Quantum Discord, EPR Steering and Bell-type Correlations for Secure CV Quantum Communications

Sara Hosseini

A thesis submitted for the degree of
Doctor of Philosophy of the
The Australian National University

February 2017

Declaration

This thesis is an account of research undertaken between February 2012 and February 2016 at the *Department of Quantum Sciences*, *The Research School of Physics and Engineering* at the *Australian National University*, in Canberra, Australia.

Except where acknowledged in the customary manner, the material presented in this thesis is, to the best of my knowledge, original and has not been submitted in whole or part for a degree in any university.

Sara Hosseini
15 February 2017

I would like to dedicate this thesis to my parents and grand parents, who have been the greatest supporters and source of motivation for me through all my life.

Acknowledgments

My PhD at Quantum Optics group led by Prof. Ping Koy Lam at the Australian National University was a great opportunity for me to learn and work on one the advanced field of science and technology. This was a challenging, beautiful and extremely fruitful journey for me that I will remember and cherish through all my life. Many people played an important role during this journey helping me to accomplish it.

At first, I would like to sincerely thank Prof.Ping Koy Lam, my supervisor and head of the group. Ping Koy has always been very kind, positive, encouraging and supportive to me, wanting the best for me and for all the group members. The level of support that he provided and the kindness that he showed were more than what I expected. Without his moral, scientific and financial supports this would not be possible for me to accomplish this program.

Secondly I would like to thank my parents Akhtar Mirza and Mir. Mohammad Hosseini who have loved me unconditionally and supported me through all my life. This happened due to their encouragement and their tolerance and scarification during these four years while I was away from them in order to peruse my passions. I also would like to thank my two sisters; Narjis Hosseini and Syede Mona Hosseini, the true friends and supporters in my life, whose love warms my heart in the most difficult situations. Mona's two years presence in Canberra specially made my PhD much more enjoyable. Those years were surely remain one the most memorable time in our lives.

In addition, I would like to thank Thomas Symul, my very kind supervisor. It was a great opportunity for me to know Thomas and work under his supervision. He has always been very gentle and supportive. In addition, I would like to thank Ben Buchler for his kind and positive attitude towards me. I sincerely thank Syed M Assad, the kindest and the most intelligent person I know, and Jiri Janousek, the hero in the lab. From the beginning of my PhD both Assad and Jiri provided incredible level of support to me. I deeply enjoyed working and discussing scientific issues with them. I also thank my colleagues and the post-doctoral fellows in our group, who I have had chance to work with for their productive collaboration and kind support including Seiji Armstrong, Jing Yan Haw, Oliver Thearle, Geng Jiao, and the ones who I have not had the chance to collaborate, but I extremely enjoyed their company and friendship including Alexandre Brieussel, Giovanni Guccione, Pierre Vernaz-Gris, Zhao Jie, Geoff Campbell, Jesse Everett, Shen Yong and Daniel Higginbottom. Besides, I would like to thank the theorists that I had chance to collaborate with; Prof.Timothy C Ralph, Prof.Howard M Wiseman, Nathan Walk and Saleh Rahimi-Keshari. My special thanks also to Mahdi Hosseini and his wife Boshra Afra who helped me to

establish in Canberra.
I also would like to thank Dr. Lan fu for her help and positive attitude towards PhD students.
My sincere thanks to my best friends Dr. Farzaneh Kordbache and Mona Golestanfar for supporting me like a family members through all the years of my PhD.
Last but not the least, I would like to thank the administrators in our group, department and school; Amanda White, Laura Walmsley and Karen Nulty.

Abstract

Quantum states can be correlated in ways beyond what is possible for classical states. These correlations are considered as the main resource for quantum computation and communication tasks. In this thesis, I present my studies on the different forms of Quantum Correlations known as "Quantum Discord", "Einstein-Podolsky-Rosen(EPR) Steering" and "Bel-type correlations" in the continuous-variable quantum states and investigate their practical applications for the secure quantum communication.

While previously quantum entanglement was considered as the only form of quantum correlation, in the recent years a notion known as quantum discord which captures extra quantum correlations beyond entanglement was introduced by Ollivier and Zurek. This sort of non-classicality that can exist even in separable states, has raised so much aspiration for the potential applications, as they are less fragile than the entangled states. Therefore, of especial interest is to know if a bipartite quantum state is discordant or not. In this thesis I will describe the simple and efficient experimental technique that we have introduced and experimentally implemented to verify quantum discord in unknown Gaussian states and a certain class of non-Gaussian states. According to our method, the peak separation between the marginal distributions of one subsystem conditioned on two different outcomes of homodyne measurement conducted on the other subsystem is an indication of nonzero quantum discord. We implemented this method experimentally by preparing bipartite Gaussian and non-Gaussian states and proved nonzero quantum discord in all the prepared states.

Though quantum key distribution has become a mature technology, the possibility of hacking the devices used in the quantum communications has motivated the scientists to develop the schemes where one or non of the devices used by the communicating parties need to be trusted. Quantum correlations are the key to develop these schemes. Particularly, EPR steering is connected to the one-sided-device-independent quantum key distribution in which devices of one party are solely trusted and Bell-type correlations to the fully device-independent quantum key distribution where non of the apparatuses of the communicating parties is trusted. Here, I will present the result of our theoretical and experimental research to develop one-sided-device-independent quantum key distribution in continuous variables. We identify all Gaussian protocols that can in principle be one-sided-device-independent. This consists of 6 protocols out of 16 possible Gaussian protocols, which surprisingly includes the protocol that applies only coherent states. We experimentally implemented both the entanglement-based and coherent state protocols and manifested their loss tolerance. Our results open the door for the practical secure quantum communications, asserting the link between the EPR-steering and

one-sided-device-independence.
Due to the maturity of quantum information using continuous variables, it is important to develop a Bell-type inequality in this regime. Despite its fundamental importance, Bell-type correlation is linked to the device-independent quantum key distribution. I developed a computer modelling based on the proposal of ref [1, 2] to demonstrate continuous-variable Bell-type correlation. The results of my computer simulations that are presented in this thesis show the feasibility of these proposals, which makes the real-life implementation of continuous-variable device-independent quantum key distribution possible.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The peculiar nature of quantum entanglement was first indicated by Einstein, Podolsky and Rosen (EPR) in their famous seminal paper in 1935 [3]. This paradox which considers two main aspects of quantum mechanics; entanglement and uncertainty principle [4], was proposed to prove that the quantum mechanics was not complete in that current formalism and should include *local hidden variable* theories. Their controversial proposal raised so many debates in physics until 1964 when John Stewart Bell quantified local realistic theories through his famous inequality [5]. The violation of Bell's inequality guarantees that a pair of particles are genuinely entangled and their correlation cannot be described by any form of local theories.
The concept of quantum entanglement, later received tremendous amount of attention as the essential resource for quantum information tasks, including *"Quantum Key Distribution (QKD)"* [6, 7] which appeared by the proposals of Bennett and Brassard's [8] in 1984, and Ekert's [9] in 1991. This cryptographic technique which rely solely on the laws of quantum mechanics, promises unbreakable security, what human beings has endeavoured to achieve during the whole history!
Though the field of Quantum Key Distribution developed rapidly with so many success stories [10, 11, 12], it is soon realized that the real-life implementation might differ from the theoretical predictions. This means that unbreakable security will no longer be guaranteed, unless less or more realistic assumptions about the devices are considered. In order to tackle this problem, protocols with least amount of assumptions on devices were developed, now known as Device Independent QKD (DI-QKD) [13, 14]. However, DI-QKD requires the strong form of quantum non-locality (Bell's non-locality) to prove the unconditional security. The fact that the violation of the detection loop-hole free Bell test [15, 16] itself is a challenge to the experimental physics, makes a field implementation of the DI-QKD protocols currently troublesome.
One may think that less stringent form of quantum correlation may be advantageous, which is indeed true. An asymmetric form of quantum correlation known as *EPR-steering*, which was first proposed by Schrödinger in 1935 as a generalization of the EPR paradox [17] is linked to the new kind of quantum security, so called one-sided device independent QKD (1SDI-QKD) [18, 19]. In these protocols only the apparatuses of one of the communicating parties are reliable. In addition, the link between entanglement and uncertainty relations which was first mentioned by EPR has been quantified by Berta et al. in ref [20] by employing entropic version of uncertainty

relations [21, 22, 23, 24, 25]. This provided new means for cryptographers, which hand in hand with the concept of EPR-steering make the development of 1SDI-QKD protocols possible. The requirements to satisfy the 1SDI-QKD protocols are less strict than DI-QKD protocols which makes them an interesting candidate for practical applications.

One of the main focus of my thesis is the advancement of 1SDI-QKD protocols in continuous-variables which are presented in Chapters 5, 6 and 7. By using entropic version of uncertainty relations in continuous variables [26, 27, 28] , we lower bounded the asymptotic secret key rate of all the 16 possible Gaussian OKD protocols, and showed that only 6 of them can manifest one-sided device-independence. We implemented 5 of these 6 protocols experimentally and demonstrated that the best system using entangled source and homodyne-homodyne measurements can tolerate an applied loss of up to 1.5 dB. Surprisingly, we implemented a protocol that utilizes only coherent states as the source, and showed that it can tolerate an applied loss of up to 0.6 dB. This was the first demonstration of 1SDI-CVQKD using coherent states. The ease and the low price of producing coherent states compared to the entangled states, make these sources a very interesting candidate for short-range networks. I also developed a detailed computer modelling to understand our experimental setups and the potential for further improvements. Our theoretical and experimental research, further strengthen the link between the 1SDI-QKD and EPR-streeing.

Though entanglement is regarded as the essential tool for quantum computation and communication, the research during the last decade has proven that it is not the unique form of quantum correlation. A form of quantum correlation which can exist even in the separable states was introduced and characterized by Henderson and Vedral in 2001 [29] and separately by Ollivier and Zurek in 2001 [30]. Ollivier and Zurek named it *"Quantum Discord"*. This new form of quantum correlation which is more robust than entanglement has evoked large number of attention during the last decade, promising new asset for quantum information tasks. Due to the increasing interest in quantum discord and the difficulty of calculating it for an unknown quantum state, it is important to find a method to verify quantum discord in an unknown quantum state. We have introduced and implemented experimentally a straightforward method to verify quantum discord in unknown Gaussian states and non-Gaussian states that are prepared by overlapping a vacuum state and a statistical mixture of coherent states on a 50:50 beamsplitter. In Chapter 3, I present a through discussion on quantum discord and our discord verification method as well as the implementation and the results of our experimental survey .

In the Chapter 8 of my thesis, I discuss Bell's inequality and show how a CHSH inequality can be extended to continuous-variables according to the proposal of ref [1, 2]. I engaged in detailed modelling to understand these experimental setups and showed the possibility of implementing them using the current technology. This work is in the direction of developing unconditional security through device-independent QKD in continuous-variables.

1.1 Publications (Article and Conference paper)

A large part of the material presented in the following chapters are published in the peer-review journals or presented in conferences. The list of publications and conference proceedings are as follows:

- N. Walk, S. Hosseini, J. Geng, O. Thearle, J. Y. Haw, S. Armstrong, S. M. Assad, J. Janousek, T. C. Ralph, T. Symul, H. M. Wiseman and P. K. Lam. *"Experimental Demonstration of Gaussian Protocols for one-sided device independent quantum key distribution"*, Optica **3**(6), 634-642 (2016).

- S. Hosseini, S. Rahimi-Keshari, J. Y. Haw, S. M. Assad, H. Chrzanowski, J. Janousek, T. Symul, T. C. Ralph and P. K. Lam, *"Experimental Verification of Quantum Discord in Continuous-Variable States"*, J. Phys. B: At. Mol. Opt. Phys. **47**, 025503 (2014).

- H. Chrzanowski, N. Walk, S. M. Assad, J. Janousek, S. Hosseini, T. C. Ralph, T. Symul and P. K. Lam, *"Measurement-based Noiseless Linear Amplification for Quantum Communication"*, Nature Photonics **8**, 333-338 (2014).

- S. Hosseini, S. Rahimi-Keshari, J. Y. Haw, A. M. Syed, H. M. Chrzanowski, J. Janousek, T. Symul, T. Ralph, P. K. Lam, M. Gu, K. Modi, and V. Vedral, *"Experimental Verification of Quantum Discord and Operational Significance of Discord Consumption"*, in CLEO: 2014, OSA Technical Digest (online) (Optical Society of America, 2014), paper FTh3A.6.

- H. Chrzanowski, N. Walk, O. Thearle, S. M. Assad, J. Janousek, S. Hosseini, T. C. Ralph, T. Symul, P. K. Lam, *"Measurement-based Linear Amplification for quantum communication"*, Quantum and Nonlinear Optics III (2014).

- J. Janousek , H. Chrzanowski , S. Hosseini, S. M Assad, T. Symul, N. Walk, T. C Ralph, P. K. Lam, *"Virtual Noiseless Amplification"*, CLEO/Europe-IQEC 2013 Conference on Lasers and Electro-Optics-Int Quantum Electronics Conference (2013) 1.

1.2 Thesis Outline

The structure of my thesis is shown in figure 1.1. This thesis consists of four main parts. The first part provides the theoretical background necessary to understand the rest of the thesis. The second part concentrates on the concept of "Quantum Discord" and our proposed verification method and experimental implementation of it. The third part of this thesis, consists of four chapters, the first one reviews the concepts on the "secure quantum communications". The second chapter presents our proposed 1SDI-QKD protocols using Gaussian states and measurements and the experimental implementation of those protocols. The last part of this thesis studies Bell-like correlations.

Chapter 2: Theoretical Background.
In this chapter I provide the theoretical background on quantum optics which are necessary to understand the rest of the thesis. This includes quantisation of the electromagnetic field, quantum states of light, Wigner function and Gaussian states, quantum measurements, phase and amplitude modulation, classical and quantum information theory and quantum correlations.

Chapter 3: Experimental Verification of Quantum Discord in CV States.
In this chapter I review the concept of Quantum Discord, Gaussian quantum discord, and a general method to verify quantum discord. Then I present the experimental method that we proposed and implemented to verify quantum discord in continuous-variable (CV) states. I describe our theoretical development of the technique as well as the details of our experimental implementation including the description on different parts of our setup and present our results.

Chapter 4: Secure Quantum Communication.
In this chapter I looked at "Quantum Key Distribution" and the standard form of it. Then I introduce the proposed methods to close the gaps between theory and practical implementation of QKD protocols. These methods include "Device-Independent QKD", "Measurement-Device-Independent QKD" and "One-sided Device-Independent QKD". I reviewed large number of researches that developed these techniques.

Chapter 5: Theoretical Development of 1SDI-QKD Gaussian Protocols.
In this chapter I discuss the one-sided device-independent quantum key distribution and its connection to EPR steering, I present our theoretical analysis to derive the key rates for 1SDI-QKD protocols using Gaussian states and measurements. I elaborate all the concepts that help to understand our theoretical development; including entropic uncertainty relations, virtual entanglement and EPR-steering.

Chapter 6: Experimental Implementation of 1SDI-QKD Protocols in EB Scheme.
In this chapter I detail our experimental implementation of 1SDI-QKD protocols using an entangled source. I describe the technique and equipments that we used to generate amplitude squeezed light and entanglement and explain our control system and data aqcusition. I elucidate our experimental results, error estimation and the computer model that I developed to simulate our experiments.

Chapter 7: Experimental Implementation of 1SDI-QKD Protocols in P&M Scheme.
In this chapter I expound our experimental implementation of 1SDI-QKD protocols employing coherent states. I present the technical details of our experiment including the calibration method and data acquisition and control system. The result of this experiment is presented at the end of the chapter along with error estimation and computer modelling.

Chapter 8: Bell-like Correlations for Continuous-Variables.

This chapter is a brief report on our research on the possibility of the experimental demonstration of Bell-like correlation for continuous variables. Due to the progress of CV regime in quantum information, it is of particular interest to perform a Bell test using continuous sources and detections. This experiment is based on the proposal of ref [1, 2]. I conducted a computer simulations to understand these experimental setups and investigate is Bell's inequality can be violated using continuous variables. I present the details of my modelling and its result in this chapter.

Chapter 9: Conclusion.

This chapter concludes the whole thesis, suggesting the possible applications or the developments that can be done to improve our theoretical and experimental investigations.

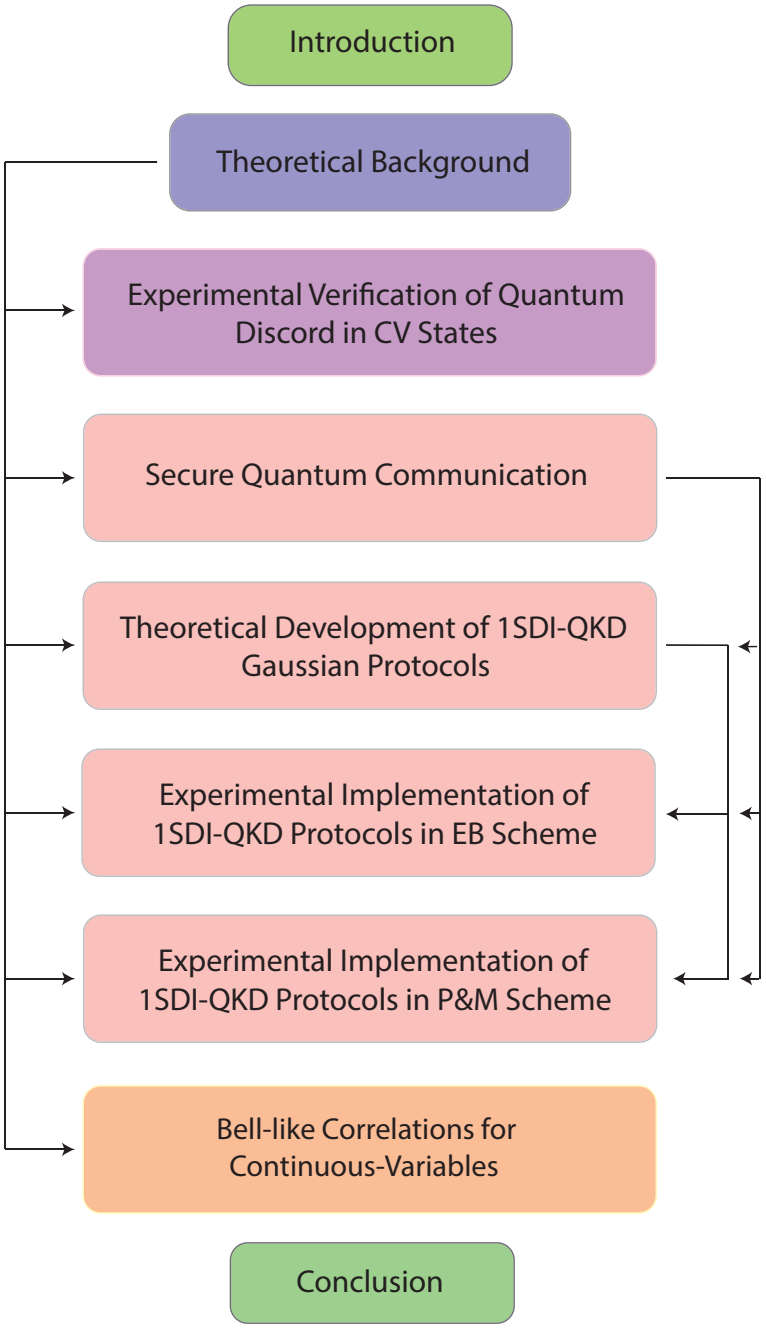


Figure 1.1: Structure of this thesis.

Chapter 2

Theoretical Background

2.1 Quantum Optics

Quantum optics is a field in which the optical phenomena can only be described employing the laws of quantum mechanics. The pioneering ideas of quantum theories of light started from 1901 with Planck's description of black-body radiation as discrete energy packets called *quanta*, followed up in 1905 by Einstein's explanation of the photoelectric effect applying Planck's hypothesis. The precise theory of quantum optics appeared after the birth of quantum mechanics with Dirac's seminal paper on quantum theory of radiation in 1927. However, looking for quantum effects associated with optical field was not important till 1963 after Glauber described new states of light with different statistical properties from classical light. Non-classical properties of light like photon antibunching were demonstrated experimentally by Kimble, Dagenais and Mandel in 1977 and squeezing in 1985 by Slusher et al. These led to the birth of the new and fast growing field of *Quantum Optics* with so many applications and other disciplines being involved with it like quantum information processing [31]. In this chapter I will review some of the key concepts of quantum optics and quantum information theory which will be used through out the entire thesis.

2.2 Quantisation of the electromagnetic field

Quantum description of light requires quantisation of the electromagnetic field. In order to quantize the electromagnetic field we can start from source free Maxwell equations [38]:

$$\nabla \cdot B = 0, \tag{2.1}$$

$$\nabla \times E = -\frac{\partial B}{\partial t}, \tag{2.2}$$

$$\nabla \cdot D = 0, \tag{2.3}$$

$$\nabla \times H = \frac{\partial D}{\partial t}, \tag{2.4}$$

Where $B = \mu_0 H$, $D = \varepsilon_0 E$, μ_0 is the magnetic permeability and ε_0 is the electric permittivity of free space. Considering the Coulomb gauge, $(\nabla \cdot A = 0)$, electric and magnetic fields can be derived from a vector potential $A(r,t)$ as follows [38]:

$$B = \nabla \times A\,, \tag{2.5}$$

$$E = -\frac{\partial A}{\partial t}\,, \tag{2.6}$$

Considering the equations (2.5) and (2.4), it is seen that the vector potential A obeys the wave equation. Hence, the vector potential can be described as follows [38]:

$$A(r,t) = \sum_k (\frac{\hbar}{2\omega_k \varepsilon_0})^{1/2} [a_k \mathbf{u_k}(\mathbf{r}) e^{-i\omega_k t} + a_k^\dagger \mathbf{u_k^*}(\mathbf{r}) e^{i\omega_k t}] \tag{2.7}$$

Where $\hbar$ is the Planck's constant, $\mathbf{u_k}(\mathbf{r})$ corresponds to the set of vector mode functions with frequency ω_k which satisfy the wave equation. This leads to the corresponding electric field as follows[38]:

$$E(r,t) = i\sum_k (\frac{\hbar\omega_k}{2\varepsilon_0})^{1/2} [a_k \mathbf{u_k}(\mathbf{r}) e^{-i\omega_k t} - a_k^\dagger \mathbf{u_k^*}(\mathbf{r}) e^{i\omega_k t}] \tag{2.8}$$

The normalization factors are chosen in a way to make the amplitudes a_k and $a_k^\dagger$ dimensionless. These amplitudes are complex numbers in classical electrodynamics. In order to quantize the electromagnetic field these amplitudes need to follow the bosonic commutation relationship [38]:

$$[\hat{a}_k, \hat{a}_{k'}] = [\hat{a}_k^\dagger, \hat{a}_{k'}^\dagger] = 0,\ [\hat{a}_k, \hat{a}_{k'}^\dagger] = \delta_{kk'} \tag{2.9}$$

Substituting equation (2.8) and the equivalent expression for H in the Hamiltonian of the electromagnetic field as $H = \frac{1}{2}\int (\varepsilon_0 E^2 + \mu_0 H^2)\, dr$, and making use of the commutation relations (2.9) one can write the quantum version of the Hamiltonian of the electromagnetic field as [38]:

$$H = \sum_k \hbar\omega_k (\hat{a}_k^\dagger \hat{a}_k + \frac{1}{2}) \tag{2.10}$$

This quantum representation of the Hamiltonian suggests that the energy of the electromagnetic field consists of the sum of the energies of the number of photons plus the energy of the vacuum fluctuation in each mode.

2.3 Quadratures of the electromagnetic field

Quadrature operators correspond to the two components of the electric fields which are 90^o out of phase with each other. Considering the amplitude of the k^{th} mode of

the optical field $\hat{a}_k$, quadrature operators are defined as:

$$\hat{q}_k = \frac{1}{\sqrt{2}}(\hat{a}_k^\dagger + \hat{a}_k) \tag{2.11}$$

$$\hat{p}_k = \frac{i}{\sqrt{2}}(\hat{a}_k^\dagger - \hat{a}_k) \tag{2.12}$$

which implies that :

$$\hat{a}_k = \frac{1}{\sqrt{2}}(\hat{q}_k + i\hat{p}_k) \tag{2.13}$$

From the bosonic commutation relation (2.9), it is seen that $\hat{q}_k$ and $\hat{p}_k$ are canonically conjugate observables, where k and l are two different modes of the optical field [39]:

$$[\hat{p}_k, \hat{q}_k] = i\hbar\delta_{kl}. \tag{2.14}$$

with the following uncertainty relationship :

$$\Delta\hat{p}_k \Delta\hat{q}_k \geq \hbar/2. \tag{2.15}$$

Hence the field quadratures fulfil the same uncertainty relation as the position and momentum operators of a harmonic oscillator. The uncertainty of field quadratures suggests that there must be some level of uncertainty in the estimation of the direction and magnitude of the electric field vector in a phasor diagram [31].
We can group together the canonical operators in a vector as follows:

$$\hat{\mathbf{R}} = (\hat{q}_1, \hat{p}_1, ..., \hat{q}_N, \hat{p}_N)^T, \tag{2.16}$$

using this vector we can write the compact form of the bosonic commutation relations between the quadrature operators as follows [32]:

$$[\hat{R}_k, \hat{R}_l] \;=\; i\hbar\Omega_{kl}, \tag{2.17}$$

where Ω is defined as :

$$\Omega = \bigoplus_{k=1}^{N} \omega, \qquad \omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{2.18}$$

I will use this compact form of quadrature operators later when I want to define the general form of Gaussian states.

2.4 Quantum States of Light

In this section I review several optical states which are important in quantum optics and most of them will be used in this thesis. This includes quadrature states, Fock

states, coherent states, thermal state and squeezed state.

2.4.1 Quadrature States

Quadrature states are the eigenstates of the quadrature operators $\hat{q}$ and $\hat{p}$ [39]. Considering the k_{th} mode of the optical field we have:

$$\hat{q}_k|q_k\rangle = q_k|q_k\rangle \tag{2.19}$$
$$\hat{p}_k|p_k\rangle = p_k|p_k\rangle \tag{2.20}$$

Due to the canonical commutation relation that the field quadratures obey, which is similar to the position and momentum, the spectrum of quadratures is unbounded and continuous. However, the quadrature states are not very useful as they are not exactly normalizable, while the quadrature wave functions $\psi(q) = \langle q|\psi\rangle$ and $\phi(p) = \langle p|\phi\rangle$ are useful and have physical meaning. In fact $|\psi(q)|^2$ and $|\phi(p)|^2$ are the quadrature probability distributions which are measured in quantum optics experiments using homodyne detection (see section 2.8 for description on homodyne detection) [39].

2.4.2 Fock States

Fock states or number states are the eigenstates of the number operator $N_k = \hat{a}_k^\dagger \hat{a}$ [38]:

$$\hat{a}_k^\dagger \hat{a}\,|n_k\rangle = n_k\,|n_k\rangle \tag{2.21}$$

$\hat{a}_k$ and $\hat{a}_k^\dagger$ are raising and lowering operators, which in respect of the photons they correspond to the creation and annihilation of a photon with a wave vector k and polarization $\hat{e}_k$. The effect of these operators on the number states are illustrated as follows[38]:

$$\hat{a}_k\,|n_k\rangle = \sqrt{n_k}\,|n_k - 1\rangle \tag{2.22}$$
$$\hat{a}_k^\dagger\,|n_k\rangle = \sqrt{n_k + 1}\,|n_k + 1\rangle \tag{2.23}$$

The ground state or the vacuum state is defined as [38]:

$$\hat{a}_k|0\rangle = 0 \tag{2.24}$$

This aids to characterize the energy of the ground state as [38]:

$$\langle 0|H|0\rangle = \frac{1}{2}\sum_k \hbar\omega_k. \tag{2.25}$$

By employing the creation operator successively, the state vector of the higher excited states can be built from the vacuum state [38]:

$$|n_k\rangle = \frac{(\hat{a}_k^\dagger)^{n_k}}{(n_k\,!)^{1/2}}|0\rangle, \quad n_k = 0, 1, 2, \ldots . \tag{2.26}$$

The number states form a complete set of basis vector for a Hilbert space, as they are orthogonal $\langle n_k|m_k\rangle = \delta_{mn}$ and complete $\sum_{n_k=0}^{\infty} |n_k\rangle\langle n_k| = 1$, and their norm is finite [38] .
Although the number states are useful basis for several problems in quantum optics, they are not good representation of optical fields with large number of photons which are generated in most quantum optics experiments [38]. In the following, I will review more realistic states in quantum optics.

