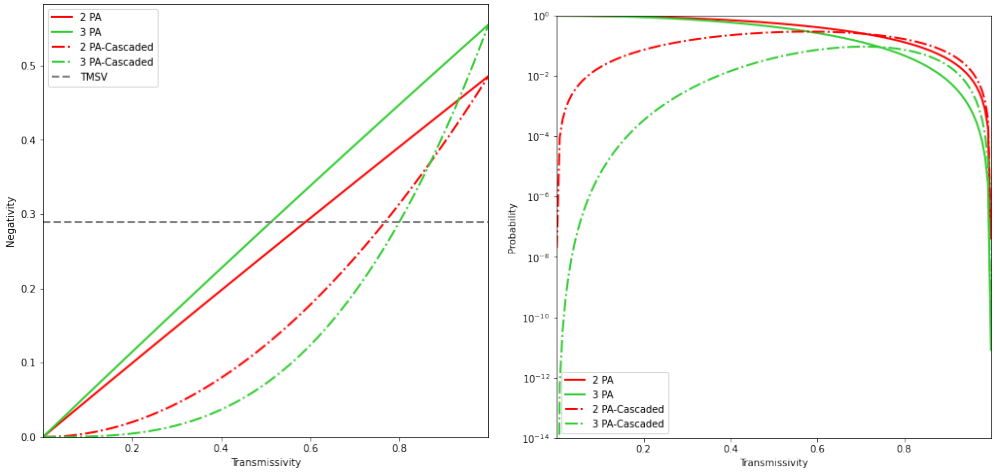


Figure 6.3.3: Photon addition with and without cascade for $\lambda = 0.1$

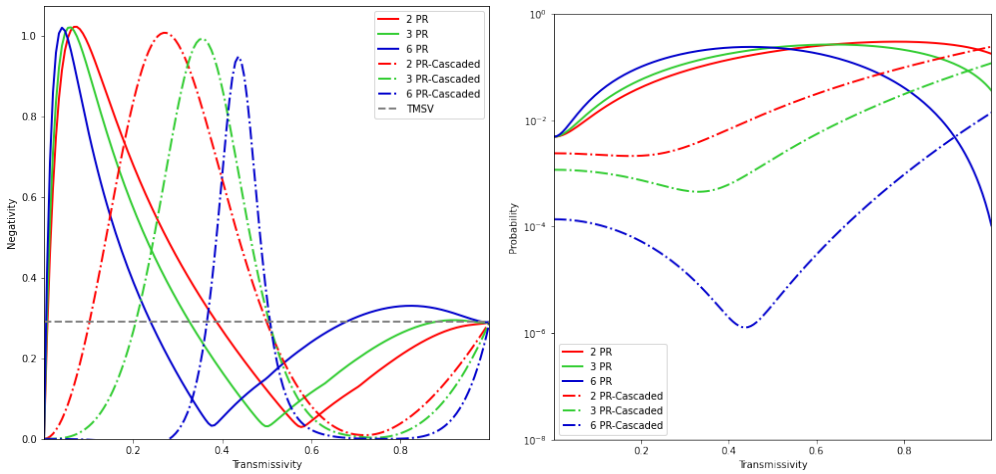


Figure 6.3.4: Photon replacement with imperfect detector (efficiency = 70%)

6.3.2 Analysis

The simulations suggest that non-cascaded method overall performs better in terms of entanglement distillation capability of the state but the peak probability of success is extremely low for such operations. It can also be seen that only cascaded photon replaced states offer a decent improvement whereas photon subtracted and added state perform almost identical with the exception of photon addition having a much better probability of success.

Chapter 7

Improving CV-MDI-QKD at low squeezing

The real advantage of using generalized functions appears when we look at the explicit form of non-Gaussian states; they are long and require significant time to calculate analytically. Combined with the fact that we cannot know which state could potentially offer improvement means that the best way to go around is to test every state. By quickly testing random states we were able to find states that improve CV-MDI-QKD protocol.

7.1 CV-MDI with PAS states

We find that a photon added-then-subtracted (PAS) state has a unique property to generate positive key rate in low squeezed TMSV states. From an experimental stand point, this is useful because currently a squeezing of $\lambda \approx 0.52$ is easily achievable in labs [20]. As previously seen CV-MDI-QKD with single photon subtraction and zero photon catalysis require λ up to 0.98 to work at their maximum performance. MDI protocols are notoriously sensitive to excess system noise too which imposes another practical constraint. PAS states tackle both of these problems. Such states show resilience to excess noise all while working with squeezing $\lambda < 0.34$.

The non-Gaussian version of this protocol, which was previously discussed in section 6.2, is shown in Fig. 7.1.1. Alice and Bob generate an independent TMSV state. They keep half of the state and send the other half to Charlie via a lossy channel. It is assumed that an eavesdropper replaces this channel with a lossless one and mimics an equivalent loss which is now credited to information given away to Eve. The lossy states are then interfered at Charlie's balanced beam splitter and the outgoing states are measured and their classical results are announced publicly. Based on these results, Bob

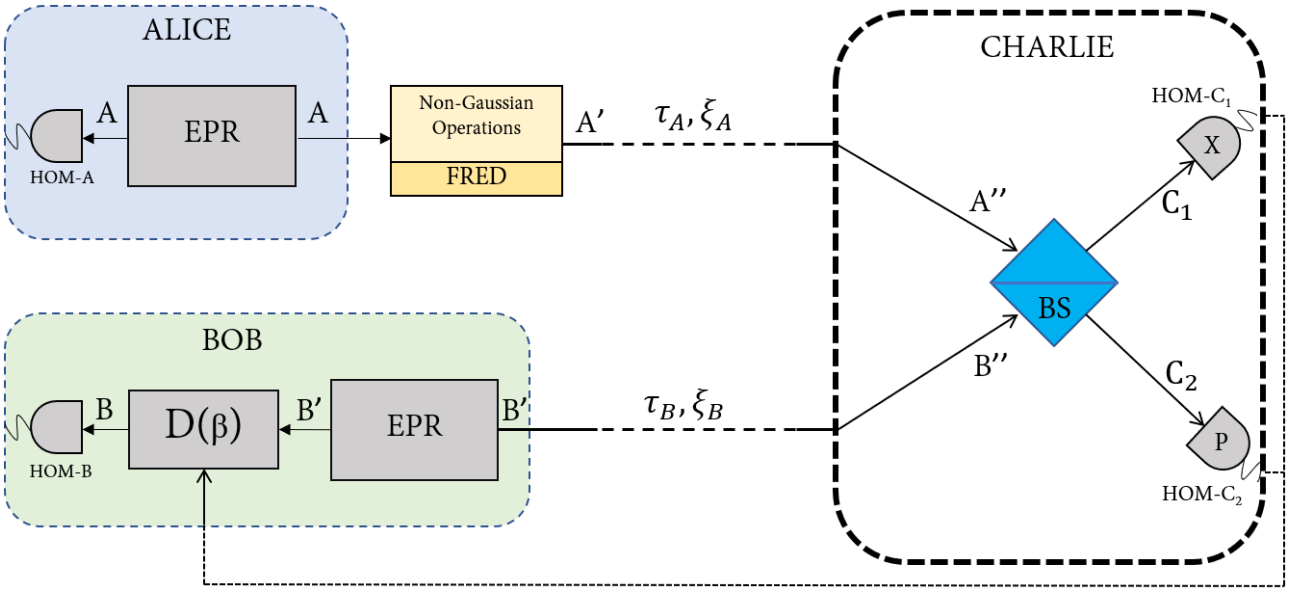


Figure 7.1.1: Entanglement based non-Gaussian CV-MDI-QKD scheme under the assumption that Eve is aware of Fred, Charlie and Bob's displacement but is unaware of Alice and Bob's homodyne measurement results. $D(\beta)$ is the displacement operator and $\tau_{\{A,B\}}, \xi_{\{A,B\}}$ are channel parameters for Alice and Bob. Non-Gaussian operations are applied at Fred's station as depicted in Fig.7.1.2.

displaces his state which correlated his local state to the one in Alice's lab concluding the transmission step of the protocol.

For unconditional security only Alice and Bob's local homodyne measurements are assumed to be out of Eve's knowledge, the remaining system is known to Alice, Bob and Eve.

We have followed previously established generalized scheme to test this state. Since it offered improvement, we evaluated it explicitly. Let us first look at the sequence of operations. Observe from Fig. 7.1.2, we can apply our specified operation by setting the values of $\{m_1, m_2, n_1, n_2\}$ which will generate the following state:

$$|\psi\rangle = \hat{\Pi}_{n_2,d}\hat{U}_{bd}(T)\hat{\Pi}_{n_1,c}\hat{U}_{bc}(T)\big(\,|\psi\rangle_{ab}^{in} \otimes |m_1 m_2\rangle_{cd}\,\big) \tag{7.1.1}$$

Where T is the transmissivity of the two beam splitters $\hat{U}$ which has been set equal, $\hat{\Pi}$ is the projection operator and the indexes $\{a, b, c, d\}$ correspond to the separate Hilbert spaces where our operators act. To get 1-PAS state, we set $|\psi\rangle_{in} = |\psi\rangle_{TMSV} = \sum_{n=0}^{\infty}\sqrt{1-\lambda^2}\lambda^n\,|nn\rangle$ and the parameters $m_1 = n_2 = 1$ and $m_2 = n_1 = 0$. We then get:

$$|\psi\rangle = \hat{\Pi}_{1,d}\hat{U}_{bd}(T)\hat{\Pi}_{0,c}\hat{U}_{bc}(T)\big(\,|\psi\rangle_{ab}^{TMSV} \otimes |10\rangle_{cd}\,\big) \tag{7.1.2}$$

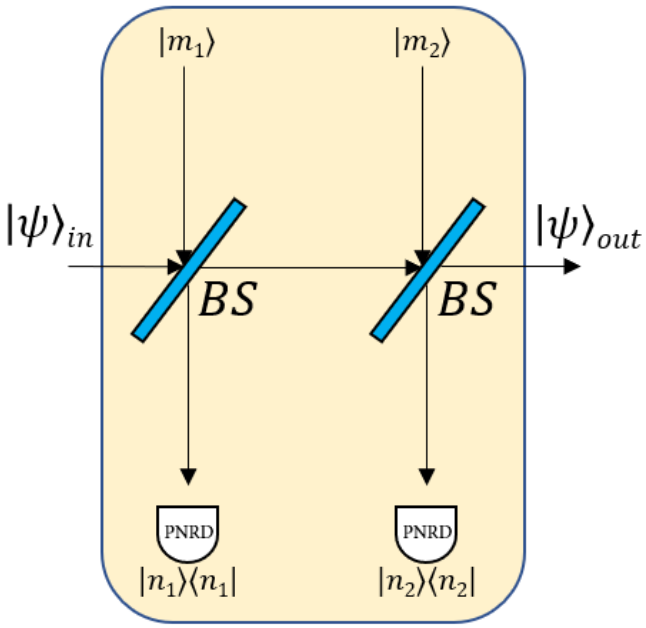


Figure 7.1.2: Non-Gaussian operation applied on Alice's outgoing state. BS are the beam splitters of tunable transmissivity and $PNDR$ are photon number resolving detectors. Specific choice of $\{m_1, m_2, n_1, n_2\}$ corresponds to a non-Gaussian operation on $|\psi\rangle_{in}$. $|\psi\rangle_{1PAS}$ is created by setting $m_1 = n_2 = 1, m_2 = n_1 = 0$ when $|\psi\rangle_{in} = |\psi\rangle_{TMSV}$, $|\psi\rangle_{2PR}$ is created by setting $m_1 = n_1 = m_2 = n_2 = 1$ when $|\psi\rangle_{in} = |\psi\rangle_{TMSV}$ and $|\psi\rangle_{2PAS}$ is created by setting $m_1 = n_2 = 1, m_2 = n_1 = 0$ when $|\psi\rangle_{in} = |\psi\rangle_{1PAS}$

where $\hat{\Pi}_0 = |0\rangle\langle 0|$ and $\hat{\Pi}_1 = |1\rangle\langle 1|$ and the beam splitter is given in fock space as:

$$\hat{U}|nm\rangle = \frac{1}{\sqrt{n!m!}} \sum_{k_1=0}^{n} \sum_{k_2=0}^{m} \binom{n}{k_1} \binom{m}{k_2} T^{k_1} T^{m-k_2} R^{k_2} (-R)^{n-k_1} \times$$
$$\sqrt{(k_1+k_2)!(n+m-k_1-k_2)!}\,|k_1+k_2,\ n+m-k_1-k_2\rangle \tag{7.1.3}$$

whereas $R = \sqrt{1-T^2}$. We can now solve (7.1.2) starting by applying the first beam splitter:

$$|\psi\rangle = \hat{\Pi}_{1,d}\hat{U}_{bd}(T)\hat{\Pi}_{0,c}\Big[\sum_{n=0}^{\infty} \sqrt{1-\lambda^2}\,|n\rangle \otimes \Big(\hat{U}\,|n1\rangle\Big) \otimes |0\rangle\Big]$$

Lets resolve the inner beam splitter expression first using (7.1.3):

$$\hat{U}_{bc}\,|n1\rangle_{bc} = \frac{1}{\sqrt{n!}} \sum_{k_1=0}^{n} \sum_{k_2=0}^{1} \binom{n}{k_1} \binom{1}{k_2} T^{k_1} T^{1-k_2} R^{k_2} (-R)^{n-k_1} \times$$
$$\sqrt{(k_1+k_2)!(n+1-k_1-k_2)!}\,|k_1+k_2,\ n+1-k_1-k_2\rangle_{bc}$$

Evaluating the sum on k_2:

$$\hat{U}_{bc}\left|n1\right\rangle_{bc} = \frac{1}{\sqrt{n!}}\sum_{k_1=0}^{n}\binom{n}{k_1}\binom{1}{0}T^{k_1+1}(-R)^{n-k_1}\sqrt{k_1!(n+1-k_1)!}\left|k_1,\ n+1-k_1\right\rangle_{bc} + \frac{1}{\sqrt{n!}}\sum_{k_1=0}^{n}\binom{n}{k_1}\binom{1}{1}T^{k_1}R(-R)^{n-k_1}\sqrt{(k_1+1)!(n-k_1)!}\left|k_1+1,\ n-k_1\right\rangle_{bc}$$

$$\hat{U}_{bc}\left|n1\right\rangle_{bc} = \frac{1}{\sqrt{n!}}\sum_{k_1=0}^{n}\binom{n}{k_1}\left[T^{k_1+1}(-R)^{n-k_1}\sqrt{k_1!(n+1-k_1)!}\left|k_1,\ n+1-k_1\right\rangle_{bc} + T^{k_1}R(-R)^{n-k_1}\sqrt{(k_1+1)!(n-k_1)!}\left|k_1+1,\ n-k_1\right\rangle_{bc}\right]$$