2.4.3 Coherent States

Coherent states are the closest quantum mechanical states to the classical monochromatic electromagnetic wave. They consist infinite number of photons which make them suitable basis for many optical fields. The coherent states are generated by applying the unitary displacement operator on the vacuum state [38]:

$$|\alpha\rangle = D(\alpha)|0\rangle, \quad D(\alpha) = exp(\alpha\hat{a}^\dagger - \alpha^*\hat{a}) \tag{2.27}$$

Besides coherent states are the eigenstates of the annihilation operator $\hat{a}$ [38]

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle \tag{2.28}$$

Since the annihilation operator $\hat{a}$ is not Hermitian, the eigenvalues of $\hat{a}$ are complex. Hence, the coherent states have well-defined amplitude $|\alpha|$ and phase $arg\,\alpha$ corresponding to the complex wave amplitude and phase in classical optics.
Coherent states are the minimum uncertainty states, while the uncertainty of both quadratures are equal [38]:

$$\Delta q = \Delta p = 1. \tag{2.29}$$

We assumed that they follow the commutation relation as $[\hat{p}, \hat{q}] = 2i$ with $\hbar = 2$ [38]. This effect is shown in figure 2.1 using the phase diagram.
Since coherent states contain an infinite number of photons they can be expanded in terms of the number states [38]:

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum \frac{\alpha^n}{(n!)^{1/2}}|n\rangle \tag{2.30}$$

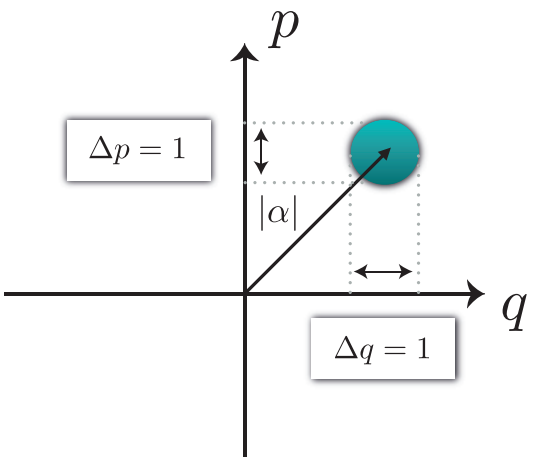


Figure 2.1: Phase-space representation of a coherent state.

This leads us to find the probability distribution of the photons in a coherent state to be Poissonian [38]:

$$P(n) = |\langle n|\alpha\rangle|^2 = \frac{|\alpha|^{2n} e^{-|\alpha|^2}}{n!}. \tag{2.31}$$

Further details on the coherent states can be found in references like [38, 39, 31].

2.4.4 Squeezed States

Squeezed states are another member of the family of the minimum uncertainty states. The uncertainty of one quadrature in these states is squeezed at the cost of the increase of the uncertainty at the other quadrature. This effect is shown in figure 2.2 using phasor diagram [38].

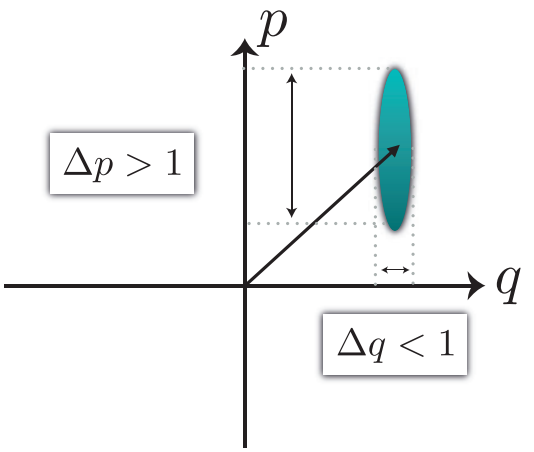


Figure 2.2: Phase-space representation of a squeezed state.

These states can be generated by applying the unitary squeezing operator [38]:

$$S(\varepsilon) = \exp(1/2\,\varepsilon^* a^2 - 1/2\,\varepsilon\, a^{\dagger 2}) \tag{2.32}$$

Where $\varepsilon = re^{2i\phi}$. The level of attenuation and amplification is given by the parameter $r = |\varepsilon|$, which is called the *squeezing factor*. To produce the squeezed state $|\alpha, \varepsilon\rangle$, at first the vacuum state should be squeezed and then displaced [38]:

$$|\alpha, \varepsilon\rangle = D(\alpha)S(\varepsilon)|0\rangle \tag{2.33}$$

Further details on squeezed states can be found in references like [38, 39, 31].

2.4.5 Thermal States

Before proceeding I will briefly mention the classification of the light based on "the standard deviation of their photon number distribution" [31]. This classification is illustrated in table2.1, where $\bar{n}$ implies the mean value of the photon numbers [31]. As suggested by table 2.1, a perfect coherent light source provides a Poissonian dis-

Table 2.1: Classification of light based on the photon statistics.[31]

Photon statistics	Classical equivalent	Δn
Super-Poissonian	Thermal or chaotic light	$> \sqrt{\bar{n}}$
Poissonian	Coherent light	$\sqrt{\bar{n}}$
Sub-Poissonian	non-classical	$< \sqrt{\bar{n}}$

tribution, while a sub-Poissonian distribution corresponds to the non-classical light. A super-Poissonian distribution of light appears when there are classical fluctuations in the intensity of light. This form of light is obviously noisier than the coherent light in terms of the classical intensity and quantum photon number fluctuations [31].

Thermal light, which is an electromagnetic radiation emitted from an object due to its temperature has super-Poissonian distribution. Its probability function for a single radiation mode consisting of n photons is defined as follows [31]:

$$P_\omega(n) = \frac{1}{\bar{n}+1}\left(\frac{\bar{n}}{\bar{n}+1}\right)^n \tag{2.34}$$

Where ω, n and $\bar{n}$ refer to the angular frequency of the single radiation mode, the photon number and the mean value of the photon number respectively. This distribution, which is famous as **"Bose-Einstein distribution"**, has a variance of [31]:

$$(\Delta n)^2 = \bar{n} + \bar{n}^2 \tag{2.35}$$

This single mode variance can be described using Einstein's interpretation of the energy fluctuations of the black-body radiation. According to him, the first term

in equation (2.35) arises from the quantum nature of light, while the second term emerges from the thermal fluctuations, hence has classical origin [31]. More details can be found in ref [31].

2.5 Wigner Function

The Wigner function which was initiated by Wigner in 1932, aims to define a probability distribution in quantum mechanics. However, due to the restriction imposed by Heisenberg uncertainty relation [4] on the observation of conjugate variables, this is not in general possible. Hence, the probability distributions in quantum mechanics are called *"Quasiprobability distributions"* [39]. Since in quantum mechanics, the objective is to find the expectation values of the physical observables, it is possible to define a Wigner function in a way that can produce these expectation values. In fact, the correct Weyl inverse transform is also necessary to complete this picture, otherwise the Wigner function is more or less a tool to envisage the quantum states [40]. The inverse Weyl transform $\tilde{A}$ is defined as follows [40]:

$$\tilde{A}(x,p) = \int e^{-ipy/\hbar} \langle x + y/2 | \hat{A} | x - y/2 \rangle \, dy, \tag{2.36}$$

The main characteristic of the inverse Weyl transform is to feature the trace of the product of two operators as follows [40] :

$$\mathrm{Tr}[\hat{A}\hat{B}] = \frac{1}{h} \int \int \tilde{A}(x,p)\tilde{B}(x,p) \, dxdp. \tag{2.37}$$

Hence, the expectation value of an observable A can be illustrated as [40]:

$$\langle A \rangle = \mathrm{Tr}[\hat{\rho}\hat{A}] = \frac{1}{h} \int \tilde{\rho}\tilde{A} \, dxdp. \tag{2.38}$$

Where $\hat{\rho}$ is the density operator of a pure state $|\psi\rangle$ being defined as $\hat{\rho} = |\psi\rangle\langle\psi|$. This leads to designate the Wigner function as [40] :

$$W(x,p) = \tilde{\rho}/h = \frac{1}{h} \int e^{-ipy/\hbar} \psi(x + y/2)\psi^*(x - y/2) dy. \tag{2.39}$$

Obviously, the expectation value of an observable A now can be written by employing the Wigner function as [40]:

$$\langle A \rangle = \int \int W(x,p)\tilde{A}(x,p) \, dxdp. \tag{2.40}$$

The projection of the Wigner function onto the x axis provides the probability distribution along the x axis as $\int W(x,p)dp = \psi^*(x)\psi(x)$, and its projection on the p axis gives the probability distribution on this axis as $\int W(x,p)dx = \phi^*(p)\phi(p)$. Therefor, despite the fact that the Wigner function is not like the classical probability distribution, and can become negative or being ill-behaved, our objective is fulfilled

[39].

2.6 Gaussian States

A Gaussian state is outlined as any state whose quasiprobabilty distribution, for example its Winger function is Gaussian on the quantum phase space. A general multi-variate Gaussian function has the following form [32]:

$$f(\mathbf{x}) = C\exp(-\frac{1}{2}\mathbf{x}^{\mathrm{T}}\mathbf{A}\mathbf{x} + \mathbf{b}^{\mathrm{T}}\mathbf{x}), \tag{2.41}$$

here $\mathbf{x} = (x_1, x_2, ..., x_N)^{\mathrm{T}}$, $\mathbf{b} = (b_1, b_2, ..., b_N)^{\mathrm{T}}$ and $\mathbf{A}$ is an $N \times N$ positive-definite matrix.
In spite of the fact that an infinite-dimensional Hilbert space is associated with continuous-variable quantum states, Gaussian states can be completely characterized through their *first* and *second* canonical moments, which are the mean and covariance matrix of their quadratures. Using the compact form of quadrature operators defined in relation 2.16, the first moment is designated as [32]:

$$d_a = \langle \hat{R}_a \rangle_\rho \,, \tag{2.42}$$

and the second moment or the so-called covariance matrix is defined as :

$$\sigma_{ab} = \frac{1}{2}\langle \hat{R}_a\hat{R}_b + \hat{R}_b\hat{R}_a\rangle_\rho - \langle \hat{R}_a\rangle_\rho\langle \hat{R}_b\rangle_\rho \,. \tag{2.43}$$

where $\langle \hat{O} \rangle_\rho \equiv \mathrm{tr}[\rho\hat{O}]$ is the mean of the operator $\hat{O}$ evaluated on the state ρ.
The covariance matrix is a real, symmetric, positive definite matrix. From the point of view of statistical mechanics, its elements are the two-point truncated correlation functions between the $2N$ canonical continuous variables [32].
For a bipartite Gaussian state, the covariance matrix can be written as follows:

$$\sigma\,(\,\hat{q}_a,\,\hat{q}_b,\,\hat{p}_a,\,\hat{p}_b) = \begin{pmatrix} \sigma_{aa}^{qq} & \sigma_{ab}^{qq} & \sigma_{aa}^{qp} & \sigma_{ab}^{qp} \\ \sigma_{ba}^{qq} & \sigma_{bb}^{qq} & \sigma_{ba}^{qp} & \sigma_{bb}^{qp} \\ \sigma_{aa}^{pq} & \sigma_{ab}^{pq} & \sigma_{aa}^{pp} & \sigma_{ab}^{pp} \\ \sigma_{ba}^{pq} & \sigma_{bb}^{pq} & \sigma_{ba}^{pp} & \sigma_{bb}^{pp} \end{pmatrix} \tag{2.44}$$

First moment of N-mode Gaussian states can be easily adjusted by a local unitary operations, known as displacement operator in phase space. These operations do not change the informationally relevant properties, such as entropy or any measure of correlations. Hence, without any loss of generality, the first moment can be set to zero $d = 0$ [32]. This suggests that the covariance matrix of a bipartite Gaussian state can be described by 10 matrix elements, since the symmetry of the covariance matrix

requires $\sigma_{ab}^{pq} = \sigma_{ba}^{qp}$.

The Wigner function of a Gaussian state has in general a Gaussian form as [32]:

$$W(\mathbf{X}) = \frac{1}{\pi^N} \frac{1}{\sqrt{\det(\sigma)}} e^{(\mathbf{X}-d)^{\mathrm{T}}\sigma^{-1}(\mathbf{X}-d)}, \tag{2.45}$$

where $\mathbf{X} \in \mathbb{R}^{2N}$.

According to what mentioned, the covariance matrix contains all the locally-invariant information on a Gaussian state. Hence it is natural to expect that any genuine covariance matrix has to obey certain constraints in order to reflect the requirements that the associated density matrix is physical. These requirements are positivity of the covariance matrix in addition to the canonical commutation relations which is described as follows [32]:

$$\sigma + i\Omega \geq 0 \tag{2.46}$$

This relation is in fact the strong form of uncertainty principle on the canonical operators, and it is the necessary and sufficient condition that the covariance matrix σ has to meet in order to describe a physical density matrix [32].

2.6.1 Symplectic Transformations and the Gaussian Unitaries

Gaussian quantum information is build based on the symplectic transformations. The symplectic matrices are defined by the following condition [32]:

$$S\Omega S^{\mathrm{T}} = \Omega \tag{2.47}$$

where Ω is the symplectic form described via 2.18. Symplectic matrices are always square $(2N \times 2N)$, invertible matrices with determinant $\det(S) = +1$ [32].

A very interesting feature of Gaussian states, is the way unitary transformations act on them. A unitary transformation is mapped to real *symplectic transformations* on the first and second moments as follows[32]:

$$\rho' = \hat{U}\rho\hat{U}^{\dagger} \longrightarrow \; d' = Sd \tag{2.48}$$

$$\sigma' = S\sigma S^{T} \tag{2.49}$$

here S is the *symplectic matrix* corresponding to the action of the unitary operator on the Gaussian state. However, this transformation only holds for the unitary transformations whose are at most quadratic in the mode operators $\{\hat{a}_k, \hat{a}_k^{\dagger}\}$. Because these unitary transformations preserve the Gaussian nature of the states [32].

2.6.2 Williamson Theorem and Symplectic Spectrum

Williamson proved that by using a symplectic transformation, any symmetric positive-definite matrix can be put into a diagonal form. A very important benefit of this result is in finding the so-called symplectic eigenvalues of an arbitrary Gaussian state

described by a covariance matrix σ. This physically corresponds to a normal mode decomposition.The theorem is formalised as follows [32]:

THEOREM: Assume σ be a $2N \times 2N$ positive-definite matrix. Then there exists a symplectic matrix S that diagonalises σ such that [32]:

$$\sigma = S \bigotimes_{k=1}^{N} \begin{pmatrix} \nu_k & 0 \\ 0 & \nu_k \end{pmatrix} S^{\mathrm{T}} \tag{2.50}$$

The N eigenvalues ν_k collected into $\boldsymbol{\nu} = diag(\nu_1, ..., \nu_N)$, is called the *symplectic spectrum* of σ. For a state to be physical, the symplectic eigenvalues must obey $\nu_k \geq 1 \, \forall \, k = 1, ..., N$. This is equivalent to the condition 2.46 [32].

2.6.3 Standard form of two-Mode Gaussian states

In section 2.6, I mentioned that the vector of first moments can be ruled out by the use of local-unitary operations. For a two-mode Gaussian state, this suggests that the covariance matrix can be described by only 10 elements. For the general case, $2N(2N+1)/2$ real parameters are needed to build the covariance matrix (CM). The number of the necessary parameters can further be reduced by applying local unitaries. This will bring the CM to the so-called *standard forms*. Here, I only limit myself to the two-mode Gaussian states, where by employing a local symplectic operations $S_l = S_1 \oplus S_2$, a covariance matrix σ can be brought to its standard form σ_{sf} [33] :

$$S_l^{\mathrm{T}} \sigma S_l = \sigma_{sf} \equiv \begin{pmatrix} A & C \\ C^{\mathrm{T}} & B \end{pmatrix} \tag{2.51}$$

where $A = diag(a, a)$, $B = diag(b, b)$, $C = diag(c_1, c_2)$. The quantities $\mathrm{Det}\, \sigma = (ab - c_1^2)(ab - c_2^2)$, $\mathrm{Det}\, A = a^2$, $\mathrm{Det}\, B = b^2$, $\mathrm{Det}\, C = c_1 c_2$ are the four local symplectic invariants. Hence, the standard form of any CM is unique [33].
Using the standard form of the CM, the symplectic eigenvalues of a two-mode Gaussian state can be written as follows [35]:

$$\nu_{\pm}^2 = \frac{1}{2}[\, \Delta \pm \sqrt{\Delta^2 - 4I_4}\,] \tag{2.52}$$

here $I_1 = \mathrm{Det}\, A$, $I_2 = \mathrm{Det}\, B$, $I_3 = \mathrm{Det}\, C$, $I_4 = \mathrm{Det}\, \sigma$ and $\Delta = I_1 + I_2 + 2I_3$.

2.7 Quantum Measurements

Due to the usage of "Quantum Measurement", especially "POVM" measurement which implies the Positive Operator-Valued Measure in this thesis, I briefly discuss these concepts here. In quantum mechanics, the measurements are represented by a set of measurement operators like $\{M_m\}$, which perform on the state space of the system under observation. Here "m" shows the possible outcomes of the measurement.

Considering that $|\psi\rangle$ describes the state of the quantum system before the observation, the probability of obtaining the result m from the measurement is represented as follows [42]:

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle \tag{2.53}$$

With the post-measurement quantum state of the system $|\psi'\rangle$, given by [42]:

$$|\psi'\rangle = \frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}} \tag{2.54}$$

Besides, the measurement operators should meet the *completeness* criterion as [42]:

$$\sum_m M_m^\dagger M_m = I \tag{2.55}$$

This guarantees the sum of all the probabilities to be equal to one [42]:

$$\sum_m p(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle = 1. \tag{2.56}$$

2.7.1 Positive-Operator-Value-Measurement (POVM)

POVM measurement, which implies the "Positive Operator-Valued Measure", is a special case of the general formalism of quantum measurement. The purpose of defining it separately is to provide a straightforward tool to inspect the measurement statistics, without looking at the quantum state after the observation. This is applicable for the experiments where the system needs to be observed only once.
Again we can assume that the measurement operators M_m function on the quantum system being in the state $|\psi\rangle$, with the outcome probability defined as $p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$. We designate the operator E_m as [42]:

$$E_m \equiv M_m^\dagger M_m. \tag{2.57}$$

Considering what mentioned earlier E_m is a positive operator, in a way that $\sum_m E_m = I$ and $p(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle$. The complete set of operator $\{E_m\}$ which are enough to describe the probability distribution obtained from the different measurement outcomes is named as a "POVM". (See ref [42] for more details.)

2.8 Measurement in Quantum Optics

In quantum optics experiments, photon numbers either can be measured employing the direct photo-detection or utilizing a technique called *homodyne* detection. In homodyne detection field quadratures defined by relations 2.11 and 2.12 are measured.

2.8.1 Quadrature Measurement

The homodyne detection technique for quadrature measurement is described in many quantum optics books and texts including ref [39]. Here I briefly review it. The schematic diagram of a balanced homodyne detection is shown in figure 2.3. As it is illustrated the signal beam is interfered with an intense coherent beam called *local oscillator* (LO). The local oscillator supplies the phase reference for the quadrature measurement. It should be much more powerful than the signal beam in order to be treated classically. The interested quantity is the subtraction of the two photocur-

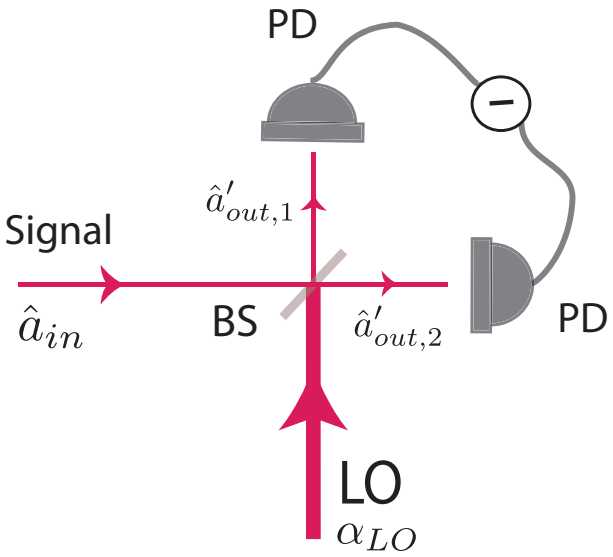


Figure 2.3: Schematic diagram of a balanced homodyne detection. Here LO is the local oscillator, BS is beam-splitter and PD is photo-detector. $\hat{a}_{in}$ shows the input mode, α_{LO} is the amplitude of the local oscillator, $\hat{a}'_{out,1}$ and $\hat{a}'_{out,2}$ refer to the emerging output modes of the beam-splitter interfering the signal and local oscillator

rents I_1 and I_2. These photocurrents are assumed to be proportional to the photon numbers of the quantum mode reaching each detector defined as follows:

$$\hat{n}_1 = \hat{a}'^{\dagger}_{out1}\hat{a}'_{out1} \quad and \quad \hat{n}_2 = \hat{a}'^{\dagger}_{out2}\hat{a}'_{out2}. \tag{2.58}$$

Here $\hat{a}'_{out1}$ and $\hat{a}'_{out2}$ are the output modes of the beam-splitter mixing the input signal and local oscillator. They are defined as [39]:

$$\hat{a}'_{out1} = \frac{1}{\sqrt{2}}(\hat{a}_{in} - \alpha_{LO}), \tag{2.59}$$

$$\hat{a}'_{out2} = \frac{1}{\sqrt{2}}(\hat{a}_{in} + \alpha_{LO}). \tag{2.60}$$

Hence, the subtracted photon numbers can be written as [39]:

$$\hat{n}_{21} = \hat{n}_2 - \hat{n}_1 = \alpha^*_{LO}\,\hat{a}_{in} + \alpha_{LO}\,\hat{a}^{\dagger}_{in}. \tag{2.61}$$

Considering the equation (2.11), this can be reduced to [39]:

$$\hat{n}_{21} = \sqrt{2}\,|\alpha_{LO}|\,\hat{q}. \tag{2.62}$$

Since the local oscillator carries the phase information, equation (2.62), hence the balanced homodyne detector indeed measures the quadrature component.

2.8.2 Simultaneous Measurement of Two Quadratures

As we know quantum mechanics imposes restriction on the observation of the *canonically conjugate* quantities simultaneously and precisely. However, it is still possible to perform such measurement if we sacrifice the accuracy and allow some extra quantum noise to be involved. Consider we have two conjugate operators $\hat{q}$ and $\hat{p}$, following the commutation relation:

$$[\hat{q}, \hat{p}] = i\hbar, \tag{2.63}$$

The concurrent observation of $\hat{q}$ and $\hat{p}$ is possible through the definition of other observables described by the relation [39] :

$$\hat{Q}_1 = \hat{q} + \hat{A}, \quad \hat{P}_2 = \hat{p} + \hat{B}. \tag{2.64}$$

The operators $\hat{A}$ and $\hat{B}$ recount the extra quantum fluctuations introduced to the system in order to perform the simultaneous measurement. They require not to carry any preexisting amplitude [39]:

$$\langle \hat{A} \rangle = \langle \hat{B} \rangle = 0. \tag{2.65}$$

And we demand that [39]:

$$[\hat{Q}_1, \hat{P}_2] = 0. \tag{2.66}$$

In order to fulfill this idea in the quantum optics experiments, the signal beam is divided into two, using a beamsplitter. Each part is then sent to a homodyne measurement station, one for observing $\hat{q}$ and the other for observing $\hat{p}$. The key point is to ensure that the local oscillator signals sent to two homodyne detection should have $\pi/2$ phase shift. This is generally realized by dividing the same local oscillator into two, by employing a beamsplitter and then applying a phase shift on one arm via a $\lambda/4$ wave-plate [39]. This technique is called *dual-homodyne* or *heterodyne* detection. A schematic diagram of the heterodyne (dual-homodyne) measurement is depicted in figure 2.4.

2.9 Phase and Amplitude Modulation

Phase and amplitude modulation are used to encode information on a beam of laser. These concepts are repeatedly used throughout this thesis.

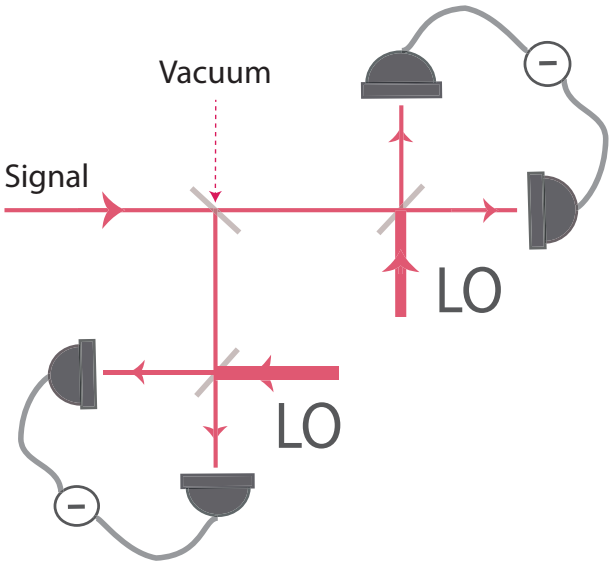


Figure 2.4: Schematic diagram of heterodyne (dual-homodyne) detection. The elements are the same as defined in figure 2.3

2.9.1 Phase Modulation

If we assume to be in a frame rotating at the carrier frequency Ω, a phase modulated optical field can be written as :

$$a_{PM}(t) = a_0 \exp(i\,\Omega t) \exp[i\xi \,\mathrm{Cos}(\omega_M t)] \tag{2.67}$$

Where $a_0 \exp(i\,\Omega t)$ is the optical field prior to modulation, ω_M is the frequency of modulation, ξ is called "modulation's depth". $\xi = 1$ corresponds to complete modulation and $\xi = 0$ to zero modulation.
For small modulation depth ($\xi \leq 1$), the field $a_{PM}(t)$ can be decomposed into a component at the laser carrier frequency Ω and sidebands at ω_M and $-\omega_M$ away from the carrier:

$$\begin{aligned} a_{PM}(t) &\approx a_0 \exp(i\,\Omega t)(1 + i\xi \,\mathrm{Cos}(\omega_M t)) \\ &= a_0 \exp(i\,\Omega t) + i\frac{\xi}{2}\left[\exp(i(\Omega + \omega_M)t) + \exp(i(\Omega - \omega_M)t)\right] \end{aligned}$$

This shows that the phase modulation transfers optical power from the carrier into sidebands at frequencies $\pm\omega_M$. These side bands only appear while the phase is measured. Obviously the intensity will not be modulated as $|a_{PM}(t)|^2 = a_0^2$. The calculation for larger modulation depth involves Bessel functions.

2.9.2 Amplitude Modulation

A beam of light which is amplitude modulated can be expressed as:

$$a_{AM}(t) = a_0 \exp(i\,\Omega t)\,(1 - \frac{\xi}{2}(1 - \mathrm{Cos}(\omega_M t))) \tag{2.68}$$

which can be written as:

$$a_{AM}(t) = a_0 \exp(i\,\Omega t)(1 - \frac{\xi}{2}) + a_0\,\frac{\xi}{4}\,[\exp[i(\Omega + \omega_M)t] + \exp[i(\Omega - \omega_M)t]] \tag{2.69}$$

We see that the effect of amplitude modulation is to create new frequency components at $\pm\omega_M$, which are known as the upper and lower sidebands. For completely modulated light with $\xi = 1$, the sidebands have exactly half the amplitude of the fundamental component. The resultant intensity is modulated and given by :

$$I(t) = |a_{AM}(t)|^2 = I_0\,(1 - \frac{\xi}{2}(1 - \mathrm{Cos}(\omega_M t)))^2 \tag{2.70}$$

Where $I_0 = a_0^2$. More information on phase and amplitude modulation can be found in ref [34].

2.10 Information Theory and Entropy

In this section I briefly review the basic concepts of the classical and quantum information theory which are based on the definition of entropy.

2.10.1 Shannon Entropy

Shannon entropy is the key concept of classical information theory. For a classical variable X with values x occurring with probability p_x, the Shannon entropy measures how much information one gains after learning the value of X. There is another complementary view of entropy as a measure of one's uncertainty before learning the value of X [42].
The entropy of a random variable is characterized as a function of the probabilities of the different possible values that the random variable can take. The Shannon entropy related to these probabilities is defined as [42]:

$$H(X) \equiv H(p_1, ..., p_n) \equiv -\sum_x p_x \log p_x. \tag{2.71}$$

Logarithms are taken to base two. The main reason for this definition of entropy is its ability to quantify the physical resources which are required to store the information [42].

2.10.2 Relative Entropy

The relative entropy is a measure of closeness of two probability distributions, $p(x)$ and $q(x)$, on the same index set, x. It is defined as [42] :

$$H(p(x)||q(x)) \equiv \sum_x p(x) \log \frac{p(x)}{q(x)} \equiv -H(X) - \sum_x p(x) \log q(x). \tag{2.72}$$

It is assumed that $-0 \log 0 \equiv 0$ and $-p(x) \log 0 \equiv +\infty$ if $p(x) > 0$ [42].

2.10.3 Shannon Entropy of Continuous Random Variable

Shannon's entropy can be extended to continuous random variables. Assume X be a continuous random variable with the probability density function defined by $p(x)$ on I, where $I = (-\infty, \infty)$. Then the Shannon's entropy for continuous random variables is given by [43] :

$$H(X) = -\int_I p(x) \log p(x)\, dx, \tag{2.73}$$

Although it has many properties of Shannon's entropy of discrete variables, unlike that it can become infinitely large or negative. In addition, the Shannon's entropy for continuous random variables does not necessary remain invariant under a change of variable, while Shannon's entropy of discrete variables remains invariant [43].

2.10.4 Joint Entropy

The joint entropy quantifies one's total uncertainty about the pair of random variables (X, Y). It is naturally defined as [42]:

$$H(X, Y) \equiv -\sum_{x,y} p(x, y) \log p(x, y). \tag{2.74}$$

2.10.5 Conditional Entropy

If we have a pair of random variables (X, Y), by performing a measurement on the random variable Y we can learn its value and acquire $H(Y)$ bits of information about the pair. The conditional entropy quantifies our lack of knowledge about the pair (X, Y), on average, given the fact that we know the value of Y. It is simply defined as [42]:

$$H(X|Y) \equiv H(X, Y) - H(Y). \tag{2.75}$$

Another way to express It, is the lack of knowledge of X when the state of Y is in the yth state, weighted by the probability for yth outcome as [45] :

$$H(X|Y) = -\sum_y p(X|y) H(X|Y = y) \tag{2.76}$$

where y is the outcome of the measurement performed on subsystem Y . Conditional entropy can be shown schematically using the *'entropy Venn diagram'* depicted in figure 2.5.

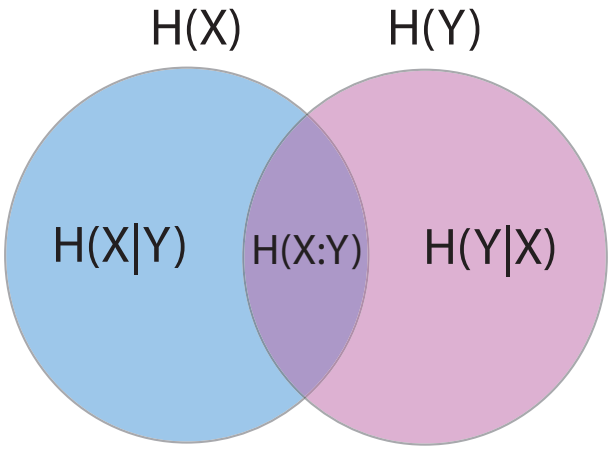


Figure 2.5: Entropy Venn diagram, showing the relationship between different entropies [42].

2.10.6 Mutual Information

The mutual information quantifies how much information two random variables (X, Y) have in common [42]. It is defined as [30]:

$$H(X : Y) = H(X) - H(X|Y) \tag{2.77}$$

This can be seen in *'entropy Venn diagram'* depicted in figure 2.5. The mutual information quantifies the average decrease of entropy of X when the value of Y is known [30]. Using the *'Bayes'* rule, which defines the conditional probability for classical variables as $p_{x|y} = p_{xy}/p_y$ [44], equation (2.77) can be written equivalently as [30]:

$$H(X : Y) \equiv H(X) + H(Y) - H(X, Y). \tag{2.78}$$

Further information can be found in ref [42, 30, 44]

2.10.7 von Neumann Entropy

In classical information theory we calculate the uncertainty of the classical probability distribution using Shannon entropy. Quantum state can be described similarly with density operators ρ, and Shannon entropy can be generalized for quantum states to Von Neumann entropy [42].
The Von Neumann entropy measures the information of a quantum state by finding the entropy of the probability distribution resulted from the state ρ by a projective measurement onto the state's eigenvectors [29]. It is defined as:

$$S(\rho) = -\mathrm{Tr}(\rho \log \rho) = H(\lambda) \tag{2.79}$$

Where $\lambda = \lambda_i$ are the eignevalues of the state. Here also the logarithms are taken to base two and $0 \log 0 \equiv 0$.

2.10.8 Quantum Mutual Information and Conditional Entropy

Classical mutual information described by equation (2.78) can be easily generalized to quantum mutual information by simply replacing the Shannon entropy by Von Neumann entropy and the classical probability distributions by density matrices ρ as follows [30]:

$$I(\rho_{XY}) = S(\rho_X) + S(\rho_Y) - S(\rho_{XY}) \tag{2.80}$$

However, equation (2.77) cannot be easily generalized to quantum states, as to define the conditional entropy $H(X|Y)$ one needs to define the state of X given the result of the measurement performed on the state of Y. This is more obvious by looking at the measurement-based version of conditional entropy defined by the relation 2.76. Such statement is ambiguous in quantum mechanics until the set of the measurement which will be performed on the state Y is selected [30]. In order to define the quantum analogue of the measurement-based conditional entropy a set of (POVM) with elements $\{E_y = M_y^\dagger M_y\}$ is assumed to perform on subsystem Y with y to be the outcome of the measurement (see subsection 2.7.1 for description on POVM). The probability of obtaining the outcome y is $p_y = \mathrm{tr}(\rho_{xy} E_y)$ and subsystem X is left in the conditional state of $\rho_{X|y} = \mathrm{tr}_Y(\rho_{XY} E_y)/p_y$. This allows us to write the quantum version of measurement- based conditional entropy as $S_{\{E_y\}}(X|Y) \equiv \sum_y p_y S(\rho_{X|y})$. Hence, the quantum analogue of mutual information defined by equation (2.77) can be written as [44]:

$$max_{\{E_y\}} J(X|Y) \equiv S(X) - S_{\{E_y\}}(X|Y) \tag{2.81}$$

The quantity $max_{\{E_y\}} J(X|Y)$ which is maximized over all possible POVMs is called one way classical correlations [29].

2.10.9 Holevo Bound

Considering the fact that quantum states are generally nonorthogonal, a nontrivial concern to address is the maximum information that can be extracted from it using a quantum measurement. This quantity is called the accessible information of the ensemble. The *Holevo bound* which is an extremely useful tool in quantum information theory, provides an upper bound on the amount of accessible information. It is

defined as follows [42] :

$$H(X:Y) \leq S(\rho) - \sum_x p_x S(\rho_x), \tag{2.82}$$

Where $\rho = \sum_x p_x \rho_x$. This refers to the situation when Alice prepares a state ρ_X, while $X = 0, ..., n$ with probability of occurring as $p_0, ..., p_n$, and Bob operates a POVM measurement on the state with elements $\{E_y\} = \{E_0, ..., E_m\}$, and y being the outcome of the measurement [42]. (See ref [42] for more details).

2.11 Quantum Correlations

Since the focus of this thesis is on *Quantum Correlations*, I specify this section to describe the well-known forms of quantum correlations and the way to quantify them especially in Gaussian states.

2.11.1 Entanglement and non-locality

When two physical systems have an interaction with each other, some form of correlation with a quantum nature is created between them, which remains even when the two systems get specially separated. This suggests that, if one performs a measurement on a local observable on the first system, the state of the second system, no matter where it is, is modified instantaneously. This phenomenon, named by Einstein, Podolsky and Rosen as "spooky action at a distance" [3], is called *entanglement* which is the non-classical and non-local quantum correlation. However, non-locality and entanglement are a bit different. It can be understood from the general framework of no-signalling theories which demonstrate more non-local features than the quantum mechanics [33, 36]. According to Bell [33, 37], non-locality is a channel in nature which allows one to distribute correlations between distant parties, in a way that the correlations are not pre-determined at the source, and the correlated random variables can be generated when distant parties perform local measurements on their subsystems. Quantum mechanics describes this channel as an entangled pair [33]. As I will describe in the following chapters this characteristic of nature is harnessed in secure quantum communications.
Considering the importance of quantum entanglement, it is desirable to have an operational criterion to examine if a given state is entangled or not. As I will show shortly, for *pure states* of the composite quantum system, it is relatively easy to quantify entanglement. However, the situation is more complicated with *mixed states*, as a mixture can be in many different ways where no one can extract all the information it contains [33].

2.11.2 Entanglement Criteria for Pure Bipartite States

A pure quantum state $|\psi\rangle \in H = H_1 \otimes H_2$ is entangled if it cannot be written as a product state such that :

$$|\psi\rangle = |\phi\rangle_1 \otimes |\chi\rangle_2 \equiv |\phi, \chi\rangle. \tag{2.83}$$

where $|\phi\rangle_1 \in H_1$ and $|\chi\rangle_2 \in H_2$.
In order to quantify entanglement one can write a pure quantum state in its unique Schmidt decomposition [42] as follows [33] :

$$|\psi\rangle = \sum_{k=1}^{d} \lambda_k |u_k, v_k\rangle, \tag{2.84}$$

where

$$d = min\{d_1, d_2\} \ , \tag{2.85}$$

$$\lambda_k \geq 0, \ \sum_{k=1}^{d} \lambda_k^2 = 1. \tag{2.86}$$

The local bases $\{|u_k\rangle\} \in H_1$ and $\{|v_k\rangle\} \in H_2$ are the Schmidt bases, the positive numbers $\{\lambda_k\}$ are the Schmidt coefficients and the number d of the non-zero terms in the Schmidt number. It can be seen that the product states $|\psi\rangle = |\phi, \chi\rangle$ can be automatically written in the Schmidt form when $d = 1$. In other words if a state can be written as Schmidt decomposition with only one coefficient, then it is necessarily a product state. Hence, a pure state $|\psi\rangle$ of a bipartite system is entangled if and only if $d > 1$ [33].

2.11.3 Entanglement Criteria for Mixed States

A mixed state can be written as a convex combination of pure states :

$$\rho = \sum_k p_k |\psi_k\rangle\langle\psi_k| \tag{2.87}$$

Now the problem is that this decomposition is not unique, unless ρ is already a pure state. This means that the mixed states can be prepared in many different ways which makes the entanglement's quantification very difficult. Considering the ambiguity on the state preparation, no one knows *a priori* if the correlations between the subsystems arose from a quantum interaction or were induced by means of LOCC (Local Operations and Classical Communications) which causes classical correlations [33].

A mixed quantum state of a bipartite system, described on the Hilbert space $H = H_1 \otimes H_2$, is separable if and only if it can be written as follows :

$$\rho = \sum_k p_k (\sigma_k \otimes \tau_k). \tag{2.88}$$

where $\{p_k \geq 0, \sum_k p_k = 1\}$, and states $\{\sigma_k\} \in H_1$ and $\{\tau_k\} \in H_2$. Otherwise, ρ is en-

tangled . However, this is a very impractical way of checking if a state is entangled or not. Since deciding entanglement or separability according to this definition would require one checks all the infinitely many decomposition of a state ρ and look for at least one of them to be in the form of 2.88. Hence, several *operational* criteria have been developed to check entanglement in mixed quantum states [33]. In addition, developing a criterion for checking the inseparability will be dramatically simplified if we restrict ourselves to the certain class of quantum states. Considering that the focus of this thesis is on the continuous-variables and particularly on Gaussian states, here I only present two entanglement criteria applicable to the two-mode Gaussian states. The first one is the *Duan inseparability criterion* introduced by Duan *et al.* [48], which provides a necessary and sufficient condition for the inseparability of two-mode Gaussian states. The second one is the EPR-paradox criterion introduced by Reid[47] which quantifies the degree of EPR paradox of a state.

2.11.4 Duan Inseparability Criterion

The Duan inseparability criterion quantifies the strength of entanglement of a quantum state. For the case of two-mode quadrature entangled state, It is defined as [49]:

$$\mathcal{I} = \sqrt{\Delta^2 \hat{x}_{a\pm b}\, \Delta^2 \hat{p}_{a\pm b}} \tag{2.89}$$

where $\Delta^2 \hat{O}_{a\pm b} = min\langle (\delta \hat{O}_a \pm \delta \hat{O}_b)^2 \rangle /2$. If $\mathcal{I} < 1$, the state is inseparable. $\mathcal{I} = 0$ corresponds to the best possible entanglement obtained from combining two perfectly squeezed beams [49].

2.11.5 EPR Paradox Criterion

EPR criterion measures the degree of the EPR paradox, introduced by Einstein, Podolsky and Rosen in 1935 [3]. It is based on the ability of a state to produce an apparent violation of the Heisenberg uncertainty relation between two conjugate variables. A quantifying measure of an EPR violation for the continuous variables was introduced by Reid in 1988 [46, 47]. This criterion which is more restrictive than the Duan inseparability criterion, is defined as the product of the conditional variances of the phase and amplitude quadratures as follows:

$$\epsilon_{ab} = \Delta \hat{q}_{a|b} \Delta \hat{p}_{a|b} < 1 \tag{2.90}$$

$$\epsilon_{ba} = \Delta \hat{q}_{b|a} \Delta \hat{p}_{b|a} < 1 \tag{2.91}$$

The conditional variances are defined as :

$$\Delta \hat{q}_{a|b} = \Delta \hat{q}_a - \frac{|\sigma_{ab}^{qq}|}{\Delta \hat{q}_b} \tag{2.92}$$

where σ_{ab}^{qq} is the covariance and $\Delta\hat{q}_a$ and $\Delta\hat{q}_b$ are the variances (please see 2.44). Similar relation applies for other quadrature $\hat{p}$ or the other direction of the conditional variances. The conditional variance quantifies the reduced uncertainty on subsystem a following a measurement on subsystem b. This gives a measure where the subsystems a and b are not perfectly correlated, but by performing a measurement on one subsystem some information can be gained about the other subsystem.
A state demonstrates an EPR paradox if the product of the conditional variances of the two orthogonal quadratures is below one. Satisfying this criterion is a *sufficient* but not the necessary condition for a state to be entangled.

2.11.6 Quantum Discord

While it was thought previously that the absence of entanglement implies the classicality of the states, recent research has shown that some form of quantum correlations can exist even in the separable states. This notion of quantumness which was first discovered by Ollivier and Zurek [30] is called *quantum discord*. This is an important form of quantum correlations that attract lots of attentions during recent years. This concept will be elaborated in the next chapter.

2.12 Summary

In this chapter I reviewed the key concepts of quantum optics and information theory which will be used though out this thesis. This includes introducing the optical field quadratures, different quantum states of light, Wigner function, Gaussian states and symplectic transformations, quantum measurement and the detection schemes, phase and amplitude modulations which are used in the continuous-variable quantum optics experiments . In the information theory part, I covered the concepts of Shannon entropy, relative entropy, conditional entropy, mutual information, von Neumann entropy, quantum mutual and conditional entropy and Holevo bound. In addition, in the section of Quantum Correlations, I discussed Entanglement and non-locality, the criterion of entanglement in pure states and two important entanglement criteria in the two-mode Gaussian states. I mentioned "Discord" here as a form of quantum correlations that can exists even in the separable states. However, this concept will be discussed thoroughly in the next chapter.

Chapter 3

Experimental Verification of Quantum Discord in Continuous-Variable States

3.1 Introduction

Quantum systems can be correlated in a superior way than the classical systems. These correlations are particularly important as the main resource for quantum information processing and quantum communication. Due to the importance of quantum correlations, quantifying the classical and quantum part of the correlations has been the subject of many studies during the last decade. As mentioned in the previous chapter, entanglement was considered before as the only form of non-classical correlation and the main resource that causes quantum computation and communication outperform the classical counterparts. Any correlation in the absence of entanglement was thought to be purely classical. This idea was also supported by the fundamental Bell's inequality [5], which cannot be violated by any classical or quantum superposition and requires genuine entanglement to be violated. However, nowadays the accepted definition of a classical bit, is in one of two fully-distinguishable states. According to this definition, general quantum states form a subset of the separable states, meaning that some separable states are quantum correlated [44]. This suggests that entanglement no longer is the only source of quantumness. In addition, quantum computation models with no or very little entanglement were suggested which can achieve much higher efficiency than classical computers [50, 51]. These models and other studies during the last decade have convinced physicists that entanglement and classical correlation do not exhaust all the possible correlations. Ollivier and Zurek were the first to characterize this extra quantum correlation beyond entanglement and named it "Discord" [30]. Quantum discord has attracted so much attention during the last decade and was suggested as a figure of merit for characterizing the quantum resources in a computational model [52]; it was also introduced as a resource for quantum state merging [53, 54], and for encoding information onto a quantum state [55]. Besides it has been shown as the necessary resource for quantum remote state preparation, outperforming entangled states [56]

This measure of nonclassical correlation has been extended to continuous-variable systems to study quantum correlations in Gaussian states [57, 35] and certain non-Gaussian states [58]. In addition, resilience of quantum illumination, a paradoxical technique that employs entanglement to detect reflecting objects in noisy environments, has also been demonstrated to be due to quantum discord [59]. It also determines the interferometric power of quantum states used in metrology [60]. Since quantum discord is more robust than entanglement, it has been shown that it can serve well in Device-Dependent quantum key distribution, where the trusted noise is so high that prevents the distribution and distillation of entanglement [61]. The relation between quantum coherence (superposition) and quantum discord [62], and incoherent operation and discord-type quantum correlation [63] has also been studied recently.
Considering the importance of quantum discord, of particular interest is to experimentally verify discord for an *unknown* quantum system. Methods have been proposed to test for nonvanishing quantum discord of bipartite discrete-variable quantum states [64, 65, 66, 67, 68, 69, 70], some of which have been experimentally implemented in nuclear-magnetic-resonance systems [71, 72] and in an optical system [73]. A more general measurement-based method for verifying quantum discord was introduced in ref [74], which can be applied to both discrete- and continuous-variable systems. We have introduced and demonstrated experimentally a simple and efficient technique to verify quantum discord in unknown Gaussian sates and a certain class of non-Gaussian states, which I will elaborate it here.
The structure of this chapter is as follows. At first, I will review the definition of quantum discord as the measure of quantum correlation beyond entanglement in section 3.2. Then I mention the Gaussian quantum discord and present the general form of it in section 3.3. After that, in section 3.4, I will then discuss the general method for verification of quantum discord proposed in ref [74]. The main part of this chapter which describes our simple experimental technique to verify quantum discord in an unknown Gaussian states and certain class of non-Gaussian states, will appear in section 3.5. It itself consists of two other sections, where in the section 3.6 I will explain the theoretical development of our technique, and in the section **??** I will detail our experimental implementation and results. This survey has been published in the " Journal of Physics B " with the title and author list as follows:

"S. Hosseini, S. Rahimi-Keshari, J. Y. Haw, S. M. Assad, H. Chrzanowski, J. Janousek, T. Symul, T. C. Ralph and P. K. Lam, *"Experimental Verification of Quantum Discord in Continuous-Variable States"*, J. Phys. B: At. Mol. Opt. Phys. **47**, 025503 (2014)."

This research has been carried out in the "CQC2T Center of Excellence". The theoretical development has been done by Saleh Rahimi-Keshari and Timothy C Ralph at the University of Queensland. The experiment which consisted of four parts; one Gaussian state and three non-Gaussian states, was implemented in our group at the Australian National University. Here I will present the theoretical development in order to make the experimental implementation and results understandable.

3.2 Definition of Quantum Discord

Quantum Discord is simply defined as the mismatch between two quantum analogues of classically equivalent expressions of the mutual information. As mentioned previously in section 2.10.6, classical mutual information is given by two equivalent expressions 2.78 and 2.77, while the mutual information in quantum mechanics, is described by two different expressions 2.80 and 2.81. According to Ollivier and Zurek, quantum discord from subsystem A to subsystem B is defined as follows:

$$\delta(B|A) = I(A:B) - J(B|A) \tag{3.1}$$

Where $J(B|A)$ is maximized over all the possible measurements. The difference basically arises from the quantum analogous of conditional entropy $J(B|A)$ due to the nature of measurements in quantum mechanics in general (see section 2.10.8). Henderson and Vedral also looked at $J(B|A)$, and have shown the $\max_{\{E_a\}} J(B|A)$ to be the classical correlations [29]. Here $E_a = \{M_a^\dagger M_a\}$ is a set of a positive-operator-valued-measurement (POVM) performed on subsystem A (see section 2.7.1). Hence, quantum Discord is the difference between the total correlation and the classical correlations. However, it is not clear how to perform the maximaization to calculate the quantum version of the measurement-based conditional entropy in general, unless there are restrictions to certain class of states and measurements. Of particular interest is Gaussian quantum discord. It is defined as the quantum discord of a bipartite Gaussian state, while the maximaization is limited to the generalized Gaussian measurements [57, 35]. Interestingly, it was shown in ref [74] that Gaussian states with nonzero Gaussian quantum discord, have also nonzero quantum discord.

3.3 Gaussian Quantum Discord

Considering that the focus of this thesis is on the two-mode Gaussian state, before presenting our experimental technique to verify quantum discord, I describe how quantum discord for a bipartite Gaussian state is calculated.
At first, one should notice that quantum discord is invariant under the operation of local unitaries [35]. Hence, we are allowed to perform our analysis using the standard form of covariance matrix (see section 2.6.3). The definition of the Gaussian quantum discord is also based on the mismatch defined in relation 3.1. We can assume a set of POVM such as [35]:

$$\Pi_{\boldsymbol{X}} = D(\boldsymbol{X})\rho_M D(\boldsymbol{X})^\dagger, \quad \int d\boldsymbol{X}\, \Pi_{\boldsymbol{X}} = I \tag{3.2}$$

here $\boldsymbol{X}$ is a two dimensional real vector and ρ_M is a bipartite Gaussian state with zero mean and a covariance matrix σ_M in the standard form as shown in 2.51. If a measurement described by the set of POVM, $\{\Pi_{\boldsymbol{X}}\}$, is performed on the mode B of a bipartite Gaussian state, the outcome is described by the distribution $p(\boldsymbol{X})$, which is a bimodal Gaussian state with the covariance matrix $(B + \sigma_{ab})$. Then the conditional

state of mode A on the outcome of measurement on mode B, which is shown by ρ_X, is a Gaussian state with covariance matrix given by the Schur complement $\sigma_P = A - C(B+\sigma_{ab})^{-1}C^{\mathrm{T}}$ and mean of $X^{\mathrm{T}}(B+\sigma_M)^{-1}C^{\mathrm{T}}$ [35]. Where $A = diag(a,a)$, $B = diag(b,b)$, $C = diag(c_1,c_2)$ as were previously defined in subsection 2.6.3.
Quantum discord can be written as [35]:

$$\delta(\rho) = S(\rho_b) - S(\rho_M) + max_{\{\Pi_X\}} \int d\boldsymbol{X}\, p(\boldsymbol{X})\, S(\rho_{\boldsymbol{X}}) \tag{3.3}$$

It was shown that the general form of *Gaussian quantum discord* is as follows [35]:

$$\delta(\rho) = h(\sqrt{I_2}) - h(\nu_-) - h(\nu_+) + max[h(\sqrt{\sigma_P})] \tag{3.4}$$

where $h(x) = (x+\frac{1}{2})\log(x+\frac{1}{2}) - (x-\frac{1}{2})\log(x-\frac{1}{2})$, and $\nu_\pm$ are the symplectic eigenvalues of ρ_M explained by relation 2.52, and $I_2 = \mathrm{Det}\, B$ which was defined in subsection 2.6.3

3.4 Verification of Quantum Discord in General

Knowing that it is not always easy to calculate quantum discord, it is important to find a method to verify quantum discord in an unknown quantum state. A measurement-based method for verifying quantum discord in general was proposed in ref [74], which is based on measuring the conditional states of one subsystem, for example subsystem B corresponding to the outcomes of an informationally complete POVM (IC-POVM) performed on the other subsystem (subsystem A). If the conditional states commute with one another then the quantum discord is zero, otherwise is nonzero. A POVM is called informationally complete when its outcome probabilities are sufficient to build the quantum state uniquely. For example, they provide enough information to perform the quantum state tomography [79, 80]. If we assume that k and k' are two outcomes of IC-POVM performed on subsystem A, then this theorem can be written mathematically as:

$$\delta(B|A) = 0 \iff [\rho_{B|k}, \rho_{B|k'}] = 0 \quad for\ any\ k\ and\ k' \tag{3.5}$$

Here $\rho_{B|k}$ and $\rho_{B|k'}$ are conditional states (see section 2.10.8). In order to apply this theorem experimentally, one needs to calculate the commutation relation for all the outcomes of the IC-POVM performed on subsystem A until one of the commutation relations between conditional states of subsystem B is nonzero. However, if some prior knowledge about the state is available, it is possible to verify quantum discord with only a few measurements. As shown in ref [74], to verify nonzero quantum discord in Gaussian states, one needs to check whether the peaks of the two conditional Wigner functions (see section 2.5) corresponding to two different outcomes of heterodyne measurements (see section 2.8) do not coincide at the same point in the phase space. Although, it seems more practical than calculating the commutation relations, it is still not very efficient as one has to repeat the measurements many

times in order to obtain sufficient data to build the conditional Wigner functions. In the next section I will detail the simple method that we propose to verify the nonzero quantum discord in continuous variable systems.

3.5 Experimental Method to Verify Quantum Discord in Continuous Variable Systems

In this section I will detail our experimental technique for verifying quantum discord of Gaussian states, which can also be applied to some class of non-Gaussian states. I will start with the theoretical description and terminate with presenting the experimental results.

3.6 Theoretical Development of Verification of Quantum Discord in Continuous-Variables

The theoretical development is divided into two parts. First part is focused on the Gaussian states and the second part on certain class of non-Gaussian states..

3.6.1 Theory: Gaussian States

It was shown in ref [74], that a bipartite Gaussian state has zero quantum discord if and only if there is no correlation between the quadratures of the two subsystems. For example, if we consider the standard form of covariance matrix defined by matrix 2.51, no correlations between the quadratures corresponds to $\mathbf{C} = 0$.

Instead of performing full tomography proposed in ref [74], we suggested to inspect the correlation between two quadratures employing only two homodyne measurements (see section 2.8). Suppose Alice and Bob are sharing a bipartite Gaussian state (see section 2.6). In order to verify quantum discord they can conduct two homodyne detections, one for each subsystem. Without loss of generality, we assume the covariance matrix to be in the standard form and the mean to be zero. Since these can be always accomplished by appropriately choosing the zero reference phase of the local oscillators and shifting the zero reference points of the quadratures being measured. Considering the overall quadrature vector to be as $\mathbf{x} = (\hat{x}_A, \hat{p}_A, \hat{x}_B, \hat{p}_B)$, the joint marginal distribution describing the outcomes of two homodyne detections is then given by [39]

$$\begin{aligned} D_{AB}(x_A, \theta_A, x_B, \theta_B) &= \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} dp_A dp_B W(\mathbf{x}\mathbf{U}_{\theta_A,\theta_B}) \\ &= \frac{\pi}{\sqrt{\lambda_{\theta_A}\mu_{\theta_B} - \nu^2_{\theta_A,\theta_B}}} \\ &\times \exp\left(-\lambda_{\theta_A} x_A^2 - \mu_{\theta_B} x_B^2 + 2\nu_{\theta_A,\theta_B} x_A x_B\right), \end{aligned} \tag{3.6}$$

where

$$\mathbf{U}_{\theta_A,\theta_B} = \begin{pmatrix} \cos\theta_A & \sin\theta_A & 0 & 0 \\ -\sin\theta_A & \cos\theta_A & 0 & 0 \\ 0 & 0 & \cos\theta_B & \sin\theta_B \\ 0 & 0 & -\sin\theta_B & \cos\theta_B \end{pmatrix}$$

with θ_A and θ_B being the phases of the local oscillators used in Alice's and Bob's homodyne detection, respectively, and λ_{θ_A}, μ_{θ_B}, and ν_{θ_A,θ_B} are functions of the the elements of the covariance matrix, which depend on θ_A and θ_B. If ν_{θ_A,θ_B} is nonzero, then the quadrature associated with the phase θ_A of subsystem A is correlated to the quadrature associated with the phase θ_B of subsystem B. In order to inspect this correlation, Bob measures two conditional marginal distributions corresponding to the outcomes $x_A > 0$ and $x_A < 0$ of Alice's measurements

$$\begin{aligned} D_{B|\pm}(x_B,\theta_B,\theta_A) &= \int_0^{\pm\infty} (\pm 1) dx_A D_{AB}(x_A,\theta_A,x_B,\theta_B) \\ &= \frac{\sqrt{\pi\lambda_{\theta_A}}\exp\left(\frac{\nu^2_{\theta_A,\theta_B}-\mu_{\theta_B}\lambda_{\theta_A}}{\lambda_{\theta_A}}x_B^2\right)}{\sqrt{\mu_{\theta_B}\lambda_{\theta_A}-\nu^2_{\theta_A,\theta_B}}} \\ &\times\left(1\pm \mathrm{Erf}\left(\frac{\nu_{\theta_A,\theta_B}x_B}{\sqrt{\lambda_{\theta_A}}}\right)\right), \end{aligned} \tag{3.7}$$

where Erf(.) is the error function. If the peaks of the marginal distributions $D_{B|+}(x_B,\theta_B,\theta_A)$ and $D_{B|-}(x_B,\theta_B,\theta_A)$ do not coincide with one another, this implies that $\nu_{\theta_A,\theta_B} \neq 0$.