We now apply $\hat{\Pi}_{0,c} = \left|0\right\rangle\left\langle 0\right|_c$:

$$\hat{\Pi}_{0,c}\hat{U}_{bc}\left|n1\right\rangle_{bc} = \frac{1}{\sqrt{n!}}\left[\binom{n}{k_1}T^{k_1+1}(-R)^{n-k_1}\sqrt{k_1!(n+1-k_1)!}\delta_0^{n+1-k_1}\left|k_1,\ 0\right\rangle_{bc} + \binom{n}{k_1}T^{k_1}R(-R)^{n-k_1}\sqrt{(k_1+1)!(n-k_1)!}\delta_0^{n-k_1}\left|k_1+1,\ 0\right\rangle_{bc}\right]$$

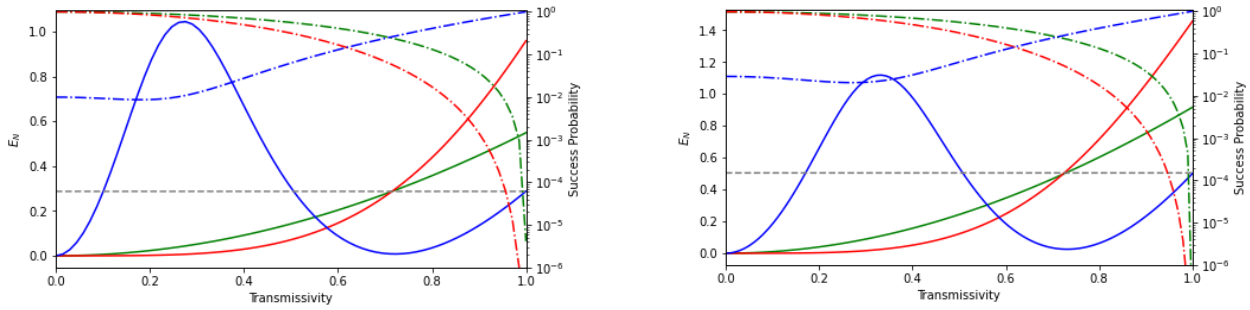
δ_0^x is the Kronecker delta which evaluate $x = 0$. Since the sum on k_1 tells us that $k_1 \leq n$, the first Kronecker delta becomes zero as k_1 cannot be equal to $n+1$. We are left with:

$$\hat{\Pi}_{0,c}\hat{U}_{bc}\left|n1\right\rangle_{bc} = \frac{1}{\sqrt{n!}}\left[\binom{n}{n}T^{n}R\sqrt{(n+1)!}\left|n+1,\ 0\right\rangle_{bc}\right]$$

After expanding the binomials and some algebra, we are left with a photon added state:

$$\hat{\Pi}_{0,c}\hat{U}_{bc}\left|n1\right\rangle_{bc} = T^{n}R\sqrt{n+1}\left|n+1,0\right\rangle_{bc}$$

A measurement on mode c removes it from the system and leaves behind an unnormalized state which



(a) (b)

Figure 7.1.3: Logarithmic negativity (solid line) and probability of successful operation (dashed dotted line) with respect to Fred's beam splitter transmissivity. Plotted lines are for 2 mode photon replaced state (2-PR, blue), 1 mode PAS state (1-PAS, green) and 2 mode PAS state (2-PAS, red). Dashed gray line represent the log-negativity of pure TMSV state. (a) When $\lambda = 0.1$ and (b) when $\lambda = 0.172$.

is normalized by a factor $\mathcal{N}$:

$$\hat{\Pi}_{0,c}\hat{U}_{bc}\left|n1\right\rangle_{bc} = \mathcal{N}T^{n}R\sqrt{n+1}\left|n+1\right\rangle_{b}$$

We can no follow these steps again to apply the photon subtraction operation and get our 1-PAS state. Using this 1-PAS state and applying the addition and subtraction operation again will give us 2-PAS state. These states are as given below:

$$\left|\psi\right\rangle_{1PAS} = \mathcal{N}_1 \sum_{n=0}^{\infty} \sqrt{1-\lambda^2}\lambda^n T^{2n}(1-T^2)(n+1)\left|nn\right\rangle \tag{7.1.4}$$

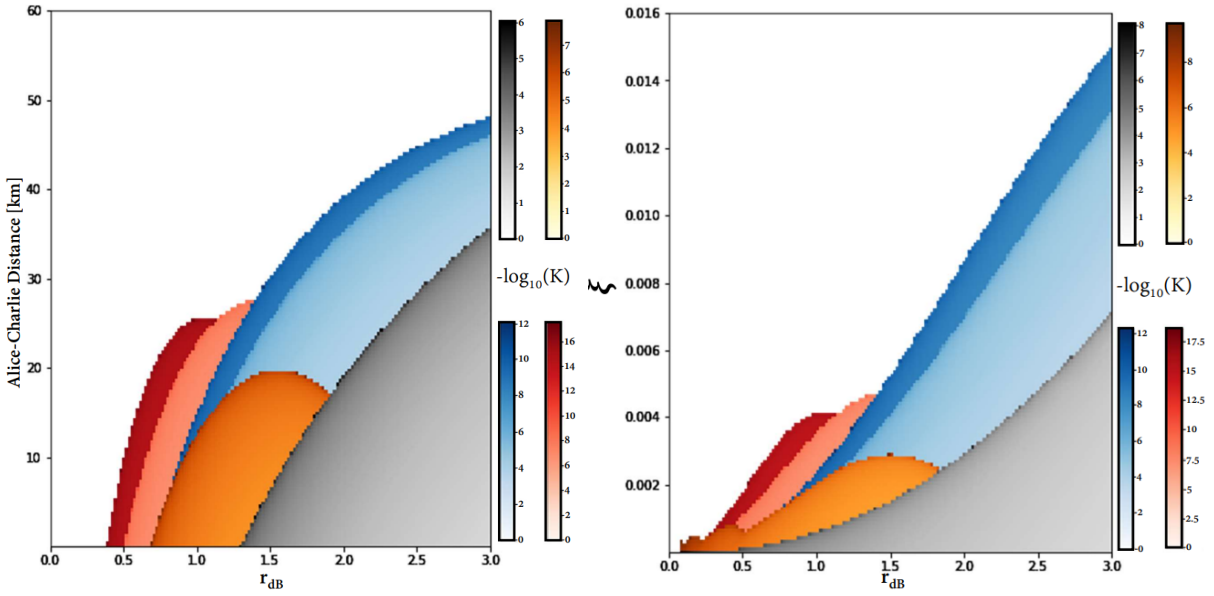
$$\left|\psi\right\rangle_{2PAS} = \mathcal{N}_2 \sum_{n=0}^{\infty} \sqrt{1-\lambda^2}\lambda^n T^{4n}(1-T^2)^2(n+1)^2\left|nn\right\rangle \tag{7.1.5}$$

where $\mathcal{N}_1$ and $\mathcal{N}_2$ are normalization constants associated to the probability of success $\mathcal{P}$ as

$$\mathcal{N}_1^{-2} = \mathcal{P}_1 = \frac{(1-\lambda^2)(1-T^2)^2\left(\zeta_1+1\right)}{(1-\zeta_1)^3}$$

$$\mathcal{N}_2^{-2} = \mathcal{P}_2 = (1-\lambda^2)(1-T^2)^4\left[\frac{-16\zeta_2^4-\zeta_2^3-11\zeta^2+5\zeta_2-1}{\zeta_2^5-5\zeta_2^4+10\zeta_2^3-10\zeta_2^2+5\zeta_2-1}\right]$$

given that $\zeta_1 = \lambda^2T^4$ and $\zeta_2 = \lambda^2T^8$. These normalization factors are calculated by first taking the inner product of the state in question and setting it equal to 1. Now we can use numerical methods to evaluate the secret key rate and log-negativity for these state as done previously. We have also plotted the performance of 2 mode photon replaced state as given in [1].