Alice and Bob can now verify quantum discord using this method. As we have:

$$\begin{aligned} \nu_{0,0} &= \frac{c_1}{2a_1b_1-2c_1^2}, \\ \nu_{0,\frac{\pi}{2}} &= \frac{c_2}{2a_1b_2-2c_2^2}, \\ \nu_{\frac{\pi}{2},0} &= \frac{c_3}{2a_2b_1-2c_3^2}, \\ \nu_{\frac{\pi}{2},\frac{\pi}{2}} &= \frac{c_4}{2a_2b_2-2c_4^2}, \end{aligned}$$

they only need to choose the phases of their local oscillator to be 0 or $\pi/2$ and observe the conditional marginal distribution $D_{B|\pm}(x_B,\theta_B,\theta_A)$ to check whether the elements of matrix **C** are zero or not. If at least one of the elements is found to be nonzero, the state has nonzero quantum discord.

3.6.2 Theory: Non Gaussian States

It was shown that the necessary condition for generating entanglement at the output of a beam- splitter is sending the non-classical input states to the beam-splitter [82, 83]. Here we show that bipartite non-Gaussian states that are prepared by subjecting

a statistical mixture of coherent states to one port of a beam splitter, and vacuum state to the other port, have nonzero quantum discord. We show that quantum discord for this class of non-Gaussian states can be simply verified by employing our technique.

By applying the Glauber-Sudarshan representation [84, 85] for an input state ρ_1 to a beam splitter as described bellow

$$\rho_1 \otimes |0\rangle \langle 0| = \int d^2\alpha P_1(\alpha) |\alpha\rangle \langle \alpha| \otimes |0\rangle \langle 0| , \tag{3.8}$$

the output state is given by:

$$\rho_{\text{out}} = \int d^2\alpha P_1(\alpha) |\eta\alpha\rangle \langle \eta\alpha| \otimes |\tilde{\eta}\alpha\rangle \langle \tilde{\eta}\alpha| , \tag{3.9}$$

here η is the transmissivity of the beam splitter and $\tilde{\eta} = \sqrt{1-\eta^2}$. The state ρ_{out} has nonzero discord, in case $P_1(\alpha)$ is a positive semi-definite Gaussian or non-Gaussian function other than the Dirac delta function. Since it is a mixture of nonorthogonal states of two subsystems [74]. By applying our technique developed in the previous subsection, one can verify nonzero quantum discord by observing any changes in the conditional marginal distributions, which indicates correlation between the two quadratures. By measuring x-quadratures of two subsystems employing two homodyne detections, the joint marginal distribution is then given by:

$$D(x_1, x_2) = \frac{1}{\sqrt{\pi}} D_1(\eta x_1 + \tilde{\eta} x_2) e^{-(\eta x_2 - \tilde{\eta} x_1)^2}, \tag{3.10}$$

where $D_1(x)$ is the marginal distribution of $W_1(x, p)$, where $W_1(x, p)$ is the Wigner function of the input state ρ_1 (see section 2.5). If the input state is not a coherent state then ρ_{out} has discord, otherwise zero discord. More details on the theoretical development can be found in our published paper. In the following sections, I will present our experimental implementation of this technique on bipartite Gaussian and three non-Gaussian states.

3.7 Experimental Implementation of Verification of Quantum Discord in Continuous-Variables

In this section I will describe the experimental implementation of our method to verify quantum discord in a bipartite Gaussian states. At first, I will describe the experimental elements that we used in the experiment, including the electro-optic modulators (EOM), laser source and the mode cleaning cavity. Then I will describe the actual implementation of my experiment and present the results.

3.7.1 Electro-Optic Modulators (EOM)

Phase modulation (see subsection 2.9.1) can be produced by varying the optical path length, while amplitude modulation (see subsection 2.9.2) can be achieved through

the attenuation experienced by the beam.
For frequencies less than 200 kHz, varying the position of the mirror can cause phase modulation. But at higher frequencies, an effective technique is to elctro-optically modulate the refractive index of a crystal with high electro-optic coefficient like lithium niobate $LiNbO_3$ or KTP, using an external electric field. Type of the crystal determines the direction of the electric field which can affect the refractive index along a particular optical axis. The change in the optical path length, hence the phase of the exiting optical field from the crystal, depends on the applied electric field. The refractive index will follow the field, up to several GHz. Hence, these devices which are called electro-optic modulators (EOM) can be used to modulate the phase of the optical beams.
For amplitude modulation, a birefringent nonlinear media such as $LiNbO_3$ is used. The polarization of the input field is set to be at 45^o to the optical axis of the crystal. In this case the applied voltage affects the two linear components of polarization differently. Hence, the crystal performs as a variable waveplate, rotating the polarization of the exiting optical field as the applied voltage changes. This causes polarization modulation. After transmission trough a polarizing beamsplitter (PBS), which passes the rotated component of polarization, an optical beam with different level of amplitude attenuation (modulation) will be achieved. Thus the intensity of the optical beam varies sinusoidally as the voltage varies linearly.
However, the birefringence of these crystals are very dependent on the temperature. In order to overcome the temperature sensitivity, generally two equally length crystal with their optical axes at 90^o to each other are used.

3.7.2 Source Laser

In all the experiments described in this thesis, an Innolight Diabolo Nd:YAG solid state laser was used, as the light source in the entire experiment. This laser is particularly designed for experiments in Quantum Optics. The Diablo laser system consists of three main units: (1) laser head, (2) laser control electronics unit and (3) frequency doubling control electronics.
Laser's head of the Diabolo system consists of two laser diodes electronically driven to provide the pump radiation for a monolithic Nd:YAG laser crystal. The fundamental emission of the monolithic Nd:YAG ring laser is at 1064 nm. The ring geometry provides high frequency stability and very narrow spectral linewidth of 1 kHz.
In order to generate second harmonic radiation, part of the infrared optical field is sent through an optical isolator and electro-optic modulator (EOM), and is focused to a SHG external resonator. This resonator contains a nonlinear crystal generating second harmonic radiation at wavelength of 532 nm. The laser system delivers 180 mW of output power at 1064 nm and 1 W at 532 nm.
The electronic units are connected to the laser head to provide the injection current of diode laser's p-n junctions. Besides, temperature stabilization of diode lasers and Nd:YAG crystal is essential, which is provided by the control electronics.
Spatial generation of pairwise frequency doubled light depends on the phase mis-

match between the fundamental and the second harmonic feeds, so called phase matching condition, and on the stability of the external SHG resonator at the fundamental laser frequency. Phase modulation at 12 MHz which is generated via an internal EOM (described in section 3.7.1), is used to keep the external SHG cavity at resonance, utilizing an active feedback control in PDH (Pound-Drever-Hall) configuration [86, 87]. The frequency doubling control electronics unit provides the circuitry for the cavity stabilization as well as the necessary temperature stabilization of the nonlinear crystal.
Besides, the Diabolo system is equipped with an intensity noise reduction system called the (*Noise Eater*). The intensity fluctuations or the noise is basically due to the laser's relaxation oscillations. This effect is caused by the oscillation of the laser's energy between atomic level population and the laser cavity field. For this system the intensity fluctuations peak at 1 MHz. The Noise Eater via an electronic feedback loop located in the laser control electronic unit suppresses the intensity noise above 100 Hz by 25 dB. Keeping Noise Eater on is particularly important for generation and measurement of squeezed light which will be described in section 6.3.
In the experiment both the fundamental and SHG laser beams are passed through Faraday isolators to avoid any unintended back-scatter to the laser.

3.7.3 Seed Beam Preparation

Quantum optics experiments are very sensitive to the spectral noise and spatial mode-mismatching. In order to prepare a quantum-noise limited optical field with well-defined spatial mode (TEM-00 in our experiment), the 1064nm (seed) beam is passed through a mode cleaning cavity (MCC). The mode cleaning cavity performs as a low-pass filter, suppressing the remnant of the intensity noise coming from the laser's relaxation oscillation, providing a quantum-noise limited optical field. Besides, it defines the spatial Gaussian mode of the transmitted optical field.
We used a 3-mirror triangular ring design for our mode cleaning resonators. Both ring cavities have the same design consisting of two flat input/output mirror, and a back curved mirror with a radius of curvature of 100 cm. The curved mirror is attached to a piezo-electric actuator (PZT), which controls the length of the cavity. This design particularly has the advantage of preventing the incidental optical beam from reflecting back towards the source. The optical path length of the MC cavities is 800 mm, with cavity linewidth of 0.4 MHz for the 1064nm beam, and 1.0 MHz for the 532 nm beam. This additional suppression of the remnant relaxation oscillation provides a quantum noise limited laser field at frequencies above 2.7 MHz.
We used the 12 MHz modulation coming from the laser to create the locking error signals. The reflected beam from each cavity is detected by a photodiode to provide an error signal using PDH locking technique [86, 87]. After the error signal is passed through an analog PID (Proportional-Integral-Derivative) controller and high voltage amplifier, the feed-back signal is fed to the PZT to keep the cavity on resonance with the optical field.

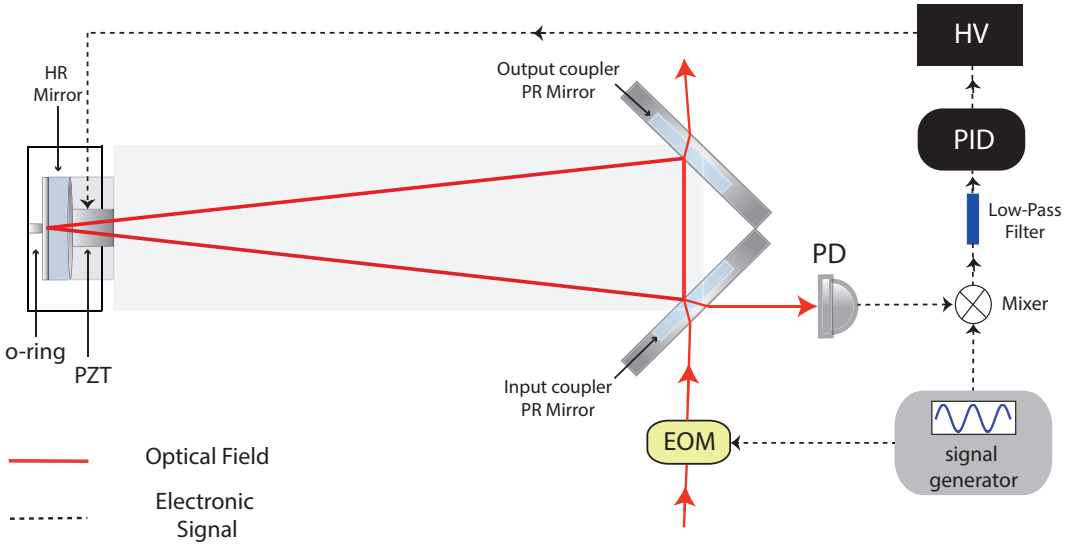


Figure 3.1: Schematic diagram of a mode cleaning ring cavity and the feed back control loop. Here EOM is electro-optic modulator, PD is photo-detector, PZT is a piezo-electric actuator, HR is highly reflective and PR is partially reflective mirror. PID is proportional-integral-derivative control system and HV is high voltage amplifier. The reflection of the laser beam is detected by a photo-detector, demodulated at 12 MHz, the resulting error signal is used in PDH feed back control loop to keep the laser on resonance. The signal generator was used to drive the crystal in EOM and provided the electrical local oscillator for demodulation.

3.7.4 Producing a vacuum state with Gaussian distributed noise

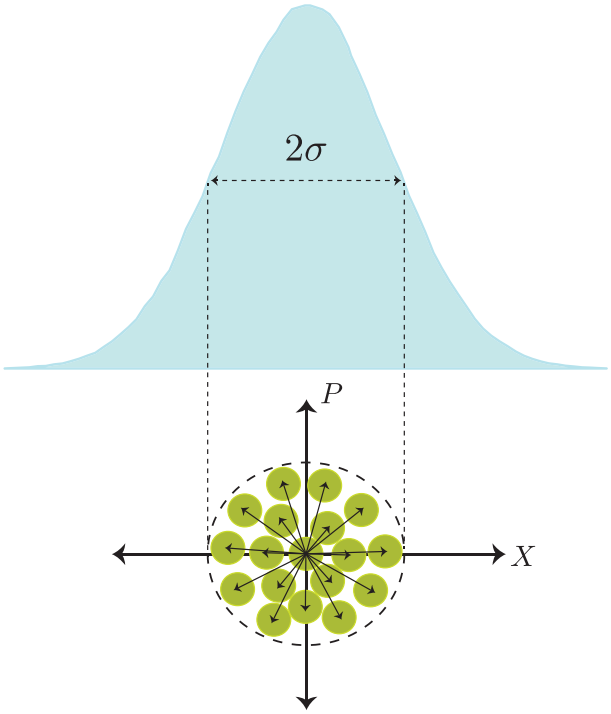


Figure 3.2: Vacuum state with Gaussian distributed noise. Here σ is the standard deviation of the distribution, and X and P refer to the phase and amplitude quadrature.

In this experiment we created the vacuum state with Gaussian distribute noise. It is shown schematically in figure 3.2. In order to prepare this state, a laser beam is modulated by a pair of phase and amplitude eletro-optic modulators, driven by function generators producing white noise. White noise refers to a signal consists of uncorrelated samples, like the numbers generated by a random number generator. Due to the randomness, the signal will consist all the frequencies with equal proportion. It has been named in analogy to the white light which consists all the frequencies. Most function generators can produce white noise with Gaussian distribution. Hence, a beam of laser modulated by Gaussian noise will be displaced randomly in phase-space, with the overall radius corresponding to the standard deviation of the Gaussian distribution, set by the function generator.

3.7.5 Experimental Implementation of Verification of Quantum Discord in Gaussian States

The experimental setup used to verify the presence of quantum discord is depicted in Figure 3.3 (a). The laser light was passed through a mode cleaning cavity to provide a quantum noise limited light source (for description on laser source and mode cleaning cavity see subsections 3.7.2 and 3.7.3). A large portion of it, was used as

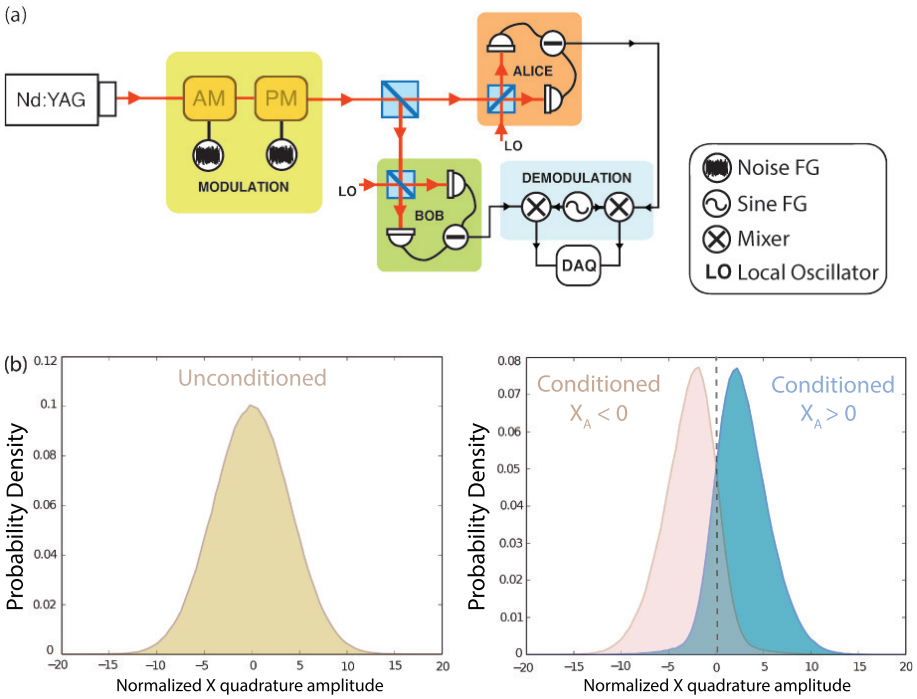


Figure 3.3: (a) Schematic diagram of the experimental setup. Here, AM and PM are the electro-optic modulators (EOM) driven by function generators (FG), which in turn provide displacement of the vacuum state in amplitude and phase quadrature with Gaussian distributed noise. Laser light is passed through electro-optic modulators and is split on 50:50 beam splitter. Each part is sent to a homodyne measurement station (Alice and Bob). Collected data points from each homodyne station are demodulated and sampled using a digital data acquisition system (DAQ). (b) The unconditioned (left) and conditioned (right) probability distributions of the bipartite Gaussian state with discord. The state is obtained from a Gaussian distributed modulated beam with modulation depth of 4.5 times the quantum noise (see subsection for the definition of modulation depth 2.9.1). The blue and pink shaded curves show the probability distributions conditioned respectively on $x_A > 0$ and $x_A < 0$, where x_A is the measured amplitude quadrature of subsystem A normalized to quantum noise. The peak separation indicates that the states A and B are discordant.

the bright source of local oscillator for homodyne detection, and a small portion, was passed through a pair of phase and amplitude elctro-optic modulators (EOM). EOMs (see subsection3.7.1) were used to provide Gaussian distributed modulation on both quadratures (as described in subsection 3.7.4). The modulated beam was then split on a 50:50 beam splitter to generate two separable but correlated bipartite state (A and B). Each part of it, was sent to a homodyne measurement station, which we labeled Alice and Bob.

In our experiment each pair of detectors were balanced electronically, providing 30 dB of common mode rejection. A pair of photo-detectors using the Uni-PD circuits with a combination of the *Epitax ETX-500* photodiodes were used for the homodyne detection. Typical suppression of cross correlation between orthogonal quadrature was around 25 dB. For each separate homodyne detection, 2.4×10^6 data points were sampled at 14×10^6 samples per second utilizing a digital data acquisition system (see section 7.3). In order to provide adequate statistics, this procedure was repeated over five times for each data point. These data were then down sampled and digitally filtered to 2-5 MHz. Our homodyne efficiency was typically 96.6%, with fringe visibility of 97.6%, generally limited by the mode distortions introduced by the EOMs and the photodiode quantum efficiency of 99%. The homodyne efficiency was estimated using the relationship $\eta_{Hom} = \eta_M \, . \, \eta_{QE}$ [39], where η_{Hom} refers to the overall efficiency of the homodyne, η_M denotes the degree of mode matching and η_{QE} is the quantum efficiency of the detector. The degree of the mode matching of the homodyne is quantified by the power of two of the fringe visibility.

Following subsection 3.6.1, in order to check whether the elements of matrix $\mathbf{C}$ are zero or not, all possible correlations between two subsystems A and B need to be inspected. In order to do so we first locked Bob's station to amplitude quadrature and performed homodyne measurements on both of the stations by locking Alice's station to amplitude quadrature, followed by phase quadrature (see section 7.3 for description on the scheme we used to lock the homodyne on a desired quadrature). The same procedure was repeated when Bob's station was locked to the phase quadrature. The marginal distributions of Bob's state conditioned on Alice's outcomes, $x_A > 0$ and $x_A < 0$, were calculated and any possible separation between the peaks of conditional marginal distributions were investigated. In our experiment, the bipartite Gaussian state had correlations in both phase and amplitude quadratures but with very little cross-correlation between the quadratures of two subsystems. Hence when Alice and Bob were both locked to the same quadrature, we observed separation between peaks of the conditional marginal distributions, as shown in Figure 3.3(b) for amplitude quadrature. In this figure the probability distribution conditioned on $x_A > 0$ is shown by a blue shaded curve and the probability distribution conditioned on $x_A < 0$ is shown by the pink shaded curve . Similar result was obtained when both subsystems were locked to the phase quadrature. As discussed in subsection 3.6.1, for Gaussian state the peak separation in the conditional marginal distributions is a necessary and sufficient condition of existence of non-zero quantum discord. Hence from our result we conclude that we have had a discordant bipartite Gaussian state as the peaks of the blue and pink curves do not coincide. The covari-

ance matrix of the bipartite state which is shown in Figure 3.3(b) is presented here. It was build from the data collected from the quadrature measurement performed on Alice and Bob's optical fields (see section 2.6 for the description on the covariance matrix and the way to build it). It shows that **C** is indeed non-zero.

$$\sigma = \begin{pmatrix} 15.96 & 0 & 17.58 & 0 \\ 0 & 14.37 & 0 & 13.55 \\ 17.58 & 0 & 22.62 & 0 \\ 0 & 13.55 & 0 & 14.81 \end{pmatrix} \tag{3.11}$$

It can be seen from this covariance matrix that there are correlations between the quadratures of two subsystems ($\mathbf{C} \neq 0$). Hence quantum discord is nonzero [74]. It confirms our method that quantum discord is not zero when peaks of the conditional marginal distributions corresponding to two outcomes of homodyne measurements do not coincide.

We also investigated the effect of the variation of modulation depth on the peaks separation of conditional marginal distributions (see section 2.9 for the description on the modulation depth). This was done by changing the variance of Gaussian noise introduced by (EOM) on the desired quadrature (see subsection 3.7.4) . Since we only modulated the phase quadrature, both subsystems were locked to this quadrature. We applied 22 different modulation depths on the phase quadrature, ranging from zero to 5 times the quantum noise. For each homodyne detection, 1.2×10^5 data points were sampled at 200 ksamp per second and then down sampled at 4 MHz sideband. The process was repeated 20 times in order to provide sufficient statistics. For each modulation depth, the conditional marginal distributions were evaluated and the separation between two peaks was measured. As shown in Figure 3.4(a), the separation of the peaks increased monotonically with the modulation depth. This was consistent with the theoretical curve plotted by equation 3.7. As the modulation depth increased, more noise was applied on the input beam and thus increases the variance of the input beam. This gave rise to output beams with higher correlations, and hence larger elements of matrix **C**. It is remarkable that despite the simplicity of our technique, it is robust enough to verify the presence of discord in weakly correlated bipartite Gaussian states, as indicated in the Fig 3.4(b).

3.7.6 Experimental Implementation of non-Gaussian State

As discussed in subsection 3.6.2, our discord verification technique can be applied to bipartite non-Gaussian states obtained by overlapping a statistical mixture of coherent states and vacuum state on a beam splitter. It was previously reported in ref [88] that a mixture of coherent states can be generated by subjecting a laser beam to time varying modulation. Here, I demonstrate our verification technique to examine quantum discord in non-Gaussian states discussed in subsection 3.6.2. In the following, I describe the preparation of three non-Gaussian states with positive-definite Wigner functions and discuss the corresponding verification results (see Figure 3.5).

1) *Switched Noise Modulation* - The first non-Gaussian state was an equal statistical

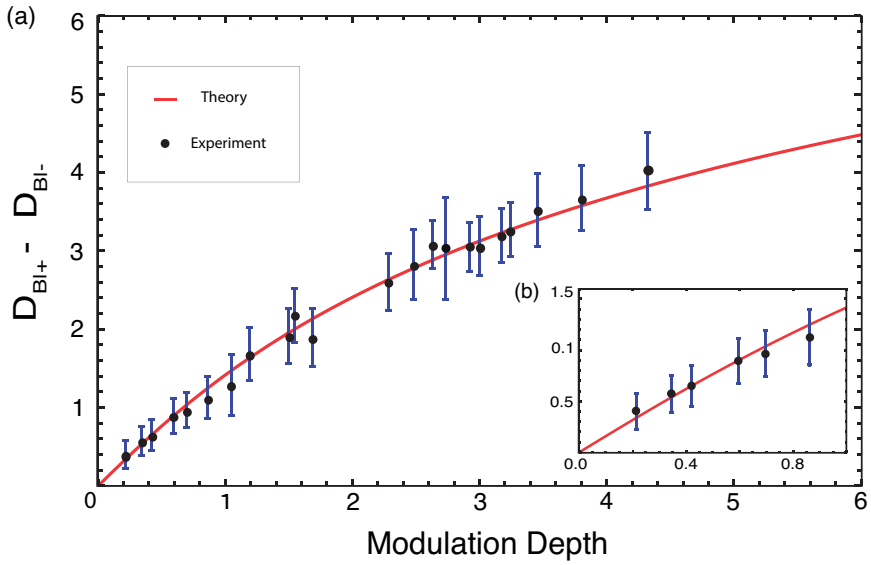


Figure 3.4: (a) Variation of peak separations of marginal distributions conditioned on two different homodyne outcomes, $D_{B|+} - D_{B|-}$, versus modulation depth. The theoretical curve was evaluated according to equation 3.7. The experimental error bars were estimated using statistical uncertainties. Inset (b) shows the zoom-in for small modulation depth. Even for the smallest modulation depth (0.2 times of quantum noise), our technique is still able to reveal the presence of quantum discord.

mixture of vacuum and a thermal state. The thermal state was produced by applying two independent Gaussian distributed noise signals to a phase and amplitude modulator. An external square wave modulation envelope at 12 kHz was then used to gate the two modulators. Square wave modulation turned the Gaussian modulation, on and off periodically. In this way the optical field had either Gaussian modulation or no modulation at all. Since the square wave gating frequency was fast compare to the detection time, the net detected statistics seen would consist of an equal contribution from both the vacuum and the thermal state. Modulation and demodulation arrangement and the Wigner function of the produced state are shown schematically in Figure 3.5(a). The laser light with this non-Gaussian modulation then splits on a 50:50 beam splitter and each part was sent to a homodyne measurement station. To investigate the correlations between two subsystems, the same measurement procedure was performed as described in subsection 3.7, and the results are presented in Figure 3.6 (a).

2) *Switched Phase Modulation* - The second prepared non-Gaussian state was a mixture of vacuum and a coherent state. As depicted in Figure 3.5(b), a sine wave modulation with frequency of 4 MHz was introduced to phase quadrature to create the coherent state. We then added a square wave modulation with frequency of 120 Hz to gate the sine modulation on and off. With this arrangement there was a sine modulation for half of the measurement time and no modulation for the other half. Signal was detected synchronously by using the same demodulation frequency as

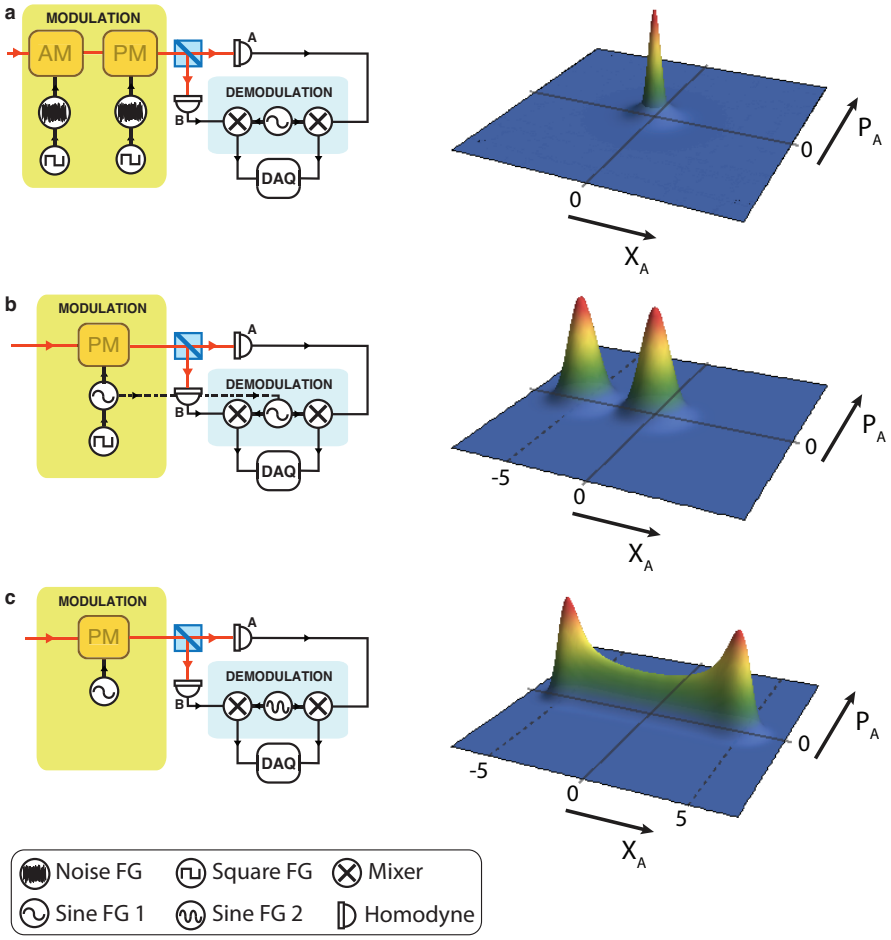


Figure 3.5: Schematic diagram of the modulation and demodulation arrangements used in preparation of the non-Gaussian states (left) and their corresponding positive-definite non-Gaussian Wigner functions (right), X_A and P_A are normalized quadrature amplitudes (a) Switched noise modulation: This vacuum-thermal superposition state is generated by gating Gaussian noise modulation on both quadratures with square waves; (b) Switched phase modulation: This state is an equal statistical mixture of a vacuum and a coherent state, created by gating a sine wave modulation with a low frequency square wave; (c) Asynchronous detection: This state is prepared by modulating one quadrature with sine wave and demodulating it with another sine wave of slightly different frequency.

used for modulation. Similar procedure as described before was repeated to prepare a correlated bipartite state. In order to verify the presence of discord, the marginal distributions of Bob's state conditioned on two different sets of Alice's outcomes $x_A < -6$ and $x_A > -6$ were calculated and any possible correlation in conditional marginal distributions was investigated[1]. The results are shown in Figure 3.6(b).