(a) (b)

Figure 7.2.1: Heat map of -$\log_{10}$(Key Rate) of CV-MDI-QKD protocol set at $\beta = 0.95$ as a function of initial squeezing r_{dB} and (a) channel length from Alice to Charlie with fixed ξ at 0.008, (b) total excess noise ξ with fixed channel length at 25km. Plotted key rates are for TMSV (Gray), 1-PAS state (Blue), 2-PAS state (Red) and 2-PR state (Brown).

7.2 Log-negativity and key rate

Logarithmic negativity is useful in our situation to assess how much entanglement is increased in these states. It is easy to calculate as well, we simply use (7.1.2) and (7.1.5) in (6.3.1) to generate Fig. 7.1.3 at two different values of squeezing.

We observe the performance of this protocol in the low squeezing regime of $r_{dB} \leq$ 3dB. r_{dB} is a measure of squeezing parameter r in units of decibel related as $r_{dB} = 10\ \log_{10}(e^{2r})$ (recall that $\lambda = tanh(r)$ and r is the squeezing parameter).

We choose 2 different squeezing values to highlight one of our findings. Recall that E_N is an upper bound on the amount of entanglement that can be distilled from a mixed state, naturally it would seem right to deduce that states with higher E_N would perform better when implemented in QKD. Such is not the case, note that in Fig. 7.1.3 (a) E_N of 2-PR state stays slightly above 2-PAS state when $\lambda = 0.1$ ($r_{dB} = 0.87$). While 2-PR state has higher E_N, transmission distance achievable in MDI-QKD using 2-PAS state is longer than 2-PR state (from Fig. 7.2.1 (a)). Another point is that between 7.1.3 (a) and (b), E_N of 2-PAS state stays above 1-PAS state but when we look at Fig. 7.2.1, 1-PAS state outperforms 2-PAS state at and beyond $\lambda = 0.172$ ($r_{dB} = 1.5$) in terms of key rate and distance achievable.

To show the practicality of this protocol, we used parameters that are closer to actual apparatus. Total excess thermal noise ξ is set to 0.008 ($\xi_A = \xi_B = 0.004$) which is twice the noise from [33]. Simulations ran taking Alice-Charlie distance to be 25km which is in the metropolitan scale and Charlie-Bob distance as 0km (extreme asymmetric setting). 2-PR state also offers some improvement, albeit in a very limited region, but reinforces the deduction that E_N is not directly proportional to improved performance in QKD. Non-overlapped graph of the performance of all states is given below.

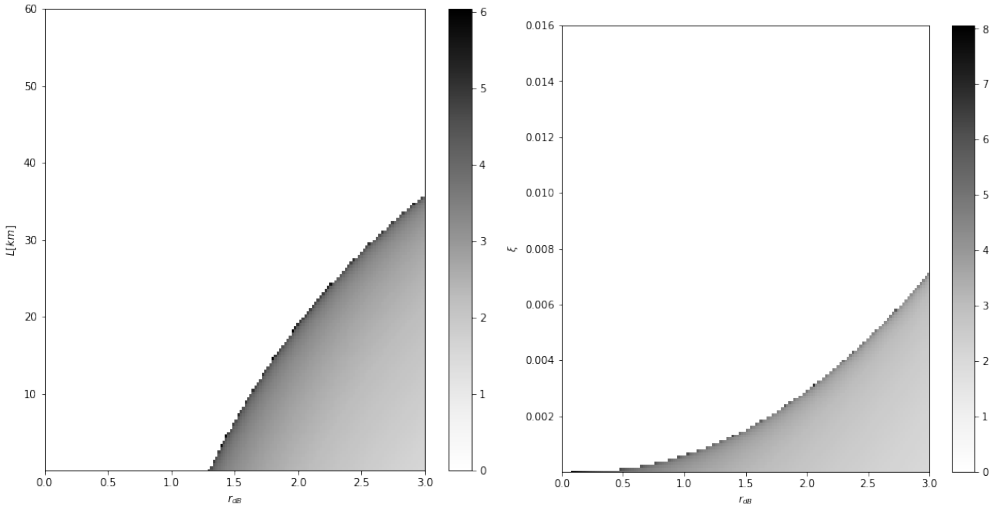


Figure 7.2.2: TMSV

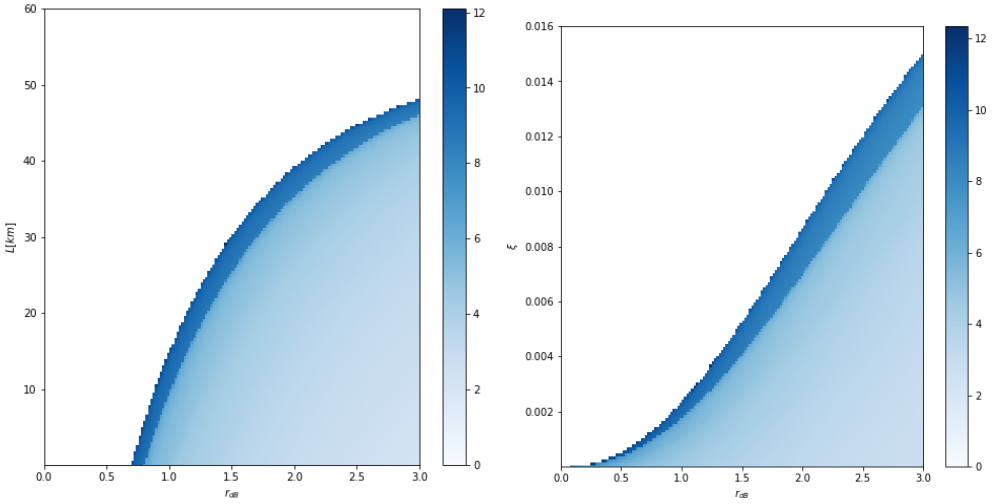


Figure 7.2.3: 1-PAS

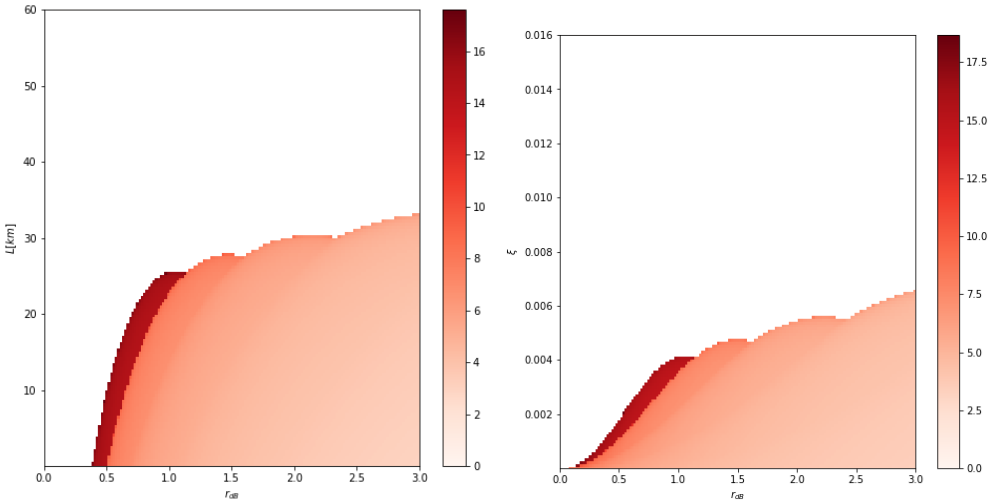


Figure 7.2.4: 2-PAS

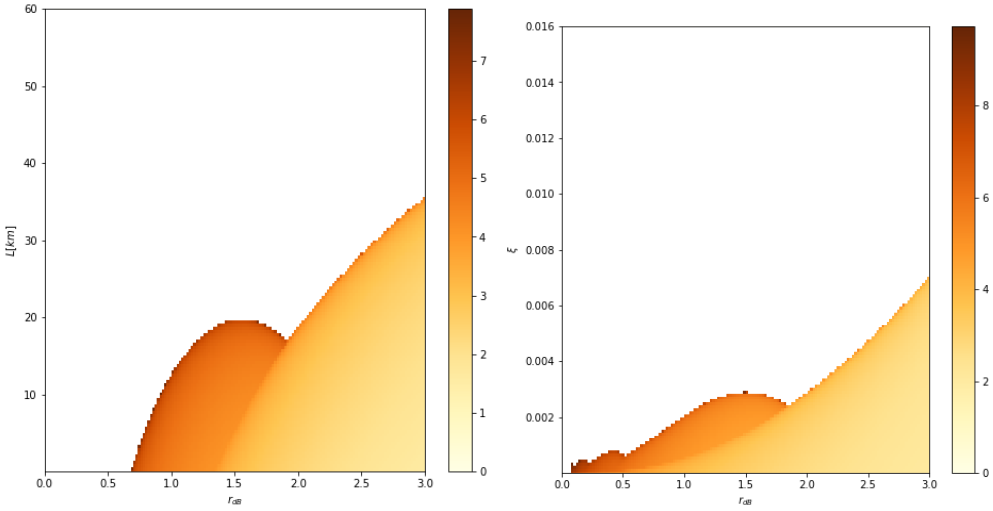


Figure 7.2.5: 2-PR

Chapter 8

Conclusion

In this thesis we have explained how QKD plays a crucial role in making sure our day-to-day communication can be unconditionally secured by using quantum packets. The two states that achieve this are either discrete in nature or continuous. Advantages offered by continuous states supersede discrete states when practicality is concerned.

Initial focus of the thesis is on developing a set of tools that can simulate any Gaussian protocol. Later we discussed how non-Gaussian protocols are accommodated. This generalized approach is strictly limited to Gaussian collective attacks in the asymptotic regime.

Being a new topic, there is much work needed in bridging the gap between theoretical models and practical parameters. Pure Gaussian entangled states are hard to produce and maintain so pure-state protocols are often modified by non-Gaussian operations for improvements. An inefficient (but fool proof) method to achieve this is to derive every modification in pure state and test their performance, since their is no definite relation between entanglement improving operations and better QKD performance, each state must be created simulated separately. To make this step efficient, we utilize programming to test as well as create non-Gaussian states with given parameters. This allowed us to rapidly test many combinations of non-Gaussian operations on TMSV pre and post channel loss as well as operating at Alice or Bob's station (or both). This model works for Gaussian collective attacks (in the asymptotic regime) which is enough to approximate the practical performance.

An improvement to CV-MDI protocol was observed when non-Gaussian operations are employed at Alice's station. Specifically a photon added-then-subtracted operation on TMSV state improves the performance of CV-MDI-QKD when available squeezing is lower than 3dB. Achievable maximum distance and tolerable thermal noise are both improved for 1-PAS, 2-PAS and 2-PR state. These

operations can work at very low squeezing of about 1dB to extend transmission distance up to 25km when standard losses are considered, note that in this domain previously proposed single photon subtracted [18] and zero photon catalysis [31] does not generate positive key rate while a pure TMSV state can be outperformed by our proposed non-Gaussian states. Our version of this protocol enables positive key rate at metropolitan distances under practical assumptions allowing it to be deployed quickly and cost effectively.

Another result shown is that no direct relation between log-negativity and QKD can be deduced from higher values alone. If not working with a general program, a plausible guess would be using states that increase entanglement of pure TMSV, we show that states with higher entanglement are not always the best choice for a better performing protocol in a certain domain which reinforces the need to work with a generalized program.

Appendices

Appendix A

Explicit calculation of TMSV CM

A complete derivation of TMSV covariance matrix from operations on the state vector can be found in [16]. We take a different approach that utilizes symplectic operations. The schematic of this method can be seen in Figure 3.2.1. TMSV can be generated by mixing a single mode position squeezed and a single mode momentum squeezed state on a balanced beam splitter. This operation can be mathematically expressed as follows:

$$\Gamma_{TMSV} = \hat{B}\Gamma^{'}\hat{B}^{T}$$

Under the assumption that both single modes have the same squeezing parameter, the combined covariance matrix $\Gamma^{'}$ is:

$$\Gamma^{'} = \begin{pmatrix} e^{-2r} & 0 & 0 & 0 \\ 0 & e^{2r} & 0 & 0 \\ 0 & 0 & e^{2r} & 0 \\ 0 & 0 & 0 & e^{-2r} \end{pmatrix} = \begin{pmatrix} V^{'} & 0 & 0 & 0 \\ 0 & \frac{1}{V^{'}} & 0 & 0 \\ 0 & 0 & \frac{1}{V^{'}} & 0 \\ 0 & 0 & 0 & V^{'} \end{pmatrix}$$

And the balanced two mode beam splitter $\hat{B}$ is given as (using (4.1.1)):

$$\hat{B} = \begin{pmatrix} \sqrt{\frac{1}{2}} & 0 & \sqrt{1-\frac{1}{2}} & 0 \\ 0 & \sqrt{\frac{1}{2}} & 0 & \sqrt{1-\frac{1}{2}} \\ \sqrt{1-\frac{1}{2}} & 0 & \sqrt{\frac{1}{2}} & 0 \\ 0 & \sqrt{1-\frac{1}{2}} & 0 & \sqrt{\frac{1}{2}} \end{pmatrix}$$

After applying these operations, we get:

$$\begin{pmatrix} \frac{V'}{2}+\frac{1}{2V'} & 0 & -\frac{V'}{2}+\frac{1}{2V'} & 0 \\ 0 & \frac{V'}{2}+\frac{1}{2V'} & 0 & \frac{V'}{2}-\frac{1}{2V'} \\ -\frac{V'}{2}+\frac{1}{2V'} & 0 & \frac{V'}{2}+\frac{1}{2V'} & 0 \\ 0 & \frac{V'}{2}-\frac{1}{2V'} & 0 & \frac{V'}{2}+\frac{1}{2V'} \end{pmatrix} \tag{A.0.1}$$