[1] As discussed in Section 3.6.2, in order to verify quantum discord in this class of non Gaussian states

3) *Asynchronous Detection* - We prepared the third non-Gaussian state by using asynchronous detection. This was experimentally realised by choosing a demodulation signal different in the frequency by an small amount compared to the modulation signal. As displayed in Figure 3.5(c), we drived the EOM by sine wave with frequency of 4 MHz and demodulated with frequency of 3.99MHz. The data collected was then digitally filtered to 3.9-4.1 MHz. The prepared state was a two peak probability distribution function along the X-quadrature as shown by Wigner function in Figure 3.5(c) right. This is analogous to the stroboscopic measurement of the quadrature of a harmonic oscillator. The marginal probability distribution of the prepared state and the conditional probability distributions are presented in Figure 3.6(c).

As can be observed from Figure 3.6, it is evident that the conditional probability distributions for all three non-Gaussian states are different from their unconditioned distributions. Neither their peaks nor the mean values of their distributions coincide, which by considering the preparation method, is a sufficient evidence of the presence of nonzero discord in the three non-Gaussian states. As the difference between two conditional marginal distributions is the criterion to verify quantum discord, in situations where the conditional distributions are very similar to each other, one can deploy χ^2 test and calculate its probability function. Generally one rejects the *null* hypothesis if the probability function is less than 0.05, which means two distributions are not the same. In our experiment, the calculated probability function is zero for all the states, indicating the two conditional distributions are completely different and the states are discordant.

3.8 Summary

In this chapter I discussed the general form of quantum correlations, existing even in separable states, known as quantum discord. I reviewed Gaussian quantum discord and the previous method for verifying quantum discord. Then I introduced our experimental technique for verifying quantum discord in unknown bipartite Gaussian states which is a development to the previous one. According to our technique by checking peak separation between the marginal distributions conditioned on two different homodyne measurements outcomes, the correlation of corresponding quadrature can be tested. With this technique, quantum discord can be verified by investigating the correlations between all four combinations of the amplitude and phase quadratures of two subsystems. By varying the modulation depth, we showed that our results are indeed consistent with the theoretical predictions within statistical errors. The robustness of our technique in small modulation depth permits one to detect nonzero discord even when the correlations are small. Moreover, we have discussed that our technique can be used for a certain class of non-Gaussian states. We applied our method to three different bipartite non-Gaussian states, which were prepared by subjecting statistical mixtures of coherent states to one port of beam

it is sufficient to calculate marginal distributions conditioned on any two sets of Alice's outcomes.

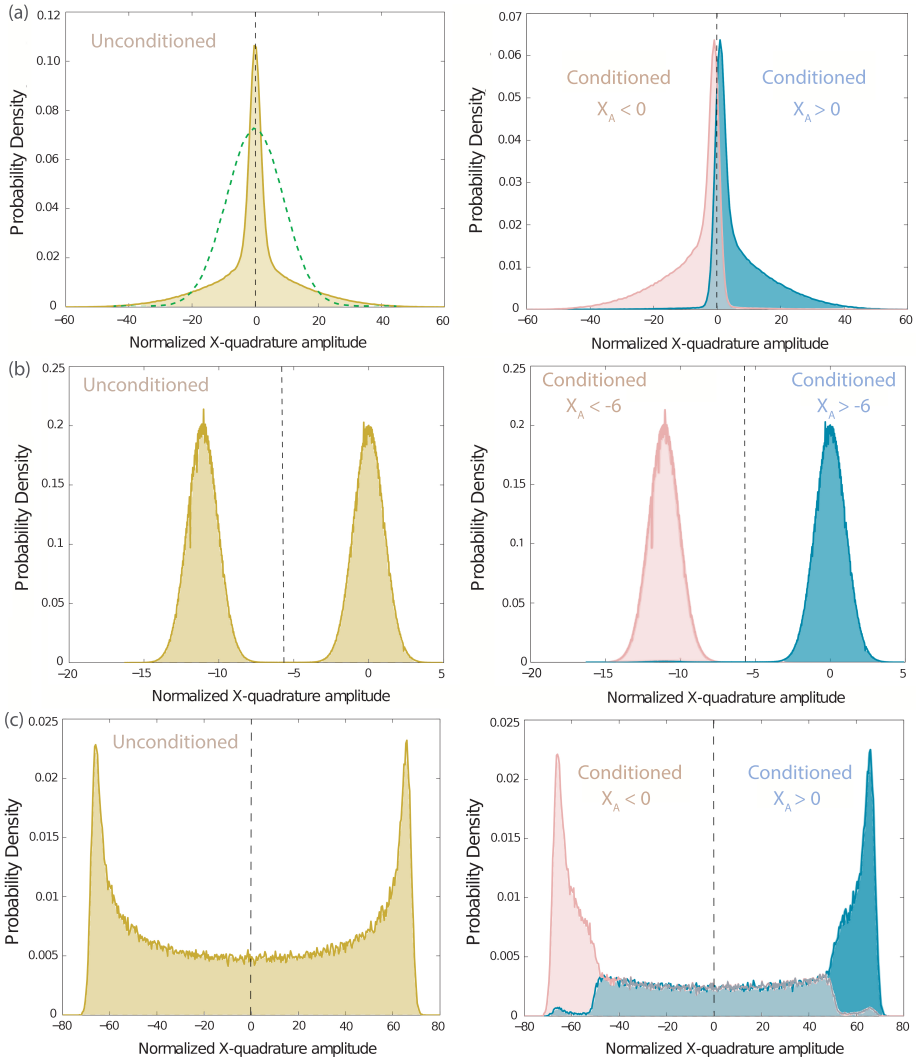


Figure 3.6: Unconditional (Brown) and conditional probability distributions of two different outcomes (Pink and Blue) of the non-Gaussian states prepared by (a) Switched Noise Modulation (The green dashed curve corresponds to a Gaussian state with average variance of the two Gaussian distributions); (b) Switched Phase Modulation; and (c) Asynchronous Detection. We observe that the unconditional distributions are non-Gaussian, and also changes in the conditional marginal distributions in all three cases. Hence, according to Section 3.6.2, all the three non-Gaussian states have nonzero discord.

splitter while the other port is in the vacuum state. Experimental results for all the non-Gaussian states show that the conditional marginal distributions are significantly different from the unconditional distributions, indicating nonzero quantum discord in each case. Our results ascertain that with some prior knowledge about a quantum state, such as being Gaussian, or about the preparation stage quantum discord can be efficiently verified with a finite number of measurements.

Chapter 4

Secure Quantum Communication

4.1 Introduction

A central task in cryptography is the distribution of a secret key among distant parties, so they can use it to encrypt the messages. This field has a long history and has its own successes and failures. Many different cryptographic techniques appeared over the centuries and all of them broke at some point. Until in 1917 Vernam invented the *one-time pad* encryption method, using a symmetric, random secret key shared between two parties. This technique cannot be broken in principle and Shannon proved that this scheme is optimal (Shannon,1949). But to implement this scheme the communicating parties require to share a secret key as long as their messages, which makes it impractical when large amount of information needs to be encrypted. Hence, in classical cryptography, other schemes are being utilized where the security actually relies on the hardness of a certain mathematical problem. For instance, large number of current Internet transactions are secured by public-key cryptography known as Rivest-Shamir-Adleman (RSA) protocol, which relies on the difficulty of factorizing large numbers. Although no efficient factorization algorithm is recognised for classical computers, these schemes can be broken if quantum computers were available by using Shor's algorithm [6].
New horizon on secure cryptography has appeared in the last three decades with Bennett and Brassard's proposal of key distribution in 1984 [8]. The proof that this so-called BB84 [8] protocol is unconditionally secure depends only on the validity of the quantum mechanics [92]. This idea which was later rediscovered by Ekert (Ekert 1991) [9], was the beginning of the *Quantum Key Distribution* [7, 6].
Quantum Key Distribution is generally divided into two regimes : DV (discrete-variable)-QKD and CV (continuous-variable)-QKD. In DV-QKD properties of single photons, like their polarization, are used to encode the information. Where in CV-QKD [93, 91] the information is encoded in the quadratures of the optical fields. The main elements of CV-QKD are the modulation or encoding of the Gaussian states and decoding through Gaussian measurement, e.g., homodyne and heterodyne detection. The early QKD schemes used DV-QKD to encode a discrete variable (DV) key in a 2 dimensional Hilbert space. However, the challenging optical implementation of DV scheme including single photon generation and detection has also attracted lots of

attention towards continuous-variable (CV) scheme. In CV scheme one has access to deterministic, high efficiency broadband sources and detectors. But it is now theoretically more demanding , as the key is a continuous variable encoded in states in infinite dimensional Hilbert space.
Quantum key distribution (utilizing either DV or CV scheme) has progressed rapidly in recent years with reported Quantum Key Distribution over 80 km of optical fibre [10] , and real-world implementation [11, 12]. Commercial devices are also readily available these days. However, despite all these improvements, it appeared that the security of QKD depends on the actual implementation of the protocol. Now the problem is how one can asses the level of the security in practice, which is inevitably different from the idealized theoretical description. Especially using the commercial devices opens the door for new kind of attacks [95, 96] and hacking of the commercial quantum cryptography systems [97, 98].

To address this challenge several approaches have been proposed. The first approach, which aims to guarantee security without making any assumptions on the devices utilized in the protocol, results to the birth of the concept now known as " Device Independent QKD (DI-QKD)" (see section 4.3). The security of DI-QKD is provided via the violation of a Bell's inequality [5]. While DI-QKD is theoretically feasible, its practical implementation is very challenging, as it requires a *loophole free* violation of a Bell test [15, 16]. Finding ways around this problem itself becomes an active field of research. One of the suggested ways is known as the "measurement-device-independent QKD" (MDI-QKD) as a simple solution to omit detector side channels (see section 4.4). Another approach is "one-sided device-independent QKD (1SDI-QKD)" where only the apparatuses of one of the communicating parties are trusted. This scheme places between standard QKD, where both parties trust their measurement apparatuses, and DI-QKD where neither do (see section 4.5).
In this chapter I will describe how a generic quantum key distribution protocol works. Then I will review briefly the concept of DI-QKD and introduce the important researches that developed this field. I will continue by summarizing the "measurement-device-independent QKD", and finish the chapter by discussing the "one-sided DI-QKD".

4.2 A Generic QKD Protocol

Here I present a generic QKD protocol. Any QKD protocol wether it is based on discrete or continuous variables consists of two main steps: (1) quantum communication part (2) classical post-processing [89].
In the quantum communication phase, at first Alice prepares a quantum state and sends it to Bob in order to perform a measurement on it. Alternatively, Alice and Bob can share an EPR state while each makes a measurement on their EPR arm. They randomly choose different bases for their measurements. Then they change a significant number of quantum states over a communication channel (quantum channel). At the end of this step, Alice, Bob and the eavesdropper (Eve) share a set of corre-

lated data [89, 90].
The next step is the classical post-processing which itself is divided into several stages. (1) The first stage is the sifting where Alice and Bob communicate and agree on the basis or quadrature they used to encode or decode the information, discarding the other observation results [89, 90]. (2) The second stage is the parameter estimation, where Alice and Bob try to estimate the amount of information they share (I_{AB}), and the amount of information the eavesdropper may gain (I_{AE} or I_{BE}). In order to do so, Alice announces some randomly chosen sample of the data that she forwarded to Bob, and Bob reveals his corresponding measurements. If they find out that the eavesdropper knows too much about their key, they will abort the protocol at this point [89, 90]. (3) The third stage is error correction, where the two communicating parties try to find the syndromes of the errors affecting their data [89]. (4) The forth step in the "reconciliation" step, where Alice and Bob, through classical communication try to extract a common binary key, with a little information leakage as possible to the third party. There are two types of reconciliations depending on if Alice's or Bob's data are used to form the key. The first one is called *Direct Reconciliation (DR)*, where Alice's data are the reference and must be estimated by Bob (and Eve). Here Bob corrects his key elements according the the correction that Alice sends to him. From the estimate of I_{AB} in the first step, Alice infers the amount of information she can reveal at this step. If $I_{AB} - I_{AE} > 0$ a usable secret key rate can be extracted. The second one is called *Reverse Reconciliation (RR)*, where Bob sends the correcting information to Alice. The she corrects her key elements to have the same values as Bob. Here if $I_{AB} - I_{BE} > 0$ a usable key can be extracted [90, 91]. (5) The fifth and the last step in a practical QKD is the "privacy amplification" where Alice and Bob try to omit the amount of information that the eavesdropper gained. The vital requirement for this step is to get a bound on I_{AE} for DR and I_{BE} for a RR protocol [90, 91]. More information on CV-QKD can be found in references like ref [89, 90, 91].

4.3 Device Independent Quantum Key Distribution

Generally the security of QKD protocols rely on the assumptions made on the dimension of the Hilbert space. As a result the security will no longer be guaranteed if the dimension of the Hilbert space changes during the actual implementation. Particularly, it has been shown that the BB84 protocol [8] will no longer be secure if two parties share four-dimensional space instead of qubits as often considered [99]. But, due to the imperfections in the devices the measurement direction may be drifted with time, or the entire device may be malicious, as they might be bought from an untrusted supplier. Hence, to guarantee the security in DI-QKD protocols the quantum apparatuses used are considered to implement a quantum process without making any assumption in terms of the Hilbert space, operators or states. In this case the security is provided, based only on the fundamental set of basic assumptions which are: (i) access of Alice and Bob to secure locations, (ii) trusted randomness, (iii) trusted classical processing devices, (iv) an authenticated classical channel, (v) and

finally the validity of a physical theory on which the security protocols rely (either quantum mechanics or no-signaling principle) [99] . In this sense, DI-QKD is in the direction of the works aiming to provide unconditionally secure cryptography.

4.3.1 Usual QKD protocols are not secure in the device-independent scenario

Let us consider entanglement-based version of BB84 protocl [8], where measurement devices of both parties Alice & Bob act on a two dimensional subspace of the incoming particles (e.g. the polarization of the photons). Two measurement settings σ_x and σ_z are assumed. If Alice and Bob conduct measurements in the same basis, they always get perfectly correlated outcomes; while if they measure in different basis, they get completely uncorrelated random outcomes. In term of measurement operators σ_x and σ_z and the two-qubit state $|\psi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$ the mentioned correlation can be written as [99]:

$$\langle\psi|\sigma_x \otimes \sigma_x|\psi\rangle = \langle\psi|\sigma_z \otimes \sigma_z|\psi\rangle = 1 \tag{4.1}$$

$$\langle\psi|\sigma_x \otimes \sigma_z|\psi\rangle = \langle\psi|\sigma_z \otimes \sigma_x|\psi\rangle = 0 \tag{4.2}$$

The only state well-matched with this set of equations is the maximally entangled state $(|00\rangle + |11\rangle)/\sqrt{2}$. Therefore Alice and Bob can derive a secret key from their measurement data [99]. However, the same correlation can be reproduced by the four-qubit state [100]:

$$\rho_{AB} = \frac{1}{4}(|00\rangle\langle 00|_z + |11\rangle\langle 11|_z) \otimes (|00\rangle\langle 00|_x + |11\rangle\langle 11|_x) \tag{4.3}$$

Here, the first and third qubit belongs to Alice. Whenever she measures in the $z(x)$ basis, she is looking at the first (third) qubit in this basis. The same is true for Bob, with the second (forth) qubit. Obviously when the same measurement basis are used, their observed results are totally correlated. Otherwise they are uncorrelated. However, this state is separable and cannot be used to extract a secure key [100].
This simple example shows that if the dimension of the Hilbert-space varies in practice from what is assumed in theory, the QKD protocol is no longer secure. Experimentally, additional Hilbert-space dimension refers to "side channels" i.e., to degrees of freedom coded accidentally. Hence, it is desirable to find a scheme that Alice and Bob can exploit a well established physical principle to extract a key from some observed correlation, without having to care about the experimental details [100].

4.3.2 How can DI-QKD possibly be secure?

As suggested from the early work on QKD by Ekert, violation of a Bell's inequality is the key to the secure communication [9]. This idea is developed further by Jonathan Barret et al [101] and Antonio Acin et al [100], which suggests that a correlation

should not be described in terms of local hidden variables in order to be secure in the device independent scenario (see section 8.2 for more discussion on the hidden variables and correlation function). Formally it can be written as [99]:

$$P(a,b|X,Y) \neq \sum_{\lambda} P(\lambda)D(a|X,\lambda)D(b|Y,\lambda), \tag{4.4}$$

where $P(a,b|X,Y)$ is the probability to observe the pair of outcomes a,b if they have made measurement X,Y. λ is a classical variable with probability distribution $P(\lambda)$ shared by Alice and Bob's apparatuses, and $D(a|X,\lambda)$ is a function defining Alice's outputs once the input X and λ are known. The same applies for $D(b|Y,\lambda)$.
In the reverse scenario Eve may posses a copy of λ. Hence knowing the input X and the classical variable λ, she can estimate the outcome a from $D(a|X,\lambda)$. The same is true for the outcome b and $D(b|Y,\lambda)$. Only the violation of a Bell's inequality [5] guarantees that the outputs of Alice's and Bob's apparatuses are correlated in a non-local way, and can be written as equation 4.4 (see sections 8.2,8.3 for more discussions on Bell's inequality). This follows from the fact that non-local correlations are generated from entangled state, whose measurement statistics are random and cannot be known completely by the eavesdropper. This is the physical principle on which all the device-independent security proofs are based [99].

4.3.3 History of DI-QKD

As mentioned earlier, the idea that the security of a QKD protocol can be based on the violation of a Bell test was the essence of Ekert's 1991 proposal [9]. But a challenge now known as Device-Independent-QKD was first introduced by Mayers and Yao [13]. However, Barret, Hardly and Kent [102] were the first to initiate the quantitative progress towards the strong security proofs. Their concern was to prove secure quantum key distribution based on other physical principle rather than quantum mechanics. They suggested a key distribution scheme secure against general attacks by a post-quantum eavesdropper limited only by no-signaling principle. The no-signaling condition says that no measuring process can be used to send information between distant locations. In other way local probabilities are independent from distant partner's inputs [99], e.g.,

$$P(a|X,Y) = \sum_{b} P(a,b|X,Y) = P(a|X). \tag{4.5}$$

According to them even if quantum mechanics were ever to fail, security can be guaranteed based on the violation of a Bell's inequality. It is true because once the no-signaling condition is assumed the security is based on the principle called monogamy which is analogous to entanglement in quantum mechanics. In its simplest form the monogamy of entangled states means that the two quantum systems that are maximally entangled cannot share entanglement with a third system [99].
Their work was a proof of principle as they proved security only for a noise-free quantum channel. However, a sequence of follow-up papers extended their idea.

In the paper "*From Bell's Theorem to Secure Quantum Key Distribution*" Antonio Acin et al [**?**] presented a QKD protocol aimed at producing data that violate the CHSH inequality (see section 8.3), and they proved its security against the most general individual attack without signaling, independently of any assumption on Hilbert spaces. Their results represented the first step towards the characterization of optimal non-signaling attacks. The improvement of their results compared to [102] was that their analysis covers the noisy situation.
A further progress was made by Antonio Acin, Serge Massar and Stefano Pironio [103]. They have shown that by adding one measurement to the CHSH test, the key rate and the noise resistance can significantly be improved. They argued that their approach can be based on any non-locality test, and as an illustration they have studied a family of protocols based on the chained inequalities for N measurement settings. Each inequality in the family provides a different estimation of Eve's knowledge. Their protocol is also noise-tolerant, but when N is large, the corresponding protocol is very sensitive to noise. As a result, Alice and Bob should estimate the properties of their channel and adopt the non-locality test to their measured parameters to maximize the key rate.
The work presented in Ref [100] has been expanded and generalized further by V. Scarani et al. in Ref [104]. One of the perspectives opened by their work was the idea of making a device-independent proof of security against an eavesdropper which would be restricted by quantum physics. The advantage of using quantum mechanics is that Eve would be limited in comparison to the power she can posses according to the no-signaling principle; so one can hope to extract better secure key rate.

A substantial progress was made by A.Acin et al in [14]. They concentrated on the more realistic situation in which Eve is restricted by quantum physics, and they have found the optimal collective attacks on a QKD protocol in the device-independent scheme. Their main outcome was a tight bound on the Holevo information between one of the authorized parties and the eavesdropper, as a function of the amount of violation of a Bell-type inequality. This work has been elaborated further in [99].

M. McKague in ref [105] extended the result of [99] to a more general class of attacks where the state is arbitrary and the measurement apparatuses have no memory. He accomplished it by reducing the arbitrary adversary strategies to qubit strategies and a proof of security for qubit strategies relying on the previous proof [99].

Another important theoretical analysis on DI-QKD carried on by L. Masanes in ref [106] where they showed that fully DI-QKD is in principle, possible. Their proof was based on both the no-signaling principle and the validity of quantum mechanics. Their approach can be applied to protocols based on arbitrary Bell's inequalities and is valid against the most general attacks. Their model was limited by the assumption that the measurement processes generating the different bits of the raw key are casually independent of each other (though they could be arbitrarily correlated). This independence condition may be justifiable in several implementations and is necessarily satisfied when the raw key is generated by N separate pairs of devices.
A fully DI-QKD protocol against the most general "coherent" type of attacks with

2% loss tolerance in apparatuses was introduced by Umesh Vazirani and Thomas Vidick in [111]. They showed that the variant of Ekert's original protocol has all the necessary features of DI-QKD. However, the experimental implementation of their protocol faces the same difficulties as other DI-QKD protocols, which are mainly due to the "detection loophole".
And finally the only DI-QKD protocol in CV regime that I found was proposed by C. J. Broadbent et al in [112]. They used generalized two-mode Schrodinger cat states and proved the security against collective attacks and some coherent attacks.

Despite all the theoretical progress on DI-QKD, realization of these protocols still remains a challenge, as all the experimental tests of Bell's inequalities that have been made so far, are subject to at least one of several loopholes. Besides it is impossible to violate a Bell's inequality utilizing only Gaussian resources [107] which makes CV DI-QKD not very feasible.
Considering Bell's test, two requirements are needed for a loophole-free Bell experiment to guarantee that no local description can be admitted : 1) no information about the input of one party should be revealed to the other party before she has produced her output; 2) high enough detection efficiency. If the first requirement is not satisfied, which is known as locality loophole, it is trivial for a classical model to account for the non-locality of the observed correlations. The second requirement arises from the fact that not all signals are detected. This loophole, known as detection loophole, suggests the idea that there is a local variable that determines if a signal will be detected or not. In usual Bell experiments, the locality loophole is dealt with by enforcing a space-like separation between Alice and Bob. This ensures that no sub-luminal signals could have traveled between Alice's and Bob's apparatuses. However the detection loophole, is a much more complicated issue to deal with [99]. Since not all entangled photons are detected, and the unavoidable losses in quantum channel, losses in the coupling between the photon-pair source and the optical fibres and finally finite detection efficiency make detection loophole a more complicated issue to deal with. In usual Bell test the fair sampling assumption is considered which states that the set of detected photon pairs is a fair set of all the photons. It is reasonable to assume that Nature is not malicious. But in DI-QKD the fight is against a possible active and malicious adversary [99].
To overcome the channel losses in Bell test, N. Gisin et al in [108] proposed a heralded qubit amplifier based on single-photon sources and linear optics. They were inspired by the proposal of Ralph and Lund on the use of quantum teleportation to realize a heralded single-photon amplifier [109]. They showed that the entangled component can be amplified in a heralded way, offering the possibility for Alice and Bob to share a maximally entangled state despite losses in the channel. Hence, the overall detection efficiency required to close the detection loophole does not depend on the transmission efficiency. The implementation of their proposal is feasible, though it is hard. Their calculations demonstrated DI-QKD over 10-20 km of standard telecom fibre.
Another approach to circumvent the detection loophole was proposed by C. C. W. Lim et al in [110]. Their protocol involves a third party Charlie, whose task is to help

Alice and Bob distribute their key strings. However, it is not necessary to trust the third party. Importantly, the protocol only requires Bell tests conducted locally on Alice's laboratory, so that the detection probabilities are not influenced by the losses in the channel connecting Alice and Bob. In contrast to most DI-QKD protocols, whose security is inferred from the monogamy of nonlocal correlations, the security of their protocol is based on the generalization of the entropic uncertainty relation that accounts for quantum side information [20]. The uncertainty relation only depends on the local properties of the states sent by Alice, which can be inferred from the local Bell test. Their estimate is that this protocol would provide a secure communication up to 17-km of optical fibre between Alice and Bob.

Although DI-QKD seems to be a solution for unconditional secure QKD, its implementation still remains a challenge. Two other schemes are suggested recently to overcome this hurdle. The first is " Measurement-Device-Independent Quantum Key Distribution " which aims to remove all the detector side channels. The other is "One-sided-Device-Independent Quantum Key Distribution" where only the devices of one of the communicating party is not trusted. It has been shown that the security of one-sided-DI-QKD is based on EPR-Steering which is less strict that Bell test and opens a new horizons for experimental implementation. In the next following sections I will introduce these two schemes.

4.4 Measurement-Device-Independent Quantum Key Distribution

The idea of measurement-device-independent QKD (MDI-QKD) suggested for the first time by Hoi-Kwong Lo , Marcos Curty and Bing Qi [113] as a simple way to remove all the detector side channels. Their protocol works as follows. Alice and Bob prepare phase randomized weak coherent pulses (WCPs) in a different BB84 polarization states, and forward them to an *untrusted* relay Charlie (or Eve) located in the middle, who conducts a bell-state measurement (BSM). In contrast to DI-QKD, in its simplest formulation MDI-QKD necessitates that Alice and Bob have almost perfect state preparation. Once the quantum communication phase is performed, Charlie uses a public channel to announce the events where he has obtained a successful outcome in the relay, including his measurement outputs. Alice and Bob keep the data that correspond to these instances and discard the rest. An important advantage of MDI-QKD is that the BSM does not need to be a perfect measurement. Even a partial imperfect BSM implemented by linear optical elements can do the job.
Silvestre Abruzzo et al [114] generalized the idea of MDI-QKD to the scheme where the Bell-state measurement station contains also heralded quantum memories. They found analytical formulas, in terms of apparatus imperfections, for all the quantities entering in the secret key rates. The sources they considered were either single-photon sources or weak coherent pulse sources plus decoy states. Their protocol may represent the step towards implementing a two-segment quantum repeater. Similar idea was presented in [115], where MDI-QKD was combined with quantum repeaters

based on quantum memories. Memory-assisted MDI-QKD protocols have the potential of beating the existing distance records for conventional quantum key distribution systems . A further theoretical improvement was carried on by Marcos Curty et al in [116], where they provided a rigorous security proof against general attacks in the finite-key regime. They also demonstrated the feasibility of long-distance implementations of MDI-QKD within a reasonable time frame of signal transmission.