Note that all diagonal elements are equal and the off diagonal elements are negatively equal to each other. As we know that diagonal elements are the variances of the quadratures, we can relabel them as follows:

$$\frac{1}{2}\big(V'+\frac{1}{V'}\big)=\frac{1}{2}\tilde{V}$$

Solving this equation for V' gives us the following relation:

$$V'=\frac{1}{2}\big(\tilde{V}+\sqrt{\tilde{V}^2-4}\big)$$

Substituting these values in (A.0.1) gives:

$$\begin{pmatrix} \frac{\tilde{V}}{2} & 0 & \frac{1}{2}\big(\tilde{V}-2V'\big) & 0 \\ 0 & \frac{\tilde{V}}{2} & 0 & -\frac{1}{2}\big(\tilde{V}-2V'\big) \\ \frac{1}{2}\big(\tilde{V}-2V'\big) & 0 & \frac{\tilde{V}}{2} & 0 \\ 0 & -\frac{1}{2}\big(\tilde{V}-2V'\big) & 0 & \frac{\tilde{V}}{2} \end{pmatrix} \tag{A.0.2}$$

Explicitly solving the off diagonal elements:

$$\begin{aligned} \frac{1}{2}\big(\tilde{V}-2V'\big) &= \frac{1}{2}\Big(\tilde{V}-2\big(\frac{1}{2}\big(\tilde{V}+\sqrt{\tilde{V}^2-4}\big)\big)\Big) \\ &= \frac{1}{2}\Big(\tilde{V}-\tilde{V}+\sqrt{\tilde{V}^2-4}\Big) \\ &= \frac{1}{2}\sqrt{\tilde{V}^2-4} \\ &= \sqrt{\frac{\tilde{V}^2-4}{4}} \end{aligned}$$

With this value of off diagonal elements, (A.0.2) simplifies to:

$$\begin{pmatrix} \frac{\tilde{V}}{2} & 0 & \sqrt{\frac{\tilde{V}^2-4}{4}} & 0 \\ 0 & \frac{\tilde{V}}{2} & 0 & -\sqrt{\frac{\tilde{V}^2-4}{4}} \\ \sqrt{\frac{\tilde{V}^2-4}{4}} & 0 & \frac{\tilde{V}}{2} & 0 \\ 0 & -\sqrt{\frac{\tilde{V}^2-4}{4}} & 0 & \frac{\tilde{V}}{2} \end{pmatrix} \tag{A.0.3}$$

If we substitute $\frac{\tilde{V}}{2} = V$, the covariance matrix becomes the TMSV covariance matrix is as expressed in the original text:

$$\begin{pmatrix} V & 0 & \sqrt{V^2-1} & 0 \\ 0 & V & 0 & -\sqrt{V^2-1} \\ \sqrt{V^2-1} & 0 & V & 0 \\ 0 & -\sqrt{V^2-1} & 0 & V \end{pmatrix} \tag{A.0.4}$$

The relation between this new variance V is related to the individually squeezed variance V' as:

$$\begin{aligned} V &= \frac{1}{2}\tilde{V} \\ &= \frac{1}{2}\Big(V' + \frac{1}{V'}\Big) \end{aligned} \tag{A.0.5}$$

Appendix B

Python code

```
import numpy as np
import sympy as sp
from numpy.linalg import eig
from sympy.matrices import Matrix, Transpose, zeros, Inverse, Trace
from sympy import symbols,eye,log,sqrt,Abs,exp,ln,factorial


"""
Generalized simulator for a CV QKD setup under
collective attacks in the asymptotic regime

"""


# Shanon's entropy from symplectic eigen values
def G(x):
  f = ((1+x)/2)*log((1+x)/2,2) -((x-1)/2)*log((x-1)/2,2)
  return f


# Generalized Beam Splitter
#  (i = first mode,
#   j = second mode,
#   t = transmissivity of the BS,
#   c = covariance matrix)

def beam_splitter(i,j,t,c):
  n = len(np.array(c))
  i = i-1
  j = j-1
  BS = eye(n)
  BS[i,i] = sqrt(t)
  BS[i+1,i+1] = sqrt(t)
```

```
  BS[i,j] = sqrt((1-t))
  BS[i+1,j+1] = sqrt((1-t))
  BS[j,i] = -sqrt((1-t))
  BS[j+1,i+1] = -sqrt((1-t))
  BS[j,j] = sqrt(t)
  BS[j+1,j+1] = sqrt(t)
  BS_T = Transpose(BS)
  y = BS @ c @ BS_T
  return y


# Covariance Matrix for n uncoupled TMSV States

def CM_TMSV(primary=1,attack=0):
  V_sym = [sp.symbols('V_%d' %(i+1)) for i in range(primary)]
  W_sym = [sp.symbols('W_%d' %(i+1)) for i in range(attack)]
  K = Matrix([0])
  for o in range(len(V_sym)):
    K = K.diag(K,Matrix([
                [V_sym[o], 0, sqrt(V_sym[o]**2-1), 0],
                [0, V_sym[o], 0, -sqrt(V_sym[o]**2-1)],
                [sqrt(V_sym[o]**2-1), 0, V_sym[o], 0],
                [0, -sqrt(V_sym[o]**2-1), 0, V_sym[o]]
                ]))
  for c in range(len(W_sym)):
    K = K.diag(K,Matrix([
                [W_sym[c], 0, sqrt(W_sym[c]**2-1), 0],
                [0, W_sym[c], 0, -sqrt(W_sym[c]**2-1)],
                [sqrt(W_sym[c]**2-1), 0, W_sym[c], 0],
                [0, -sqrt(W_sym[c]**2-1), 0, W_sym[c]]
                  ]))
  K.col_del(0)
  K.row_del(0)
  return K

# Pull out a sub matrix from a bigger matrix
#(lower row, upper row, lower column, upper column, matrix)
def mode_M_separator(r_low, r_up, c_low, c_up, matrix):
  r = r_up - r_low + 1
  c = c_up - c_low + 1
  k = zeros(r,c)
  r_up = r_up - 1
  r_low = r_low - 1
  c_up = c_up - 1
  c_low = c_low - 1
  for i in range(r):
    for j in range(c):
      k[i,j] = matrix[i+r_low,j+c_low]
  return k
```

```
# partial measurements
#   [format: the two measured modes should be
#   on the lower right side of the covariance matrix]
def partial_homodyne_q(M):
  Piq = Matrix([[1,0],
                [0,0]])
  n = len(np.array(M))
  r0 = n-1
  r1 = n
  c0 = n-1
  c1 = n
  A = mode_M_separator(1, r0-1, 1, c0-1, M)
  C = mode_M_separator(1, r0-1, c0, c1, M)
  B = mode_M_separator(r0, r1, c0, c1, M)
  V = A - (C*((Piq*B*Piq).pinv())*Transpose(C))
  return V

def partial_homodyne_p(M):
  Pip = Matrix([[0,0],
                [0,1]])
  n = len(np.array(M))
  r0 = n-1
  r1 = n
  c0 = n-1
  c1 = n
  A = mode_M_separator(1, r0-1, 1, c0-1, M)
  C = mode_M_separator(1, r0-1, c0, c1, M)
  B = mode_M_separator(r0, r1, c0, c1, M)
  V = A - (C*((Pip*B*Pip).pinv())*Transpose(C))
  return V

def partial_heterodyne(M):
  w = Matrix([[0,1],
              [-1,0]])
  n = len(np.array(M))
  r0 = n-1
  r1 = n
  c0 = n-1
  c1 = n
  A = mode_M_separator(1, r0-1, 1, c0-1, M)
  C = mode_M_separator(1, r0-1, c0, c1, M)
  B = mode_M_separator(r0, r1, c0, c1, M)
  th = B.det() + Trace(B) + 1
  V = A - (1/th)*(C*(w*B*Transpose(w) + eye(2))*Transpose(C))
  return V


# Intakes float-valued 4x4 covariance matrix shared by party A and B
# Optionally: takes the efficiency of sifting (1 by default)
# and reconciliation efficiency (1 by default)
```

```
def hom_key_rate(Sigma,sifting = 1,beta = 1):
  O2 = Matrix([[0,1,0,0],[-1,0,0,0],[0,0,0,1],[0,0,-1,0]])
  # I_AB
  m = Sigma
  vqb = m[0,0]
  vqbqa = m[0,0] - (m[0,2]**2)/(m[2,2])
  vpb = m[1,1]
  vpbpa = m[1,1] - (m[1,3]**2)/(m[3,3])
  i = eye(2)
  i[0,0] = Abs((0.5*log(vqb/vqbqa,2)).doit())
  i[1,1] = Abs((0.5*log(vpb/vpbpa,2)).doit())
  p1 = max(i)
  # X_EB
  mab = Sigma
  mab2 = Sigma
  mab = 1j*O2*mab
  q = mab.eigenvals()
  q = list(q.items())
  q = np.array(q)
  c1 = floor(Abs(q[0][0])*10**20)
  c2 = floor(Abs(q[1][0])*10**20)
  if len(q) != 2:
    if c1 == c2:
      v1 = Abs(q[0][0])
      v2 = Abs(q[2][0])
    else:
      v1 = Abs(q[0][0])
      v2 = Abs(q[1][0])
  elif len(q) == 2:
    v1 = Abs(q[0][0])
    v2 = Abs(q[1][0])
  else:
    print('Unbound␣eigen␣value␣array')
  meb = eye(2)
  meb[0,0] = sqrt(mab2[0,0]*(mab2[0,0] - (1/(mab2[2,2]))*(mab2[0,2]**2)))
  meb[1,1] = sqrt(mab2[1,1]*(mab2[1,1] - (1/(mab2[3,3]))*(mab2[1,3]**2)))
  X = eye(2)
  X[0,0] = (G(v1) + G(v2) - G(meb[0,0])).evalf()
  X[1,1] = (G(v1) + G(v2) - G(meb[1,1])).evalf()
  p2 = max(X)
  # K
  p = (sifting*beta*p1 - sifting*p2).evalf()
  return p

def het_key_rate(Sigma,sifting=1,beta = 1):
  O2 = Matrix([[0,1,0,0],[-1,0,0,0],[0,0,0,1],[0,0,-1,0]])
  # I_AB
  m = Sigma
  vqb = m[0,0] + 1
```

```
    vqbqa = m[0,0] + 1 - Abs((m[0,2]**2))/(m[2,2] + 1)
    vpb = m[1,1] + 1
    vpbpa = m[1,1] + 1 - Abs((m[1,3]**2))/(m[3,3] + 1)
    i = eye(2)
    i[0,0] = Abs((log(vqb/vqbqa,2)).evalf())
    i[1,1] = Abs((log(vpb/vpbpa,2)).evalf())
    p1 = max(i)
    # X
    mab = Sigma
    mab2 = Sigma
    mab = 1j*O2*mab
    q = mab.eigenvals()
    q = list(q.items())
    q = np.array(q)
    c1 = floor(Abs(q[0][0])*10**20)
    c2 = floor(Abs(q[1][0])*10**20)
    if len(q) != 2:
      if c1 == c2:
        v1 = Abs(q[0][0])
        v2 = Abs(q[2][0])
      else:
        v1 = Abs(q[0][0])
        v2 = Abs(q[1][0])
    elif len(q) == 2:
      v1 = Abs(q[0][0])
      v2 = Abs(q[1][0])
    else:
      print('Unbound␣eigen␣value␣array')

    meb = eye(2)
    meb[0,0] = mab2[0,0] - (1/(mab2[2,2] + 1))*(mab2[0,2]**2)
    meb[1,1] = mab2[1,1] - (1/(mab2[3,3] + 1))*(mab2[1,3]**2)
    X = eye(2)
    X[0,0] = (G(v1) + G(v2) - G(meb[0,0])).evalf()
    X[1,1] = (G(v1) + G(v2) - G(meb[1,1])).evalf()
    p2 = max(X)
    # K
    p = (sifting*beta*p1 - sifting*p2).evalf()
    return p

# Standard form homodyne key rate for faster calculations
# Usable only for standard form 1
def s_hom_key_rate(M,recon):
    a = M[0,0]
    b = M[2,2]
    c = M[0,2]
    delta = a**2 + b**2 - 2*c**2
    iab = 0.5*log(a/(a - (c**2/b)),2)
    v1 = sqrt(0.5*(delta + sqrt(delta**2 - 4*M.det())))
    v2 = sqrt(0.5*(delta - sqrt(delta**2 - 4*M.det())))
```

```
    v3 = sqrt(a*(a-(c**2/b)))
    xeb = G(v1) + G(v2) - G(v3)
    k = complex(recon*iab - xeb)
    if k.imag>10**-8:
      print(k.imag)
    return k.real

# Standard form heterodyne key rate
def s_het_key_rate(M,recon):
    a = M[0,0]
    b = M[2,2]
    c = M[0,2]
    delta = a**2 + b**2 - 2*c**2
    iab = log((a+1)/(a+1 - (c**2/(b+1))),2)
    v1 = sqrt(0.5*(delta + sqrt(delta**2 - 4*M.det())))
    v2 = sqrt(0.5*(delta - sqrt(delta**2 - 4*M.det())))
    v3 = a-(c**2/(b+1))
    xeb = G(v1) + G(v2) - G(v3)
    k = complex(recon*iab - xeb)
    if k.imag>10**-8:
      print(k.imag)
    return k.real

# standardize covariance matrix to standard form-1
# Works only for an already diagonalized A,B,C
def standard_form(m):
    mab = m
    A = Matrix([ [mab[0,0],mab[0,1]],[mab[1,0],mab[1,1]] ])
    B = Matrix([ [mab[2,2],mab[2,3]],[mab[3,2],mab[3,3]] ])
    C = Matrix([ [mab[0,2],mab[0,3]],[mab[1,2],mab[1,3]] ])
    ro = symbols('r_o')
    Sqo = Matrix([[exp(-ro),0],[0,exp(ro)]])

    ro1 = (ln(A[0,0]) - ln(A[1,1]))/4
    ro2 = (ln(B[0,0]) - ln(B[1,1]))/4

    s1 = Sqo.subs(ro,ro1)
    s2 = Sqo.subs(ro,ro2)
    s = s1.diag(s1,s2)
    s = (1/(s1.det())**2)*(1/(s2.det())**2) * s
    St = s*m*Transpose(s)
    return St

# Checks for standard form 1
def diagonality_test(m):
    a = m[0,0] - m[1,1]
    b = m[2,2] - m[3,3]
    if a < 10**-20 and b < 10**-20:
      return True
    else:
```

```
    return False

# Move modes inside a matrix
def move_mode(i,j,m):
  v = len(np.array(m))
  i = i-1
  j = j-1
  d1 = zeros(v)
  d2 = zeros(v)
  for p1 in range(v):
    for p2 in range(v):
      d1[p1,p2] = m[p1,p2]
      d2[p1,p2] = m[p1,p2]
  for c in range(v):
    if c==i or c==i+1 or c==j or c==j+1:
      a=1
    else:
      d1[c,i] = d2[c,j]
      d1[c,i+1] = d2[c,j+1]
      d1[i,c] = d2[j,c]
      d1[i+1,c] = d2[j+1,c]
  for c in range(v):
    if c==i or c==i+1 or c==j or c==j+1:
      a=1
    else:
      d1[c,j] = d2[c,i]
      d1[c,j+1] = d2[c,i+1]
      d1[j,c] = d2[i,c]
      d1[j+1,c] = d2[i+1,c]
  d1[i,i] = d2[j,j]
  d1[i+1,i+1] = d2[j+1,j+1]
  d1[j,j] = d2[i,i]
  d1[j+1,j+1] = d2[i+1,i+1]
  return d1

# Implement entangling cloner attack on i'th mode
# (i = mode index, cm = covariance matrix,
    err = line error, tc = channel transmittance)
def attack_mode(i,cm,err,tc):
  w = 1 + (err)/(1-tc)
  attack = Matrix([[w,0,sqrt((w**2-1)),0],
                   [0,w,0,-sqrt((w**2-1))],
                   [sqrt((w**2-1)),0,w,0],
                   [0,-sqrt((w**2-1)),0,w]])
  cm = cm.diag(cm, attack)
  cm = beam_splitter(i,len(np.array(cm))-1,tc,cm)
  cm = mode_M_separator(1,len(np.array(cm))-4,1,len(np.array(cm))-4,cm)
  return cm
```