Several attempts have been devoted to the experimental realization of MDI-QKD. One of the successful experiments was conducted by Yang Liu et al [117]. To demonstrate MDI-QKD they developed up-conversion single photon detectors with high efficiency and low noise. By assuming a reliable source scenario, their system generated more than 25 kbit secure key over 50 km of fibre link. Another experimental demonstration of MDI-QKD was performed by Zhiyuan Tang et al [118]. They have shown the first polarization encoding MDI-QKD experiment over 10 km of optical fiber, with active phase randomization implemented to defeat attacks on imperfect sources. They mentioned that their work can be extended to free space polarization encoding MDI-QKD with an untrusted satellite in the future. The notion of MDI has also been extended theoretically and experimentally to continuous variable (CV) systems [119], where Alice and Bob communicate by connecting to an untrusted relay via insecure links. To create secret correlations, they transmit random coherent states to the relay where a CV Bell detection is performed and the outcome broadcast to the parties. The authors showed that this protocol is secure theoretically up to 25 km and by extrapolating the result of their experiment to the telecom wavelength, they estimated their protocol to be secure experimentally up to 20 km in fibre optics, despite the possibility that the relay could be fully corrupted and the links being subject to coherent attacks.

4.5 One-sided Device-Independent Quantum Key Distribution

So far I discussed about the necessity of higher level of security in quantum communication and how it motivated the researchers to create the concept of DI-QKD and finding the practical ways of implementing it. However, the fact that DI-QKD is based on non-locality strongly suggests that only entanglement-based protocols are suitable for obtaining this notion of strong security. But, most of the practical QKD systems use the so-called "Prepare & Measure" scheme, where Alice prepares a quantum state and sends to Bob who then performs a measurement on it. M. Pawlowski and N. Brunner argued that a form of DI security, which they called "*semi-device-independent*", can be obtained without using entanglement [120]. They assumed that for semi-DI, the Hilbert space dimension of the quantum system is known, but the quantum preparations and measurements are noncharacterized. Since no assumptions on the devices are required except the fact that Alice's device emits preparations of one bounded dimension, it can be applied directly to the one-way configuration. Using this assumption they proved the security of one-way QKD against individual

attacks. However, it was only proof of principle.
The intermediate scenario between standard QKD (S-QKD) and DI-QKD further developed by C.Branciard et al [19] so-called as one-sided DI-QKD (1SDI-QKD). In this scenario only one of the two parties trusts his/her measurement apparatuses. They showed that the requirement for obtaining the secure key in 1SDI-QKD is the violation of the *EPR-steering inequality* [17]. That is, if one imagines that Bob's system has a definite (albeit unknown to him) quantum state, the protocol must prove that Alice, by her choice of measurement, can affect (steer) this state. It corresponds to the link between S-QKD or DI-QKD and the violation of a separability criterion or a Bell's inequality respectively. The authors proved the security of a 1SDI-QKD protocol using an approach based on an uncertainty relation for smooth entropies developed by Tomamichel and Renner [18]. This uncertainty relation enables one to prove security against coherent attacks in 1SDI-QKD scenario. They considered realistic implementation by taking into account the imperfect detection efficiencies.
Utilizing the entropic uncertainty relations recently developed for CV regime, we investigated theoretically and experimentally the entire family of 16 Gaussian CV-QKD protocols in the asymptotic setting. In the following chapters I will describe our theoretical and experimental results in detail.

4.6 Summary

In this chapter I reviewed the concept of secure quantum communication. I started with a standard QKD protocol and discussed the necessity to develop a more secure notion of QKD, which led to the development of the concepts of Device-Independent Quantum Key Distribution, Measurement-Device-Independent Quantum Key Distribution and One-sided Device-Independent Quantum Key Distribution. I mentioned that the violation of a Bell's inequality is the key that guarantees security in device-independent quantum key distribution and measurement-device-independent quantum key distribution, while the asymmetric form of non-locality know as EPR-steering provides security in one-sided device-independent quantum key distribution. Schematic diagram of all these protocols is shown in Fig 4.1. In the next chapter I will discuss one-sided device-independent quantum key distribution and EPR steering in detail, and will present our theoretical and experimental results on the development of the CV one-sided device independent QKD.

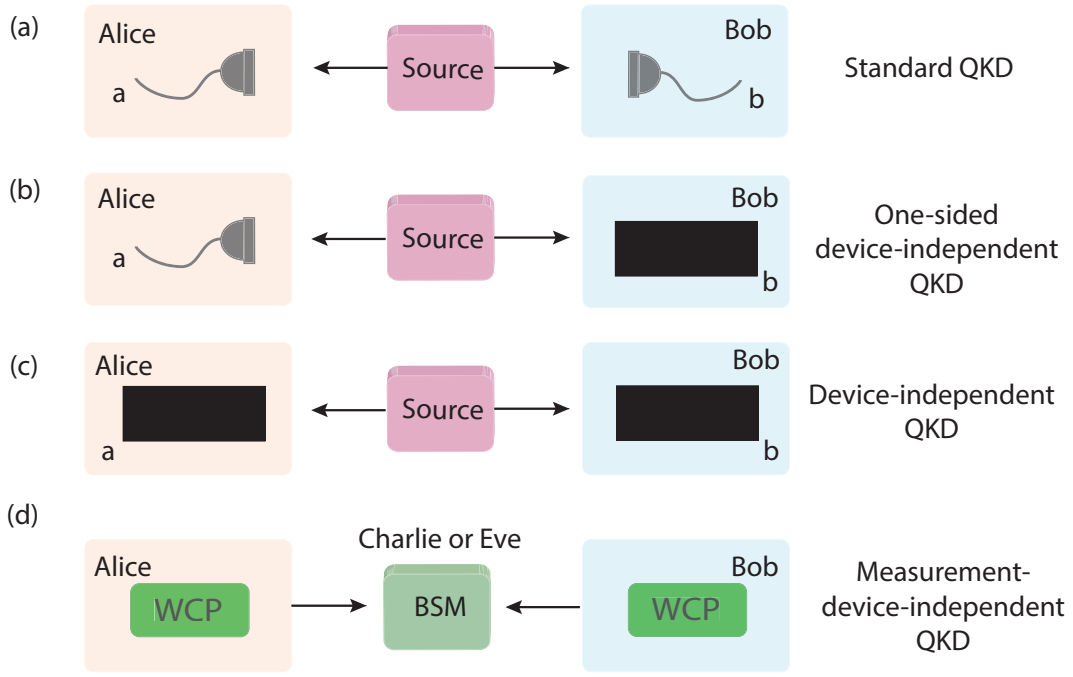


Figure 4.1: Schematic diagram of (a) standard quantum key distribution where both parties trusts their devices as described in section 4.2 (b) one-sided-device-independent quantum key distribution where only one of the communicating parties trust his/her devices and the devices of the other party is considered as a black box as described in section 4.5 and in more detail will be discussed in Chapter 5 (c) device-independent quantum key distribution where no assumption is made on devices and the devices of both communicating parties are considered as black boxes as described in section 4.3 (d) measurement-device-independent quantum key distribution, where two parties Alice and Bob prepare phase randomized weak coherent pulses (WCPs) in four possible BB84 polarization states and send them to an untrusted relay Charlie or (Eve) where he performs a Bell state measurement (BSM) as described in section 4.4.

Chapter 5

Theoretical Development of 1SDI-QKD Protocols Using Gaussian States and Measurements

5.1 Introduction

As mentioned in the previous chapter, the physical implementation of DI-QKD [13, 14], which aims to close the gap between the theoretical prediction and the real-life implementation of QKD protocols, still remains a challenge. This made scientist to explore the other possible ways to close this gap. One of the suggested approaches is called 1SDI-QKD [18, 19], where devices of one party solely are trusted. Besides, an elegant tool for cryptographic tasks appeared as M. Berta et al [20] characterized the connection between the uncertainty relations [4] and entanglement by employing the entropic version of uncertainty relations [21, 22, 23, 24, 25]. Utilizing further advances in entropic uncertainty relations [26, 27], we investigate theoretically and experimentally in the asymptotic setting, the entire family of 16 Gaussian CV-QKD protocols which can be proven 1SDI. Our investigations confirm 6 of the 16 Gaussian protocols to be 1SDI. The results of this investigation is published in Optica with the title and author list as follows :
"Experimental Demonstration of Gaussian Protocols for one-sided device independent quantum key distribution", "N. Walk, S. Hosseini, J. Geng, O. Thearle, J. Y. Haw, S. Armstrong, S. M. Assad, J. Janousek, T. C. Ralph, T. Symul, H. M. Wiseman and P. K. Lam. Optica **3**(6), 634-642 (2016)."
This research has been conducted under the "CQC2T Center of Excellence". The theory of this research has been developed by Nathan Walk, Howard M Wiseman and Timothy C Ralph at the University of Queensland and Griffith. The experiment which included four parts applying both "entanglement-based (EB)" and "Prepare and Measure (P&M)" sources was completed in our group at the Australian National University.
In this chapter I will present my own understanding of the theoretical investigation, which is essential to know before presenting the experimental implementation and results. I tried to elaborate all the key concepts including; entropic uncertainty

relations, steps of QKD in general, virtual entanglement and EPR steering and its connection to 1SDI-QKD to make our theoretical development more understandable. Further details can be found in ref[**?**]. The experimental implementation and results will be presented in the next following two chapters.

5.2 Uncertainty Relations

The uncertainty principle originally proposed by Heisenberg [4] imposes constrains on the potential knowledge one can learn about the physical properties of a system. It states that even with full knowledge of the state of a particle, it is impossible to predict the outcomes of all the measurements. This lack of knowledge first characterized by Heisenberg using standard deviation [20]:

$$\Delta X \cdot \Delta P \geq \frac{1}{2} \left| \langle [X, P] \rangle \right| \tag{5.1}$$

However, from information-theoretic aspects, it is more useful to quantify the uncertainty relations in terms of entropy. Several authors tried to derive the entropic version of uncertainty relations [21, 22, 23, 24, 25]. The improved relation is as follows [20]:

$$H(X) + H(P) \geq \log_2 \frac{1}{c} \tag{5.2}$$

where $H(X)$ stands for the Shannon entropy (see section 2.10.1) of the probability distribution of the outcomes when observable X is measured. The same applies for $H(P)$ and the outcome of the measurement of the observable P. The term $\frac{1}{c}$ shows the complementarity of the observables, with $c := \max_{i,j} |\langle x_i | p_j \rangle|^2$ where $|x_i\rangle, |p_j\rangle$ are the eigenvectors of the observable X and P respectively. Equation (5.2) quantifies the uncertainty relation where one starts without any additional information or at most only classical information describing the system in question, i.e. the density matrix [20].

However, if observers could share quantum correlation with the measured system, there would be significant reduction in the level of uncertainty. M. Berta et al derived a generalized relation, allowing for this so-called quantum side information for finite dimensional Hilbert spaces and observables [20]. They assumed that Bob entangles his quantum memory with the state he forwards to Alice. They found a bound on the uncertainties of the measurement outcomes, based on the amount of entanglement existing between the measured particle, A, and the quantum memory B, as follows [20]:

$$S(X_A|B) + S(P_A|B) \geq \log_2 \frac{1}{c} + S(A|B) \tag{5.3}$$

here $S(A|B)$ stands for the conditional von Neumann entropy of the bipartite state ρ_{AB}, and $S(X_A|B)$ is the conditional von Neumann entropy of the outcome of the

measurement of the observable X on subsystem A given the knowledge of subsystem B (see sections 2.10.7 and 2.10.8 for the description on von Neumann and conditional entropy).
Since a negative conditional entropy is a sign of entanglement [123], relation (5.3) shows the effect of entanglement in reducing the uncertainty.
One can also consider that the state ρ_{AB} could have experienced some decoherence which is purified by an environment, or eavesdropper, in a way that $\rho_{AB} = \mathrm{tr}_E(|ABE\rangle\langle ABE|)$. Considering the purity of the overall state i.e. $S(AB) = S(E)$ one can modify the relation (5.3) to find [20] :

$$S(X_A|E) + S(P_A|B) \geq \log_2 \frac{1}{c} \tag{5.4}$$

Although relation (5.4) is an elegant mechanism to bound the key that Alice and Bob can extract as shown in ref [20], it is only valid for measurement and states in finite-dimensional Hilbert space. For CV-QKD we need an uncertainty relation valid for infinite-dimensional Hilbert spaces and continuous-valued measurements. Particularly, we are interested in homodyne measurements (see section 2.8.1) of the canonically conjugate quadratures (see section 2.3).
Fortunately such a relation has been lately derived, based on the previous findings for discrete and finite measurements on infinite dimensional Hilbert spaces [124]. At first it was extended to countably infinite measurements with the possible application for a discretised version of a homodyne detection [26]. By considering the infinite precision limits of these coarse-grained POVM's, results for the continuous spectra, had previously been extensively investigated for the Shannon entropies, with an analogous procedure for the quantum conditional von Neumann entropy employing by Ferenczi [28] and Furrer et al [26]. An alternative derivation was also presented by Frank and Lieb [27]. The ultimate result is the following relation for the homodyne detection performed on the infinite dimensional Hilbert spaces [26, 27, 28],

$$S(X|E) + S(P|B) \geq \log 2\pi\hbar \tag{5.5}$$

Utilizing relation (5.5) which bounds Eve's information, we developed a key rate in infinite dimensional Hilbert space. I will describe it in detail in the following sections.

5.3 Quantum Cryptography in Continuous-Variable Regime

Since the focus of this thesis is on continuous-variable QKD, before showing how we use relation (5.5) for QKD purposes, I will briefly describe the most important families of continuous-variable QKD protocols using Gaussian states and measurements. A generic QKD protocol was previously described in section 4.2.
The most common CV-QKD protocols are the Gaussian protocols in which the information is encoded in the field quadratures (see section 2.3). In Gaussian protocols one can use either an entangled source (EB) or the equivalent picture; prepare and

measure (P&M) scheme, where Alice by using a random number generator, prepares an ensemble of signal states. In fact, one of the most significant results in CV-QKD was the discovery that the secret key can be generated by using coherent states [126]. It is easier to generate coherent states in the laboratory which opens the door for the real-life implementation of CV-QKD protocols. In this scenario Alice encodes two real variables a_q and a_p, onto a coherent state. She draws these variables from a Gaussian distribution of variance V_a and zero mean. By considering $V_a = V - 1$, Alice obtains a thermal state of variance V as an output (see section 3.7.1 and 3.7.4 for more details on the preparation of the coherent states). Alice sends the thermal state to Bob, where for each incoming state he measures either $\hat{q}$ or $\hat{p}$ quadrature by performing a homodyne detection (see section 2.8.1) . At the end, Alice has a long string of encoded data with the values (a_q, a_p) which are correlated with Bob's homodyne outcomes. After sifting, Alice keeps only the string of data compatible with Bob's quadrature measurements [89].
The previous protocol can be modified by changing the homodyne detection to the heterodyne detection (see section 2.8.2) where both quadratures are observed simultaneously. This protocol is famous as "no-switching protocol". The advantage of this protocol is that Alice can keep both real random variables, hence producing higher secret-key rates [89, 127].
Although coherent states are better candidates for CV-QKD protocols, squeezed states are also utilized especially in the early QKD protocols [93, 125, 89]. In this protocol Alice randomly chooses to squeeze and displace either $\hat{q}$ or $\hat{p}$ quadrature. When the state received by Bob, he randomly decides to perform a homodyne measurement on one quadrature. After sifting, Alice and Bob keep only the data which correspond to the same quadratures. Squeezed-state protocol can also be conducted where Bob performs heterodyne measurement on his received state [89].
In entanglement-based representation, a bipartite entangled state is distributed between Alice and Bob. Here Alice's preparation is realized by performing a suitable measurement on the entangled source. For (P&M) scheme, either squeezed [93, 125] or coherent [126] states, are respectively equivalent of performing the homodyne or heterodyne measurement on one part of the entangled state.
The communicating parties Alice and Bob, can implement either a direct reconciliation (DR) or the reverse reconciliation (RR) which make a total of 16 possible Gaussian protocols.

5.3.1 Virtual Entanglement

In (EB) scheme [47], an entangled state is shared between two communicating parties Alice and Bob, while in (P&M) approach Alice prepares a coherent (squeezed) state and forwards it to Bob. The interchangeability between these two approaches has been demonstrated in a device dependent scenario [90]. This one-to-one analogy between (P&M) and (EB) schemes is famous as "*virtual entanglement*". This effect is captured in figure 5.1 for heterodyne measurement and coherent states. It can be understood as if the EPR source and measuring apparatus of Alice shown in

figure 5.1 (a) are hidden in a black box. The only things emerging from this box are the measurement values Q_A and P_A, and Q and P which are sent to Bob. The outputs of this black box are equivalent to the outputs of the other black box depicted in figure 5.1 (b), where Q_A and P_A are chosen by the adequate random number generator. The physical implementation of (P&M) scheme is easier and cheaper, while the equivalent (EB) scheme is better to use for the mathematical calculations. We will use the equivalence between these two schemes later to prove the key rate for the (P&M) scheme.

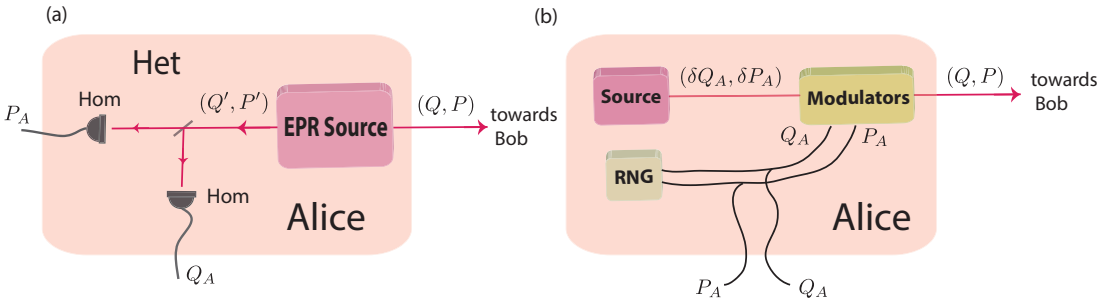


Figure 5.1: (a) showing an EB scheme where Alice measures both quadratures of her beam by performing a heterodyne (dual homodyne) measurement on her EPR arm. (b) showing the equivalent black box to (a), where a coherent state source generates the beam, which is then displaced in phase space using a modulator. The two numbers are produced by a random number generator (RNG)

In the next section, I will show how we employed the uncertainty relation (5.5) to lower bound the secret key rate, in the asymptotic regime and taking into account only the Gaussian collective attacks. Asymptotic regime is when two communicating parties exchange infinite number of data to establish a key. Besides the collective attacks are shown to be the optimal attack using de Finetti theorem adapted to infinite dimension [128].

5.4 CV-QKD using entropic uncertainty relations

I will describe here the derivation of the key rate for RR protocol. Finding the secret key for DR protocol is straightforward. As mentioned earlier, in CV-QKD the secret key can be extracted from Alice and Bob's quadrature measurements, symbolized by the random variables $X_{A(B)}$ with outcomes $x_{A(B)}$ which follow probability distributions $p(x_{A(B)})$. Here the detector and reconciliation efficiencies are neglected for simplicity. These effects will be included later. The asymptotic RR secret key rate is lower bounded by [129, 130] :

$$K^{\triangleleft} \geq I(X_B : X_A) - \chi(X_B : E) \tag{5.6}$$

where the left white triangle denotes the information flow during reconciliation from Bob to Alice. Here $I(X_B : X_A)$ denotes the classical mutual information between Alice and Bob (see section 2.10.6), with $H(X)$ being the continuous Shannon entropy of the measurement strings defined as $H(X) = -\int dx\ p_X(x) \log p_X(x)$ (see section 2.10.3), and $\chi(X_B : E) = S(E) - \int dx_B p(x_B) S(E|x_B)$ denotes the continuous Holevo bound (see section 2.10.9) with $S(X)$ being the von Neumann entropy (see section 2.10.7) and $S(A|B)$ the conditional von Neumann entropy of A given B (see section 2.10.8). In the case that systems are classical, i.e. $B = X_B$, the von Neumann entropies may be replaced by the Shannon entropy.
By substituting the classical mutual information and the Holevo bound in the relation (5.6) we have:

$$K^{\triangleleft} \geq H(X_B) - H(X_B|X_A) - S(E) + \int dx_B p(x_B) S(E|x_B) \tag{5.7}$$

Using the following definition:

$$S(X_B|E) = H(X_B) + \int dx_B p(x_B) S(\rho_E^{x_B}) - S(E) \tag{5.8}$$

where $\rho_E^{x_B}$ is the conditional state of E given measurement outcome x_B, and combining the relations (5.7) and (5.8) we have :

$$K^{\triangleleft} \geq S(X_B|E) - H(X_B|X_A) \tag{5.9}$$

Now using the entropic uncertainty relation (5.5) and changing the places of A and B, one can bound the eavesdropper's information as follows:

$$S(X_B|E) \geq \log 2\pi\hbar - S(P_B|A) \tag{5.10}$$

Considering $S(P_B|A) \leq S(P_B|P_A) = H(P_B|P_A)$, we can have:

$$S(X_B|E) \geq \log 2\pi\hbar - H(P_B|P_A) \tag{5.11}$$

By substituting relation (5.11) in (5.9) and assuming $\hbar$=2 we have:

$$K^{\triangleleft} \geq \log 4\pi - H(P_B|P_A) - H(X_B|X_A) \tag{5.12}$$

Thus by employing an expression that relies only upon the conditional Shannon entropies, we have bounded the secret key. These conditional Shannon entropies are directly available for Alice and Bob. Besides for any probability distribution $p(x)$, it can be demonstrated via a variational calculation that the analogous Shannon entropy is maximized for a Gaussian distribution of the same variance. In other words, by measuring Bob's conditional variances, Alice and Bob can bound their secret key rate for this protocol . Substituting the Shannon entropy for a Gaussian distribution $H_G(X_B|X_A) = \log \sqrt{2\pi e V_{X_B|X_A}}$, where $V_{X_B|X_A} = V_{X_B} - \frac{\langle X_A X_B \rangle^2}{V_{X_A}}$ is Bob's variance conditional on Alice's measurement, we derive the final expression for the

RR key rate as:

$$K^{\triangleleft} \geq \log(\frac{2}{e\sqrt{V_{X_B|X_A} V_{P_B|P_A}}}) \tag{5.13}$$

The DR expression is obtained by simply permuting the labels of Alice and Bob. The extension of equation (5.13) to the other Gaussian protocols is straightforward and is given in ref [122]. Due to the importance of the protocol with coherent states and homodyne measurement in this thesis, I will present its key rate calculation here.
As mentioned in section 5.3.1, a DR coherent state in EB picture involves Alice making a heterodyne detection upon her arm of an EPR pair, where she mixes her mode with the vacuum. The resulting modes are A_1 and A_2 upon which she measures $\hat{x}$ and $\hat{p}$ respectively. Bob makes a homodyne detection by switching between the quadratures. The DR key rate is then bounded by:

$$K^{\triangleright} \geq S(X_{A1}|E) - H(X_{A1}|X_B) \tag{5.14}$$

where the right white triangle denotes here the information flow during reconciliation from Alice to Bob. After Alice's projective measurement upon A_2 the state ρ_{A_1BE} is pure and we can again apply the entropic uncertainty relation :

$$K^{\triangleright} \geq \log 4\pi - S(P_{A1}|B) - H(X_{A1}|X_B) \tag{5.15}$$

$$\geq \log 4\pi - H(P_{A1}|P_B) - H(X_{A1}|X_B) \tag{5.16}$$

Although we do not measure $\hat{p}$ upon mode A_1, we trust the device in Alice's station. Therefore we can assume $H(P_{A1}|P_B) = H(P_{A2}|P_B)$ which is measured. Hence we have:

$$K^{\triangleright} \geq \log 4\pi - \log\sqrt{2\pi e V_{P_{A2}|P_B}} - \log\sqrt{2\pi e V_{X_{A1}|X_B}} \tag{5.17}$$

$$= \log(\frac{2}{e\sqrt{V_{X_{A1}|X_B} V_{P_{A2}|P_B}}}) \tag{5.18}$$

In order to compare with the previous protocol (EB scheme and homodyne detection) we use the fact that mode A is mixed with the vacuum as shown in figure 5.1. Hence we have:

$$X_{A1} = \frac{1}{\sqrt{2}}(X_A + X_v) \tag{5.19}$$

$$V_{X_{A1}} = \frac{1}{2}(V_{X_A} + 1) \tag{5.20}$$

where X_v is the vacuum fluctuation, and its variance is $V_{X_v} = 1$.
Alice's variance on Bob's measurement is as follows:

$$V_{X_{A1}|X_B} = V_{X_{A1}} - \frac{\langle X_{A_1} X_B \rangle^2}{V_{X_B}} \tag{5.21}$$

Using the expressions (5.21) and (5.20) we have :

$$V_{X_{A1}|X_B} = \frac{(V_{X_A} + 1)}{2} - \frac{\langle \frac{1}{\sqrt{2}}(X_A + X_v) X_B \rangle^2}{V_{X_B}} \tag{5.22}$$

$$= \frac{1}{2} V_{X_A} - \frac{1}{2} \frac{\langle X_A X_B \rangle^2}{V_{X_B}} \tag{5.23}$$

$$2V_{X_{A_1}|X_B} - 1 = V_{X_A|X_B} \tag{5.24}$$

A similar expression can be written for $V_{P_{A_2}}$. Hence considering the equation (5.18) the key rate will be given as follows:

$$K^{\triangleright} \geq \log\left(\frac{4}{e\sqrt{(V_{P_A|P_B} + 1)(V_{X_A|X_B} + 1)}}\right) \tag{5.25}$$

5.5 Security proof with imperfect reconciliation efficiency

In the previous section the secret key rates were derived assuming the ideal situation. In reality we won't be able to perfectly achieve this and we should take into account the effect of imperfect reconciliation between Alice and Bob. Thus the key rate will instead be bounded by:

$$K \geq \beta I(X_A : X_B) - S(X_A : E) \tag{5.26}$$

where $0 < \beta \leq 1$ is the reconciliation efficiency. In this scenario, rather than applying the entropic uncertainty relation to lower bound the secret key rate, we will employ it to upper bound the eavesdropper's (Eve's) information and then independently estimate $\beta I(X_A : X_B)$ to obtain the actual key rate. Considering that Eve's information is upper bounded by the Holevo quantity we will have:

$$S(X_A : E) \leq S(E) - \int dX_A \, p(X_A) \, S(\rho_E^{X_A}) \tag{5.27}$$

Besides the conditional von Neuman entropy of the observable X_A is given by:

$$S(X_A|E) = H(X_A) + \int dX_A p(X_A) S(\rho_E^{X_A}) - S(E) \tag{5.28}$$

Hence Eve's information can be written as:

$$S(X_A : E) \leq H(X_A) - S(X_A|E) \tag{5.29}$$

We now make use of equation (5.5), our CV entropic uncertainty relation as :

$$S(X_A|E) + S(P_A|B) \geq \log 4\pi \tag{5.30}$$

to obtain,

$$S(X_A : E) \leq H(X_A) + S(P_A|B) - \log 4\pi \tag{5.31}$$

Knowing the fact that $S(P_A|B) \leq S(P_A|P_B) = H(P_A|P_B)$ and the Gaussian distribution for a fixed variance maximizes the Shannon entropy such that $H(X_A) \leq \log \sqrt{2\pi e V_{X_A}}$ we arrive finally at:

$$S(X_A : E) \leq \log 2\pi e \sqrt{V_{X_A} V_{P_A|P_B}} - \log 4\pi \tag{5.32}$$

Thus the secret key rate for an arbitrary β is defined as:

$$K \geq \beta \log \sqrt{\frac{V_{X_A}}{V_{X_A|X_B}}} + \log 4\pi - \log 2\pi e \sqrt{V_{X_A} V_{P_A|P_B}} \tag{5.33}$$

Considering that in the real situation $\hat{x}$ and $\hat{p}$ quadratures are not symmetric, we need to average over them. Hence, the key rate in real situation becomes:

$$\begin{aligned} K \geq (\beta \log \sqrt{\frac{V_{X_A}}{V_{X_A|X_B}}} + \log 4\pi - \log 2\pi e \sqrt{V_{X_A} V_{P_A|P_B}})/2 \\ + (\beta \log \sqrt{\frac{V_{P_A}}{V_{P_A|P_B}}} + \log 4\pi - \log 2\pi e \sqrt{V_{P_A} V_{X_A|X_B}})/2 \end{aligned} \tag{5.34}$$

We used this expression in the experimental implementation of one-sided device-independent QKD protocols that I will describe in the next chapters.

5.6 One-sided device-independent CVQKD

An important benefit of employing entropic uncertainty relations which ended to equation (5.13), is that they lend themselves towards one-sided device-independent (1SDI) protocols. As mentioned in section 4.5 for 1SDI-QKD protocols only one of the communicating parties, Alice or Bob, is trusted and the other is regarded as a black box. Since the trusted partty is assumed to involve a particular set of quantum operations, the security is linked to the steering inequalities [17] associated with the observables on the trusted side. In the following I will describe EPR steering briefly, and then explain the connection between quantum steering and the possible one-sided device-independent Gaussian protocols based on equation (5.13).

5.6.1 EPR Steering

The concept of EPR steering was pioneered by Schrödinger in 1935 as a generalization of the EPR paradox. In his response to EPR paper, Schrödinger introduced *Steering* for Alice's ability to affect (steer) Bob's state by her choice of measurement. In this scenario Alice prepares a bipartite quantum state and forwards one part to Bob. Her job is to assure Bob that their state is entangled. Bob relies on quantum mechanics but does not trust her. To convince him, Alice randomly chooses a measurement base and conducts measurement on her state. Bob does tomographic measurement of his state. If Bob finds a well-defined state conditioned on Alice's announced outcomes through the entire experiment and all the measurement choices, he will be convinced that Alice can steer his state and as a result their shared state is entangled. Otherwise, he would conclude that Alice has drawn a pure state at random from some ensemble, where the correlation between Bob's measurement result and Alice's announced results can be described utilizing a local hidden state (LHS) model for Bob [17]. An operational definition for EPR steering is provided by H.M.Wiseman et al. [17] where they proved that the states that exhibit Bell-type correlations are a subset of EPR steerable states, and steerable states are a strict subset of entangled states .
Due to the asymmetry between the parties, it is easier to show EPR steering experimentally than violating a Bell's inequality [131]. Since in EPR steering, instead of considering correlation functions for measurement outcomes for two parties in Bell's inequality, the correlation is considered between measurement outcomes announced by Alice and Bob's measurement results conditioned on Alice's outcome [131]. For example, for the simplest case of the Gaussian states where Alice and Bob each have one mode with correlated positions X and momenta P, the EPR steering is demonstrated through violation of Ried [47] EPR criteria [17], which says that the product of the conditional variances $V_{X_B|X_A}$ and $V_{P_B|P_A}$ should violate the uncertainty principle for Alice to steer Bob's state as follows :

$$\mathcal{E}_{\triangleright} = V_{X_B|X_A} V_{P_B|P_A} \leq 1 \tag{5.35}$$

It also shows that "EPR Paradox" is a special case of steering. The steering task when Alice is affecting Bob's state is shown schematically in figure 5.2.
This asymmetric correlation of EPR steering makes one-sided device-independent QKD possible. In the following I will discuss Gaussian protocols for 1SDI-QKD and their connection to the EPR steering.

5.6.2 One-sided device-independent CV-QKD protocols and their connection to EPR steering

Here I will discuss which of the 16 Gaussian protocols mentioned in section 5.3 can possibly show one sided-device independence. Similar to steering inequalities, the 1SDI nature of the entropic proofs is clear in expressions like equation (5.13) in that it relies only on measuring a known observable upon one side. For example, in the derivation we only need to know that Bob is observing either $\hat{x}_B$ or $\hat{p}_B$ and then

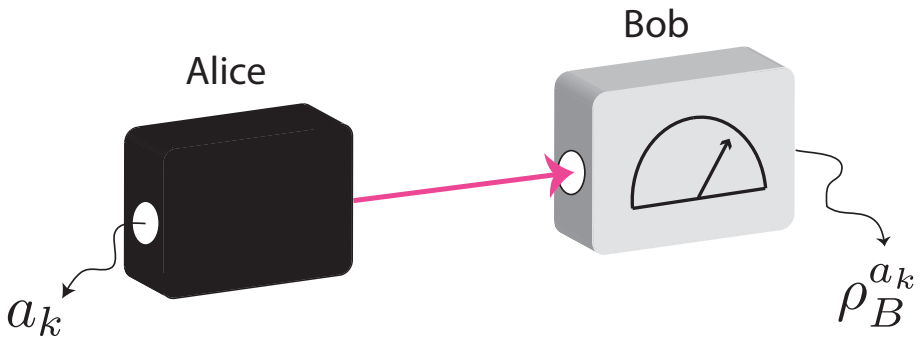


Figure 5.2: Schematic diagram of steering task when Alice is affecting Bob's state. Bob trusts his devices which is shown by the white box, but he has no knowledge about Alice's devices which is depicted by a black box. Only the outcomes of Alice's measurement a_k are important to Bob. By performing the complete measurement on his received state and conditioning on Alice's announced outcomes, Bob will be convinced that Alice has the ability to steer his state if he finds a well defined state conditioned on Alice's outcomes

conditioned on the outcomes of Alice's observation in order to use the entropic uncertainty relations. Alice could choose any measurement and the security would still hold if the conditional variance was sufficiently small to violate Ried EPR criteria (equation 5.35).
Hence for entanglement-base (EB) scheme and homodyne detection, by definition any positive key proved by the entropic uncertainty relation is 1SDI, independent of Alice for RR and Bob for DR protocols. Though the protocols involving heterodyne detection does not necessarily exhibit device independence. This is basically due to the fact that extracting the non-zero key rates for the heterodyne protocols depends upon characterizing the devices utilized in the heterodyne detection. Hence, using a heterodyne measurement by the supposedly untrusted party immediately disproves the device-independence. However, the heterodyne measurement can be performed safely by the trusted party with high efficiency sources and detection, making the implementation of 1SDI-CVQKD protocols possible with current technology. It means that Bob can safely perform heterodyne for an RR protocol and Alice may conduct heterodyne for a DR protocol. Finally, for DR protocols where Alice who is trusted and controls the source, we can also benefit from the equivalence between prepare and measure (P&M) and entanglement-based (EB) schemes (see section 5.3.1). Surprisingly, this means that for direct reconciliation it is possible to extract 1SDI key utilizing only coherent states. The table in figure 5.3 summarizes the possible Gaussian protocols which are potentially 1SDI out of the all 16 Gaussian protocols .

The idea that the 1SDI-QKD protocols should be related to EPR steering was confirmed in DV regime by C.Branciard et al. [19] before. For CV-QKD the EPR-steering criteria is defined by equation 5.35. Comparing Ried EPR criteria with

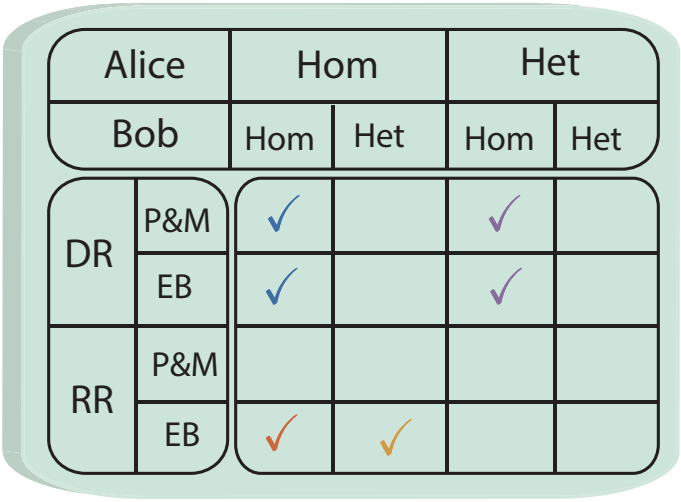
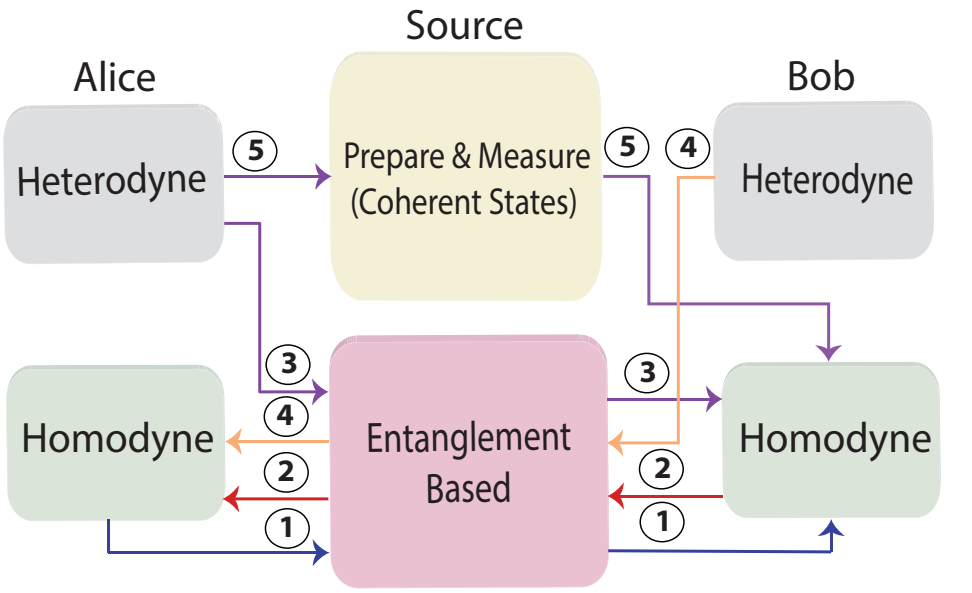


Figure 5.3: Gaussian protocols which can potentially be 1SDI. Alice and Bob can choose either homodyne or heterodyne detection. DR and RR reconciliation protocols can be performed for both (EB) and (P&M) schemes. The same colors are chosen to show the equivalence between the (EB) and (P&M) protocols.

equation (5.13) we can rewrite the key rate as a function of EPR-steering $\mathcal{E}_{\triangleright}$:

$$K^{\triangleleft} \geq \log(\frac{2}{e\sqrt{\mathcal{E}_{\triangleright}}}) \tag{5.36}$$

For the RR protocols the key rate $K^{\triangleleft} > 0$ if and only if $\mathcal{E}_{\triangleright} < (\frac{2}{e})^2 \approx 0.55$, with the similar relation between the DR key rate and $\mathcal{E}_{\triangleleft}$ following straightforwardly. In other words, the condition for obtaining the positive one-sided device-independent key is more strict than EPR steering, analogous to the case for DV-QKD [19]. For the protocols where a trusted party performs the heterodyne detection, the security of the protocol is instead based on the steerability of the outcome of the heterodyne measurement which will be more challenging due to the extra loss introduce to the system. Now secure key enforces an EPR condition $\mathcal{E}_{\triangleright(\triangleleft)} < 0.22$. In the next chapters where I present the experimental results, I will demonstrate the connection of achieving the positive key rates and the EPR steering criteria mentioned here.
From the 6 possible 1SDI Gaussian protocols, we conducted 5 protocols experimentally. However, only 3 of the 5 demonstrated sufficient correlations to allow 1SDI key distribution. Two different experimental setups were used, the first for the (EB) protocols based on EPR correlations and the second for a coherent state (P&M) protocols. A schematic diagram of all the performed experiments and the achieved results are summarized in figure 5.4.



		Alice		Bob					
		Hom	Het	Hom	Het	RR	DR	Positive key	Transmission distance in fibre optics (km)
Entanglement-based	1	✓		✓			✓	✓	≈ 2.52
	2	✓		✓		✓		✓	≈7.57
	3		✓	✓			✓	×	0
	4	✓			✓	✓		×	0
P&M	5		✓	✓			✓	✓	≈ 3.47

Figure 5.4: Schematic diagram of all the experimentally realised 1sDI protocols. Alice and Bob can choose between homodyne and heterodyne measurements (indicated respectively by green and grey color boxes on each side), using a source that generates either EPR or coherent states (indicated respectively by pink and yellow boxes). Direct (reverse) reconciliation protocols are demonstrated using right (left) pointing arrows. The table summarizes each performed protocol and the experimentally achieved results. The same color scheme as figure 5.3 is used here to show the different performed protocols.

5.7 Summary

In this chapter I reviewed the entropic uncertainty relations and showed how we used them to derive 1SDI-QKD key rates. I discussed the connection between EPR steering and 1SDI-QKD protocols. I looked at all the 16 Gaussian QKD protocols and showed that only 6 of them can manifest device independence. We experimentally implemented 5 of these 6 protocols. In fact, Implementation of 1SDI-QKD using continuous variables against coherent attacks has been reported recently by T. Gehring et al. in ref [132]. However, they just implemented one protocol, while we extended the notion of 1SDI-QKD to the whole family of continuous variable protocols for the first time. In the next two chapters I will detail our experimental setups, the computer simulation and the results.

Chapter 6

Experimental Implementation of 1SDI-QKD Protocols in EB Scheme

6.1 Introduction

In this chapter I will describe the experimental implementation of one-sided device-independent protocols using an entangled source. I will start by giving the overall view of our experimental setup, then I will explain each part in more detail. I will introduce the detection, data acquisition and control systems that we utilized in the experiment, and present the experimental results, error estimation and computer simulation at the end.

6.2 Experimental Setup

We performed three 1SDI-QKD experiments using an entangled source. The general form of the experimental setup is shown in Fig 6.1 and the different parts of the setup will be described in the following sections. In all these three experiments the entangled state was distributed between two parties, Alice and Bob, where one part of the entangled state was sent to Alice locally and the other part to Bob through a lossy channel. In the first experiment both Alice and Bob performed homodyne measurement on their states alternating between two quadratures. Where in the second experiment Alice heterodyned, measuring both quadratures at the same time, while Bob conducted a homodyne detection on his received state. The third experiment was the reverse scenario where Alice homodyned and Bob performed heterodyne detection on his state. These three experiments are depicted schematically in Fig 6.2. All the synchronizations were local in these experiments and no finite size effects are taken into account.
We utilized a 1064nm laser source which is frequency doubled to 532nm. This laser source was the same as described in subsections 3.7.2 . Considering that the squeezing and entanglement experiments are very sensitive to the spectral noise and spatial mode-mismatching, it is important to prepare a quantum-noise limited optical field with well-defined spatial mode (TEM-00 in our experiment). Hence both the 1064nm (seed) and 532nm (pump) beams were passed through the mode cleaning cavities

(MCCs) as shown in Fig 6.1. The mode-cleaning cavities were the same as described in subsection 3.7.3. The two OPAs which were used to produce squeezed light and entanglement will be detailed in sections 6.3 and 6.4. The estimated values of squeezing and anti-squeezing generated from both OPAs were respectively -6 dB and 10.7 dB at 3 MHz. A simple model was used to infer the pure squeezing produced inside the cavity and also the effective loss of the system. According to this model, the OPAs were assumed to produce pure squeezed states and the effective loss which considered as the combination of the cavities's escape efficiencies EFs, propagation and detectors' losses, was modelled with a beam splitter after the squeezer. This model is shown schematically in figure 6.7. The control and data acquisition systems which were used in these experiments will be described in section 6.5.

6.3 Optical Parametric Amplifier

We used optical parametric amplifiers (OPA) to produce squeezed light. A detailed schematic of our OPA is depicted in Fig 6.3. Both OPAs that we used were designed and built by Jiri Janousek [49]. These OPAs are based on a periodically poled KTP (PPKTP) crystal as a nonlinear material. KTP or Potassium titanyl phosphate is a nonlinear optical material which is commonly used for three wave mixing applications like frequency doubling or optical parametric down conversion. The crystal is housed in a bow-tie cavity resonant for the seed frequency to enhance the nonlinear interaction. PPKTP material has the advantage of high nonlinearity plus a large temperature bandwidth. This will guarantee that the phase-matching condition will not significantly change if the crystal heats up due to the absorption of the pump filed. Our crystals were fabricated by *Raicol* with identical dimensions of $10 \times 5 \times 1\,\mathrm{mm}^3$ and poling periods of $\Lambda_p = 9\,\mu m$. The surfaces of both crystals are anti-reflection coated at both the fundamental and SH wavelengths. In order to temperature stabilize the crystals, each of them was placed in a copper oven where the temperature was controlled with 0.1^{o}c precision using a Peltier element.
Both OPA cavities are formed of four mirrors in bow tie geometry, having an optical round trip path length of 275 mm with cavity linewidth of 19 MHz and finesse of 57. The two concave mirrors of each cavity (m_3,m_4) have the radii of curvature of 38 mm, spacing 44 mm apart. These two mirrors are highly reflective at the fundamental wavelength and have 95% transmission for the SH field. The other two mirrors are plane (m_1,m_2), from which one is the input coupler of transmission 99.9% and the other is the output coupler of transmission of 90% at 1064 nm. The resulting beam waist is 19 μm centered between the two curved mirrors. This waist is almost optimum for the Boyd-Kleinman condition. This condition places a constraint on the optimum focusing of the beams into the nonlinear crystal [133].

6.3.1 Locking loops of the OPAs

In order to operate each squeezer, two feed-back control loops were used. The first one controlled the cavity length, keeping it on resonance with 1064 nm seed field, and

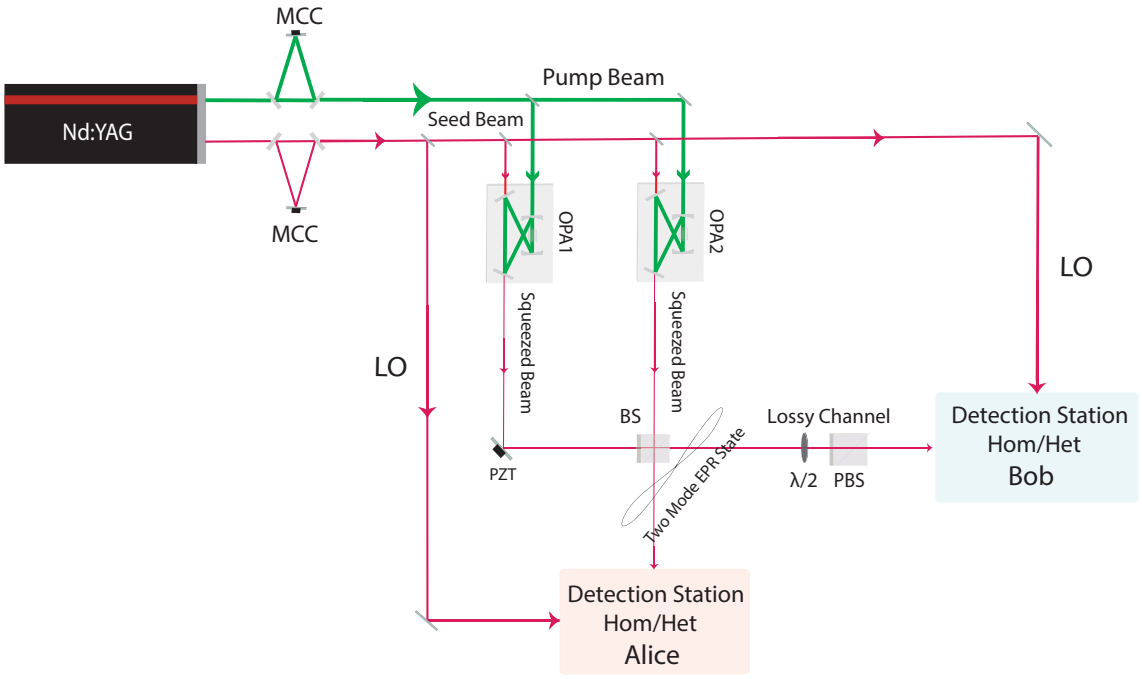


Figure 6.1: Schematic diagram of the experimental setup with entangled source. A 1064nm Nd:YAG laser which is frequency doubled to 532 was used as the source. MCC is the mode cleaning cavity which was used to provide a quantum-noise limited optical field with well-defined spatial mode. Both 1064nm and 532nm beams were passed though a mode-cleaning cavity. OPA1 and OPA2 are two similar optical parametric amplifiers which produced amplitude-squeezed beams. The 1064nm optical field coming from the Nd:YAG laser was used to seed the OPAs and the 532nm optical field to pump them. Both OPAs generated - 6.5 dB of squeezing and 10.7 dB of anti-squeezing. LO is the local oscillator. This was the bright 1064nm optical field, separated from the 1064nm laser beam and sent to Alice and Bob's detection stations. PZT is a piezo-electric actuator and BS is a 50:50 beamsplitter. Two amplitude squeezed beams were mixed on a beamsplitter with their relative phase locked in quadrature to produce an EPR state. One part of the entangled state is sent to Alice locally and the other through a lossy channel to Bob. A half wave plate $(\lambda/2)$ and a polarizing beamsplitter (PBS) were used to simulate the lossy channel. Depending on the QKD protocol, Alice and Bob perform a Homodyne (Hom) or Heterodyne (Het) measurements on their subsystem.

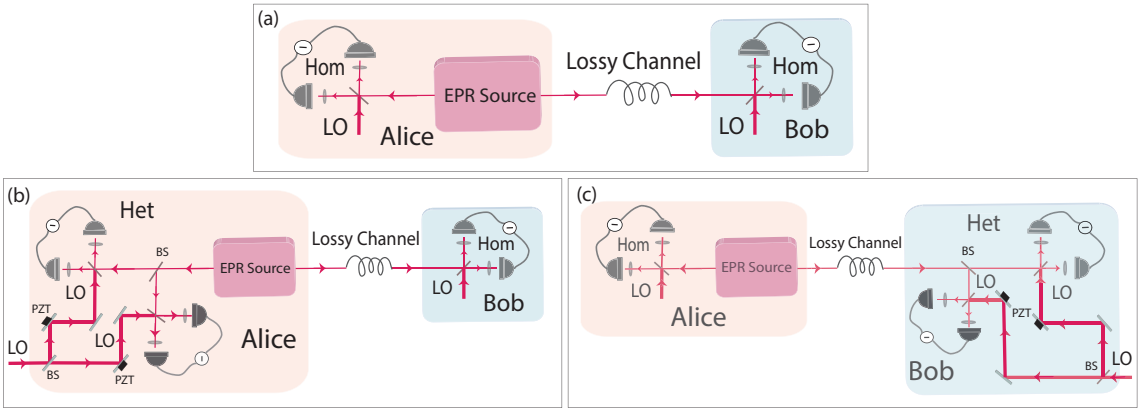


Figure 6.2: Schematic diagram of the three experimental setups using an entangled source and different measurement configurations chosen by Alice and Bob. In all these experiments one part of the entangled state is sent to Alice locally and the other through a lossy channel to Bob. Here EPR source refers to the setup shown in Fig 6.1 including two OPAs and a beamsplitter which produce a two-mode EPR state. Lossy channel as shown in Fig 6.1 consists of a half wave plate $\lambda/2$ and a polarizing beamsplirre. "Hom" refers to alternating homodyne measurements, and "Het" to a heterodyne (dual-Homodyne) measurement. "LO" is the local oscillator. As shown in Fig 6.1, it is separated from the 1064nm optical field coming from the laser. In order to provide the local oscillator for the Heterodyne (dual-homodyne) measurement, the LO coming to the detection station is again divided to two. By using two piezo-electric actuators (PZTs) and separate locking loops (see section 6.5), two homodynes in the dual-homodyne configuration were locked to different quadratures. The measurements configurations for Alice and Bob are (a) Homodyne (Alice) - Homodyne (Bob), (b) Heterodyne (Alice) - Homodyne (Bob) and (c) Homodyne (Alice) - Heterodyne (Bob).

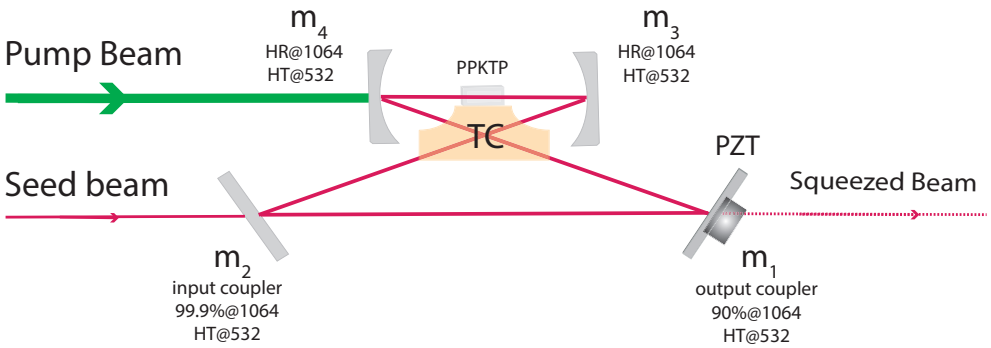


Figure 6.3: Schematic diagram of the optical parametric amplifier bow-tie cavity. Here PPKTP is periodically poled KTP nonlinear crystal, PZT is piezo-electric actuator, TC is temperature controller, HR is highly reflective mirror and ROC is the radius of curvature.

the second loop controlled the phase relation between the seed and pump field. This phase relation is very important since it defines the direction of the nonlinear process, resulting either amplification or deamplification. In order to generate amplitude squeezed light, we operate the OPA in the deamplification regime. Phase drifting will degrade the squeezing in the desired quadrature.
In order to use PDH locking technique, the seed beams of OPA1 and OPA2 were modulated at 7.1 MHz and at 16 MHz respectively, using electro-optic modulator (EOM). Each seed beam was coupled to a bow-tie cavity. The error signal for each squeezer was extracted from the reflection of the seed beam from the cavity detected by a photo-detector. This error signal was split into two. The first part was used in a PDH configuration to keep the cavity length on resonance with the seed beam. In order to use the second part in locking the phase of the pump field, a 90^{o} electronic phase shift was applied to it. This phase shift decoupled the two error signals from each other. In the experiment we maximized each error signal independently, and ensured that when looking at one error signal the other one was not interfering. After passing the second error signal through a PDH locking loop, it was fed to the piezo-electric crystal which scanned the pump beam. This feed-back loop enabled us to control the relative phase of the pump and seed beams and lock the non-linear process to de-amplification.

6.3.2 Alignment of the OPAs

Our squeezers were doubly passed (resonant) for the seed fields and single passed for the pump fields. Hence, the cavity could be aligned for the seed beam by simply scanning the length of the cavity and looking at the cavity resonances. However, aligning the pump beam was more tricky. In order to align the pump field, a bright reverse-propagating seed field was sent to the OPA cavity. This produced SHG field which could be aligned all the way back to the mode cleaning cavity, guaranteeing

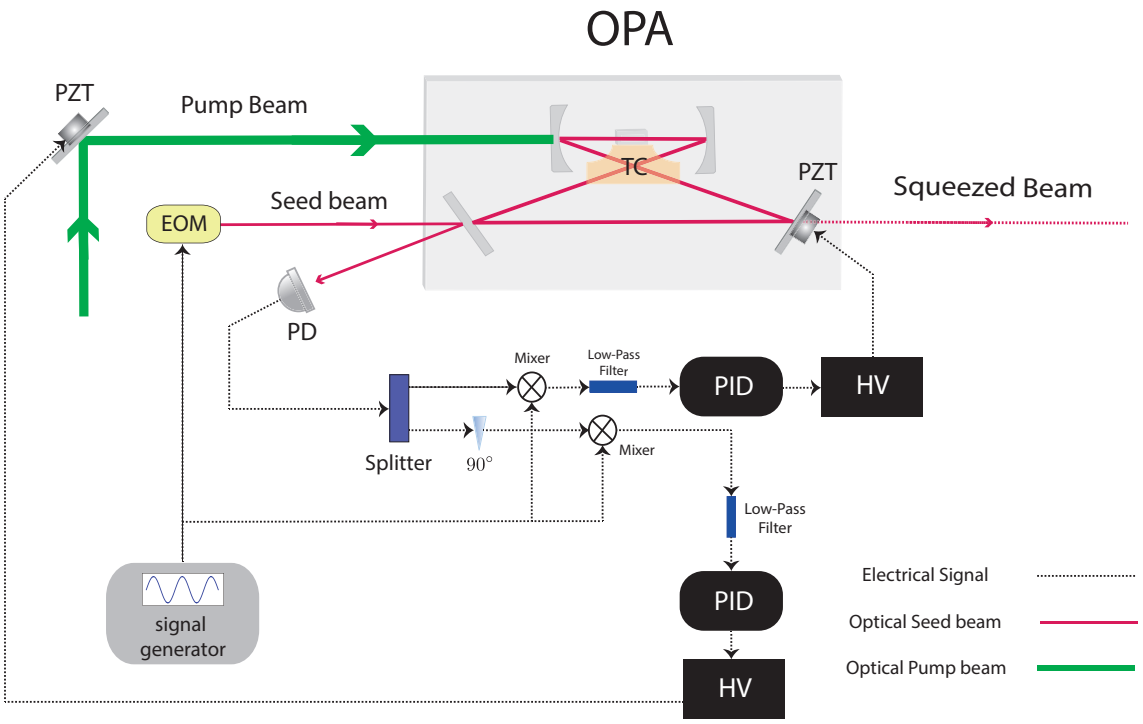


Figure 6.4: Schematic diagram of the Optical Parametric Amplifier and the feed back control loops. The reflection from the cavity was detected by a photodiode and the high frequency signal was split into two. The first part was used in a PDH configuration to keep the cavity length on resonance. An electronic phase delay of 90º was applied to the second part and was used to control the relative phase of the pump beam and seed beam utilizing the PDH locking technique. Here 90º represents the phase delay, other symbols are the same as figure 3.1 and 6.3.

that the mode coming from the green MC cavity is coupled optimally to the OPA.