Bibliography

[1] Tim J Bartley and Ian A Walmsley. Directly comparing entanglement-enhancing non-gaussian operations. *New Journal of Physics*, 17(2):023038, feb 2015.

[2] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, 2014. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[3] N. J. Cerf, M. Lévy, and G. Van Assche. Quantum distribution of gaussian keys using squeezed states. *Phys. Rev. A*, 63:052311, Apr 2001.

[4] Winter Devetak. Distillation of secret key and entanglement from quantum states. *Royal Society publishing*, 01 2005.

[5] Eleni Diamanti. Security and implementation of differential phase shift quantum key distribution systems. *Physical Review A*, 01 2006.

[6] Lu-Ming Duan, G. Giedke, J. I. Cirac, and P. Zoller. Inseparability criterion for continuous variable systems. *Physical Review Letters*, 84(12):2722–2725, mar 2000.

[7] M. Eisaman, Jingwen Fan, Alan Migdall, and Sergey Polyakov. Invited review article: Single-photon sources and detectors. *The Review of scientific instruments*, 82:071101, 07 2011.

[8] J. Eisert, S. Scheel, and M. B. Plenio. Distilling gaussian states with gaussian operations is impossible. *Phys. Rev. Lett.*, 89:137903, Sep 2002.

[9] Raúl García-Patrón and Nicolas J. Cerf. Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.*, 97:190503, Nov 2006.

[10] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and Ph. Grangier. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables, 2003.

[11] Frédéric Grosshans and Philippe Grangier. Reverse reconciliation protocols for quantum cryptography with continuous variables, 2002.

[12] A. S. Holevo, M. Sohma, and O. Hirota. Capacity of quantum gaussian channels. *Phys. Rev. A*, 59:1820–1828, Mar 1999.

[13] Liyun Hu, M. Al-amri, Zeyang Liao, and M. S. Zubairy. Continuous-variable quantum key distribution with non-gaussian operations. *Phys. Rev. A*, 102:012608, Jul 2020.

[14] Lane P. Hughston, Richard Jozsa, and William K. Wootters. A complete classification of quantum ensembles having a given density matrix. *Physics Letters A*, 183(1):14–18, 1993.

[15] Fotini Karinou, Hans H. Brunner, Chi-Hang Fred Fung, Lucian C. Comandar, Stefano Bettelli, David Hillerkuss, Maxim Kuschnerov, Spiros Mikroulis, Dawei Wang, Changsong Xie, Momtchil Peev, and Andreas Poppe. Toward the integration of cv quantum key distribution in deployed optical networks. *IEEE Photonics Technology Letters*, 30(7):650–653, 2018.

[16] Fabian Laudenbach, Christoph Pacher, Chi-Hang Fred Fung, Andreas Poppe, Momtchil Peev, Bernhard Schrenk, Michael Hentschel, Philip Walther, and Hannes Hübel. Continuous-variable quantum key distribution with gaussian modulation-the theory of practical implementations. *Advanced Quantum Technologies*, 1(1):1800011, jun 2018.

[17] A. I. Lvovsky. Squeezed light, 2014.

[18] 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.

[19] Yasamin Mardani, Ali Shafiei, Milad Ghadimi, and Mehdi Abdi. Continuous-variable entanglement distillation by cascaded photon replacement. *Phys. Rev. A*, 102:012407, Jul 2020.

[20] Klaus Mølmer. Non-gaussian states from continuous-wave gaussian light sources. *Phys. Rev. A*, 73:063804, Jun 2006.

[21] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. *Nature Communications*, 8(1), apr 2017.

[22] Alessio Serafini. *Quantum continuous variables: A Primer of Theoretical Methods*. CRC Press, 2017.

[23] Yun Shao, Yang Li, Heng Wang, Yan Pan, Yaodi Pi, Yichen Zhang, Wei Huang, and Bingjie Xu. Phase-reference intensity attack on continuous-variable quantum key distribution with a real local oscillator, 2021.

[24] Jaskaran Singh and Soumyakanti Bose. Non-gaussian operations in measurement-device-independent quantum key distribution. *Physical Review A*, 104(5), nov 2021.

[25] Daniel B. S. Soh, Constantin Brif, Patrick J. Coles, Norbert Lütkenhaus, Ryan M. Camacho, Junji Urayama, and Mohan Sarovar. Self-referenced continuous-variable quantum key distribution protocol. *Phys. Rev. X*, 5:041010, Oct 2015.

[26] G. Vidal and R. F. Werner. Computable measure of entanglement. *Phys. Rev. A*, 65:032314, Feb 2002.

[27] Christian Weedbrook, Stefano Pirandola, Raú l García-Patrón, Nicolas J. Cerf, Timothy C. Ralph, Jeffrey H. Shapiro, and Seth Lloyd. Gaussian quantum information. *Reviews of Modern Physics*, 84(2):621–669, may 2012.

[28] Christian Weedbrook, Stefano Pirandola, Seth Lloyd, and Timothy C. Ralph. Quantum cryptography approaching the classical limit. *Physical Review Letters*, 105(11), sep 2010.

[29] Christian Weedbrook, Stefano Pirandola, and Timothy C. Ralph. Continuous-variable quantum key distribution using thermal states. *Physical Review A*, 86(2), aug 2012.

[30] Wei Ye, Hai Zhong, Xiaodong Wu, Liyun Hu, and Ying Guo. Continuous-variable measurement-device-independent quantum key distribution via quantum catalysis, 2019.

[31] Wei Ye, Hai Zhong, Xiaodong Wu, Liyun Hu, and Ying Guo. Continuous-variable measurement-device-independent quantum key distribution via quantum catalysis. *Quantum Information Processing*, 19(10):1–22, 2020.

[32] Yi-Chen Zhang, Ziyang Chen, Christian Weedbrook, Song Yu, and Hong Guo. Continuous-variable source-device-independent quantum key distribution against general attacks. *Nature*, 4 2020.

[33] Yi-Chen Zhang, Zhengyu Li, Song Yu, Wanyi Gu, Xiang Peng, and Hong Guo. Continuous-variable measurement-device-independent quantum key distribution using squeezed states. *Phys. Rev. A*, 90:052325, Nov 2014.