6.3.3 Characterization of the OPAs

Our both squeezers are type I OPA, which means that both photons generated in the down conversion process are in the same polarisation. We operated both squeezers below the threshold of the optical parametric oscillator (OPO), and in the de-amplification regime. In this regime the quantum fluctuations in the amplitude quadrature are de-amplified leading to the amplitude squeezing [49].
In order to characterize both OPAs, squeezing noise variances are measured as a function of the pump power using a spectrum analyzer. These graphs are shown in figure 6.5. The temperature was kept at 30°C. However, it was seen that changing the temperature from 30°C to 35°C would not disturb significantly the mode matching condition. This is not surprising due to the large temperature bandwidth of the PPKTP crystal.
We used these graphs to find a regime where both OPAs function identically.

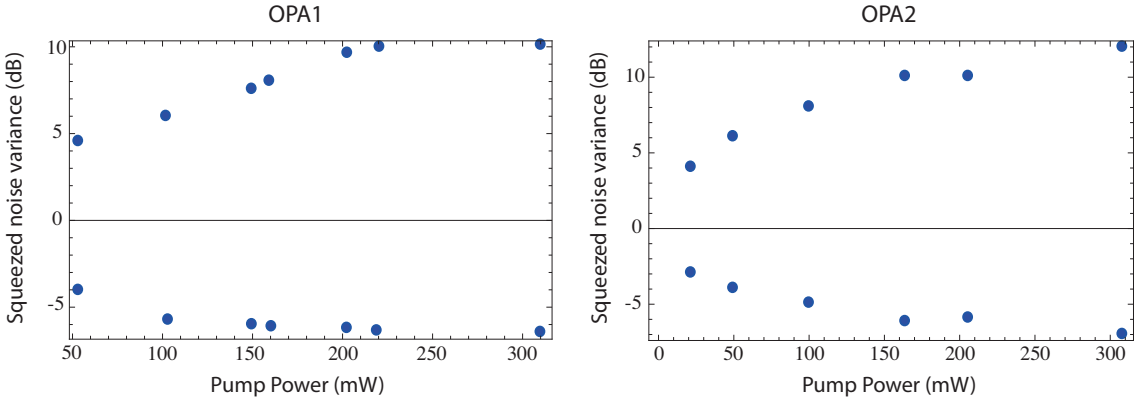


Figure 6.5: Squeezing and anti-squeezing values of OPA1 and OPA2 measured at 3 MHz, as a function of the pump power. These graphs were used to characterize the OPAs.

6.4 Entanglement Generation

The purpose of generating squeezed states, was to produce an entanglement for the 1SDI-QKD experiment. An Einstein-Podolsky-Rosen (EPR) state can be generated via quadrature phase measurement performed on the two output beams of a non-degenerate parametric amplifier [47]. In our experiment in order to produce an EPR state, we generated two amplitude squeezed states and interfered them on a 50:50 non-polarizing beam-splitter (NPBS), while controlling their relative phase to be $\pi/2$. It is shown schematically in Fig 6.6.

To control the relative phase between the two squeezed fields, we used DC locking technique. In this method, 1% of each output of the mixing beam-splitter is tapped off utilizing a pellicle AR coated for 1064 nm. The two resulting photocurrents are then subtracted producing a sinusoidal signal. The zero-crossing of this signal corresponds to $\pi/2$ relative phase between the two fields.

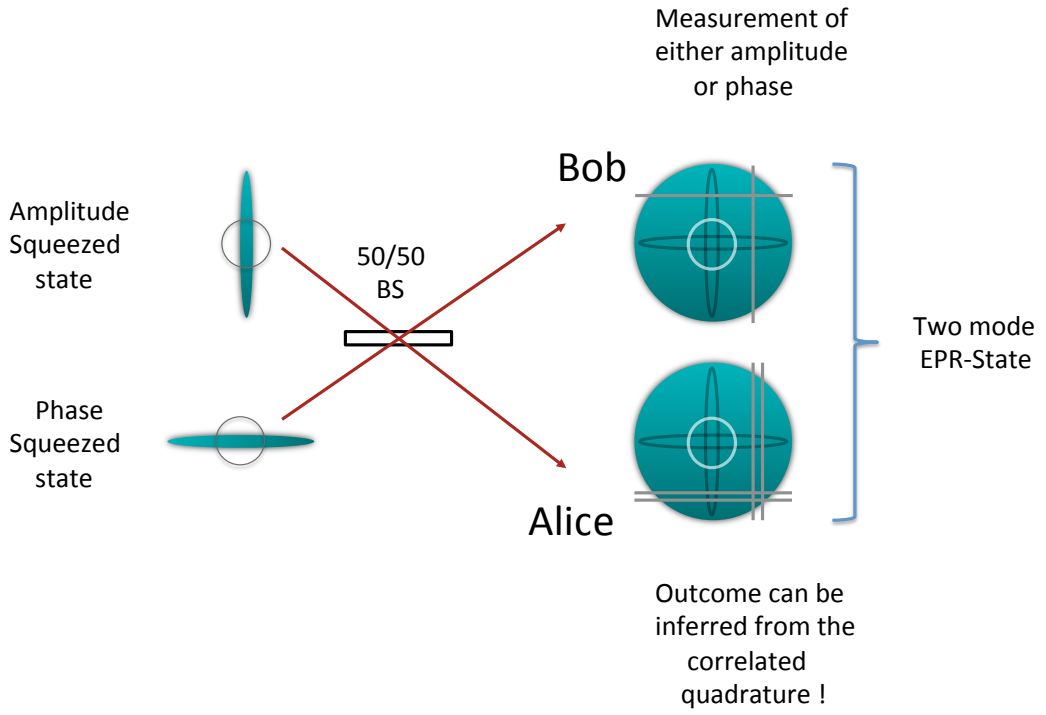


Figure 6.6: Generation of two mode EPR state by interfering an amplitude squeezed state and a phase squeezed state, or two amplitude (phase) squeezed states which are locked in quadrature.

Here $\hat{X}_s^{\pm}$ are the quadrature operators, $\hat{X}_m^{\pm}$ are the measured quadratures, and η_{eff} is the effective loss. Hence the squeezed noise variances can be found using the relation :

$$V_m^{\pm} = \eta_{eff}\, V_s^{\pm} + (1 - \eta_{eff}) \tag{6.1}$$

where $V_s =< X_s^2 >$ and $V_m =< X_m^2 >$. Since we assumed in the model that the squeezed states are pure, we have $V_s^+ = \frac{1}{V_s^-}$. Using this model and the measured values of the squeezing and anti-squeezing, I predicted that each OPA produced 11.5 dB of pure squeezing (-11.5 dB of squeezing and 11.5 dB of anti-squeezing), and the

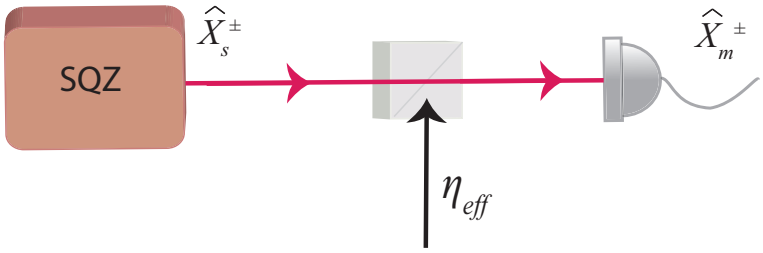


Figure 6.7: Schematic diagram of the model used to predict the pure squeezing produced by the OPA and the effective loss of the system.

effective loss of this system was calculated to be around 20% with 14% loss due to the EFs of each squeezer's cavity and also the propagation of the optical beams through the optical components and nearly 6% loss due to each detection station.

Four identical photo-detectors using Uni-PD circuits with a combination of *Epitax ETX-500* photodiodes were used in the detection stations. The detection efficiency of Alice and Bob's stations were estimated to be 94% and 92% respectively, with fringe visibility of 99% and the photodiodes' quantum efficiency of around 96% for all the detectors. We estimated 2% extra loss on Bob's side due to the loss introduced by the half wave plate and polarizing beamsplitter that were used to simulate the lossy channel. Each pair of detectors were balanced electronically, providing 30 dB of common mode rejection. Each detector had at least 16 dB of dark noise clearance.

6.5 Control System and Data Acquisition

As mentioned before and illustrated in Fig 5.4, the EB scheme consisted of four protocols and three experiments. We controlled the first experiment where both Alice and Bob performed homodyne measurement with nine locking loops; two to control the length of the 1064 nm and 532 nm mode-cleaning cavities, two to control the length of the OPAs' cavities and two to control the phase of the pump and seed fields, one to control the relative phase between the two squeezed beams and two to control the measured quadrature of homodyne detections. The first six feed-back loops were controlled by extracting error signals using analog demodulation and analog PI (Proportional-Integrator) servo controllers built in house, as shown previously in figures 3.1 and 6.4.

The error signals for homodyne detections were generated by exploiting the 7.1 MHz and 16 MHz phase modulations imposed previously on seed beams of the OPAs (see subsection 6.3.1). Since the two squeezed beams are mixed on a beam-splitter and locked in quadrature, the modulations appeared on both quadratures. This enabled us to extract two error signals to lock the homodynes to any desired quadrature. This is analogues to the locking technique, where both quadratures are modulated separately. We employed this technique in the prepare & measure experiment for locking the homodyne as will be described in section 7.3. Although all the error signals were

extracted using analog demodulation, we used digital PID controller developed by S. Armstrong [134] to lock the homodynes and the relative phase between the two squeezed beams. I will describe digital locking more in section 7.3.
The experiments involving the heterodyne (dual homodyne) detection, have the same locking loops. Except we needed one extra control loop to lock the heterodyne.

For each separate homodyne detection 5×10^7 data points are sampled at 14×10^6 samples per second using digital data acquisition system. In order to provide sufficient statistics for each data point, this process is repeated ten times. These data were then digitally filtered to 2.5-3.5 MHz and then resampled. After this process, the number of data points was reduced to 4×10^6 which is sufficient to extract the key rates.

6.6 Experimental Results

I used the relation 5.34 to calculate the key rate from the obtained experimental data. Considering that the reconciliation efficiencies for CV-QKD have increased a lot in the recent years [135, 10], with reported efficiencies of between 94% and 95.5% [132], we assumed the reconciliation efficiency to be $\beta = 0.95$ for all the experiments. This would make the comparison between different protocols possible.
Among all the implemented experiments using an entangled source, only the protocols where both Alice and Bob performed homodyne measurement succeeded. The reason that the heterodyne protocols failed to produce any positive key rates, was the strong correlations required to overcome the quantum noise penalty. Our calculation showed that a perfect system with no losses of any kind and reconciliation efficiency of 0.95 would still require at least 7 dB of pure squeezing to get any positive key.
The measured secret key rates as a function of the applied loss in dB scale for the EB experiment with homodyne-homodyne measurement is shown in Fig 6.8. Solid lines are calculated from a theoretical model based upon the characterisation of various imperfections in the experiment (see section 6.7). Using the RR protocol we measured a positive key rate independent of Alice's devices up to the applied loss of nearly 1.5 dB. And using the DR protocol, we measured a secret key independent of Bob's devices up to the applied loss of nearly 0.5 dB. Our theoretical model, which is in good agreement with the experimental data, predicts a maximum applied loss of 1.6 dB and 0.6 dB for the RR and DR protocols respectively (see section6.7). I also display the behavior of the measured steering parameter with respect to the thresholds required for key generation and violation of the Reid EPR-steering criteria (see Fig.6.8 (b)). For each data point, I graphically represent the relevant steering parameter with respect to these thresholds in Fig 6.8 (c). In accordance with our earlier discussion we show that a positive key is achieved with an RR protocol only when $\mathcal{E}_{\triangleright} < \frac{2}{e}^2 \approx 0.55$, while the corresponding relationship holds between the DR protocol and $\mathcal{E}_{\triangleleft}$. Hence, all the plotted points with positive key rate demonstrate EPR-steering through a violation of the Reid criteria. The error estimation is the same as will be described later by equation 7.4 in section 7.5.

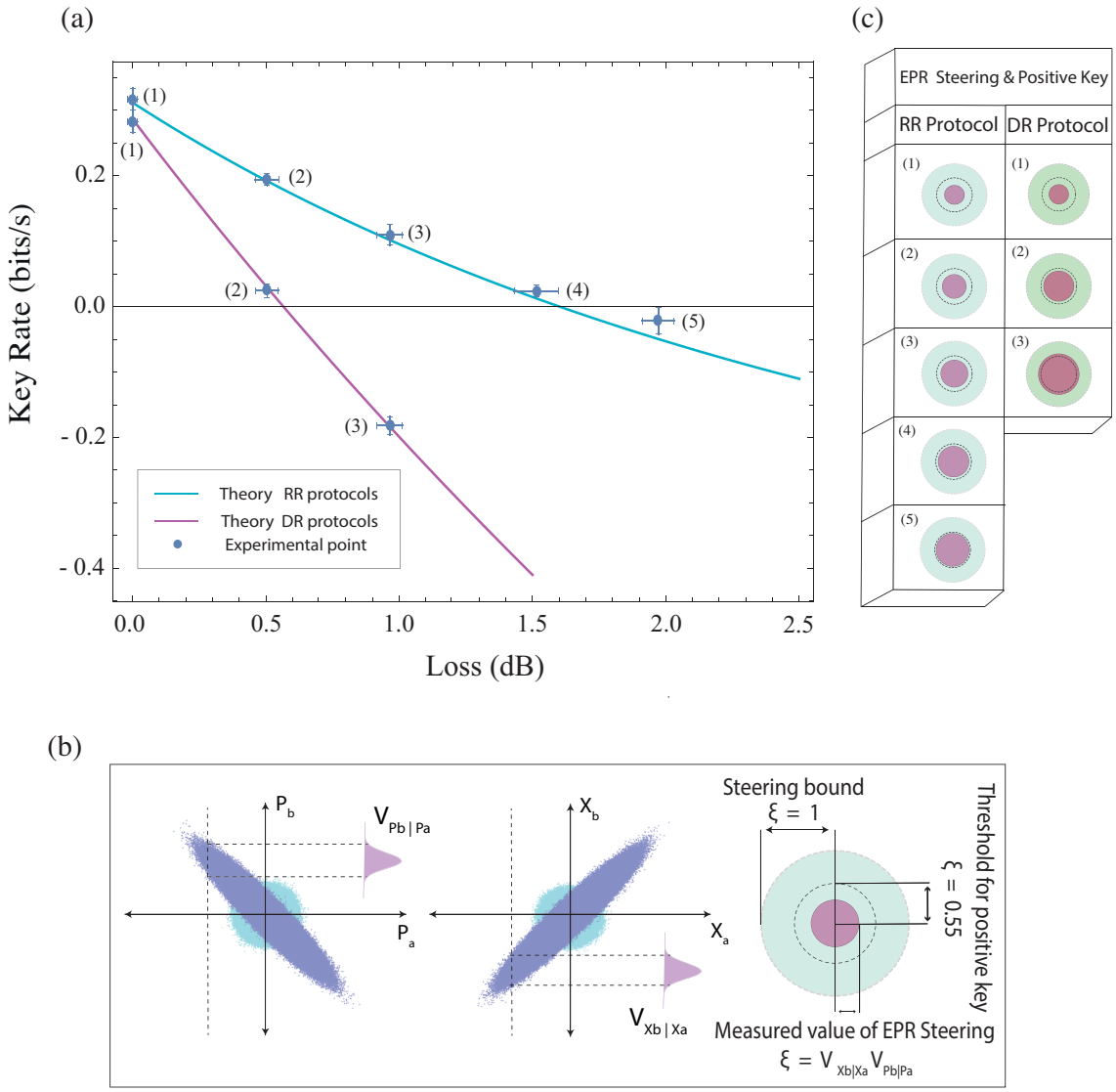


Figure 6.8: Key rates versus the applied loss in dB scale for (a) DR and RR protocols with EB source and homodyne-homodyne detections (protocols 1, 2 and 5 in the Table of Fig.5.4). Theoretical curves are evaluated from the models described in section 6.7. Experimental error bars are estimated using error propagation of uncertainties. (b) Example experimental data points from the EB protocol. Phase-space plots show the correlation between the quadratures, P_A and P_B and X_A and X_B, measured by Alice and Bob. Using their statistics, the conditional variances are calculated and used to estimate the EPR-steering parameters. The circle on the right illustrates the comparison of the measured value of the EPR steering (purple), the threshold for obtaining a positive key rate (dashed) and the upper bound for EPR steerability (green). Panels (c) illustrates circles corresponding to each plotted data point in (a), showing the connection between the measured values of EPR steering and the generation of the positive key rates. Numbers are assigned to each data point in (a) to connect them to the circles in (c).

6.7 Computer Modeling

Since all the states and operators were assumed to be Gaussian in this experiment, the states can be easily described by their mean values and covariance matrices CM's, see section 2.6. The effect of Gaussian operations on Gaussian states can be compactly calculated via symplectic transformations as described in subsection 2.6.1. Under an arbitrary symplectic operation, S, an input CM, σ_{in} transforms via

$$\sigma_{\text{out}} = S\,\sigma_{\text{in}} S^T. \tag{6.2}$$

The CM of a two-mode squeezed vacuum with squeezing in quadrature in modes i and j is given by applying the following symplectic operator,

$$SQ_{i,j}(s_1, s_2) = \begin{pmatrix} e^{s_1} & 0 & 0 & 0 \\ 0 & e^{-s_1} & 0 & 0 \\ 0 & 0 & e^{-s_2} & 0 \\ 0 & 0 & 0 & e^{s_2} \end{pmatrix} \tag{6.3}$$

where s_1 and s_2 are squeezing parameters applied on the i^{th} and j^{th} second mode respectively. Implicit in this notation is the fact that when applied to a multi-mode CM one should appropriately pad out the above matrix such that the identity is applied to all modes other than i and j.

The loss of each squeezer is modelled by introducing a vacuum mode, and then applying a beamsplitter of transmittance $\eta_{A(B)}$ on each squeezed mode and a vacuum mode to mix them together. The beamsplitter transformation between the modes i and j is:

$$BS_{i,j}(\eta) = \begin{pmatrix} \sqrt{\eta} & 0 & -\sqrt{1-\eta} & 0 \\ 0 & \sqrt{\eta} & 0 & -\sqrt{1-\eta} \\ \sqrt{1-\eta} & 0 & \sqrt{\eta} & 0 \\ 0 & \sqrt{1-\eta} & 0 & \sqrt{\eta} \end{pmatrix} \tag{6.4}$$

In order to create an EPR state two squeezed states are locked in quadrature and mixed on a 50:50 beamsplitter. To model the imperfect locking point a phase shift θ is applied to one mode before they mix on a beamsplitter. The applied operator is as follows:

$$RT(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \tag{6.5}$$

To model the loss of the transmission channel, a vacuum state was introduced and mixed with the second mode on a beamsplitter with transmittance T. The loss of

each homodyne station was modelled by a beamsplitter of transmittance $\eta_{D_{A(B)}}$, equal to the efficiency of the homodyne station, with the other mode being in a thermal state of variance $V_{\Delta_{A(B)}} = 1 + \Delta_{A(B)}/(1 - \eta_{D_{A(B)}})$ to model the detector dark noise of magnitude $\Delta_{A(B)}$. Thus the final CM is given by (6.2) where

$$\begin{aligned} S =& BS_{2,7}(\eta_{D_B})BS_{2,6}(T)BS_{1,5}(\eta_{D_A})BS_{1,2}(1/2)RT_2(\theta) \\ & BS_{2,4}(\eta_B)BS_{1,3}(\eta_A)SQ_{1,2}(s_1, s_2) \end{aligned}$$

with

$$\sigma_{\text{in}} = \text{diag}(1, 1, 1, 1, 1, 1, 1, 1, V_{\Delta_A}, V_{\Delta_A}, 1, 1, V_{\Delta_B}, V_{\Delta_B}) \tag{6.6}$$

a 14x14 diagonal matrix. The whole process is shown schematically in Fig 6.9.

To determine the value of the applied loss, T, from the measured correlations it is sufficient to consider the ratio of the correlation between Alice and Bob at particular loss setting with the case where the channel is set to full transmission. From the simulated covariance matrix, key rates were calculated and plotted as a function of the effective transmission distance. Using the measured parameters in our model resulted in a good agreement with the experimental results as shown in Fig 6.8 (a).

The model was also used to estimate the performance of a more efficient system with two squeezers each producing -10 dB of squeezing and 16 dB of anti-squeezing and detection efficiency for Alice and Bob's stations of 96% and 95% respectively. Using these parameters, our model shows the improvement of the secure communication, where the tolerable applied loss to the system would extend from 1.6 dB to 3.3 dB for the RR protocol and from less than 0.6 dB to nearly 1.4 dB for DR protocol (see Fig 6.10). Achieving this level of quadrature squeezing is experimentally challenging but feasible as up to -12 dB of squeezing was reported previously [136].

6.8 Summary

In this chapter I described the experimental setup that we used to implement the 1SDI-QKD protocols using entangled source. I presented the overall view of our setup then detailed the optical parametric amplifiers that we used to generate amplitude squeezed light and EPR state. I showed how I estimated the loss of the squeezers and described our control system and data acquisition. I presented our experimental results and detailed the computer modelling I conducted to understand the setup better and the way to improve it.

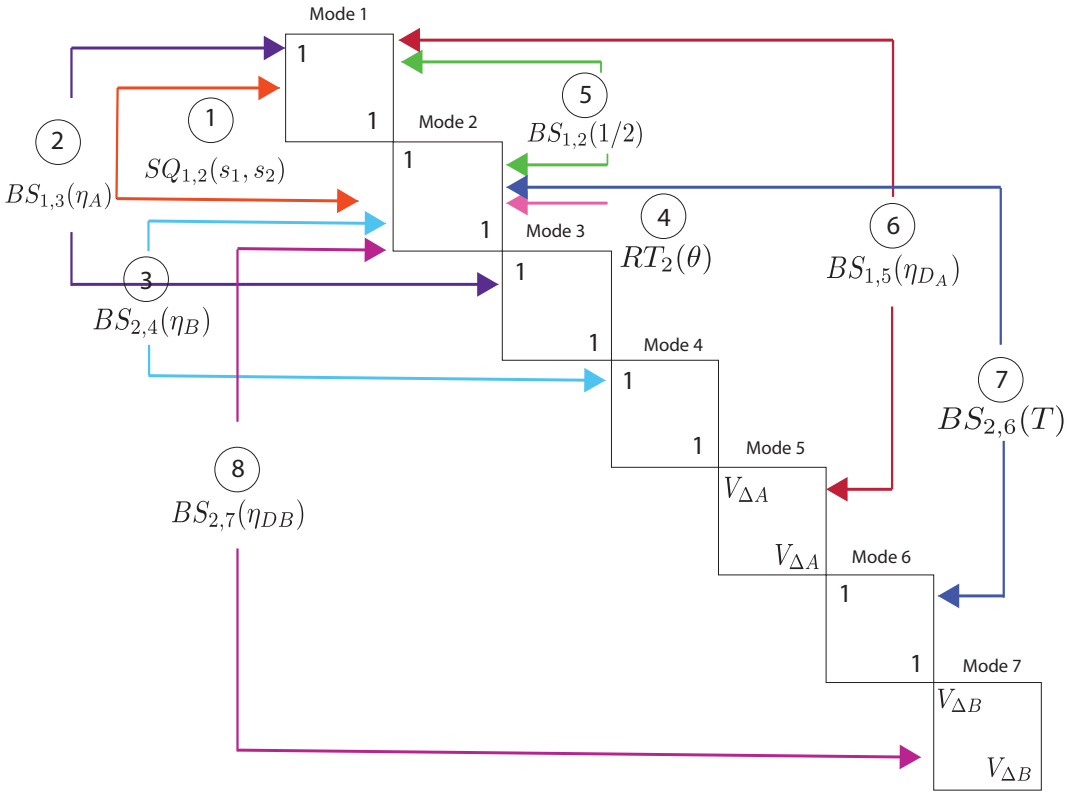


Figure 6.9: Schematic diagram of the modelling of the 1SDI-QKD experiment using entangled source and homodyne-homodyne measurements based on the symplectic transformations. In the calculation, 7 Gaussian modes were involved which are shown as Mode1 to Mode 7 in the diagram. To simulate the sequence of the experiment, appropriate Gaussian unitary operators were applied to these modes, in the order shown by numbers 1 to 8. Number 1 shows a squeezing operator applying on Modes 1 and 2 to produce a two-mode squeezed vacuum state. Numbers 2 and 3 depict the beamsplitter transformation with transmittance $\eta_{A(B)}$ applying between Modes 1,3 and 2,4 to model the loss introduced to each squeezers. Number 4 shows a phase shift θ applying to the second Mode to model the imperfect locking point. Number 5 demonstrates Modes 1,2 mixing on a 50:50 beamsplitter to create a two-mode EPR state. Numbers 6 and 8 shows a beamsplitter transformation to mix Modes 1,5 and 2,7 in order to model the loss on each homodyne detection. Number 7 illustrates a beamsplitter operator with transmittance T between modes 2,6 to model the lossy channel.

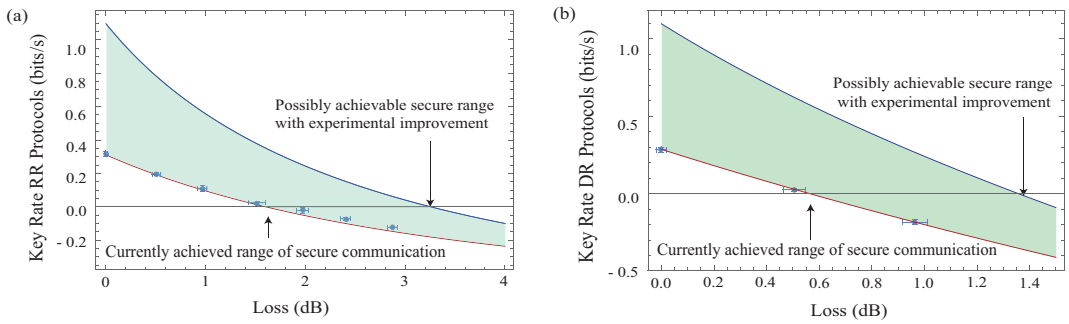


Figure 6.10: Predicted improvement of secure communication for the EB protocols with an improved experimental setup (blue curve) for the (a) RR protocol and (b) DR protocol. The model for the current system (red curve) is plotted along with experimental data (blue points) for comparison. The two OPAs in our system each produced -6 dB of squeezing and 10.7 dB of anti-squeezing and suffered from 13% combined loss due to the squeezers' cavities and the propagation through the optical components. A further loss of 6% and 8% was due to the inefficiency of Alice and Bob's homodyne detections respectively. The value of the unknown rotation, θ, was estimated to be $3\pi/180$. The improved system consists of two squeezers each producing -10 dB of measurable squeezing and 16 dB of anti-squeezing, 5% loss due to the cavities and propagation of the optical beams through the optical components with 4% and 5% loss for Alice and Bob's stations respectively and a rotation of $\pi/120$. Reconciliation efficiency is chosen to be 0.95 for both cases. These theoretical lines are produced using the model described in the text.

Chapter 7

Experimental Implementation of 1SDI-QKD Protocols in P&M scheme

7.1 Introduction

In this chapter I will describe the experimental implementation of the one-sided-device-independent protocol using (P&M) scheme. I will elaborate our experimental setup, the control system and data acquisition and will present the experimental results along with the error estimation and computer modelling .

7.2 Experimental Implementation of P&M Scheme

The experimental setup is depicted in Fig 7.1. A 1064 Nd:YAG laser was used in the experiment. It was the same laser as was described in section 3.7.2. The mode cleaning cavity that we used to prepare a quantum-noise limited optical field was also similar to the one elaborated in section 3.7.3. A large portion of the light was used as the local oscillator for the homodyne detection and small portion of it was passed through a pair of phase and amplitude electro-optic modulators (EOMs). EOMs were used to provide a Gaussian distributed modulation on each quadrature to produce a randomly displaced coherent states as described in section 3.7.4. It was shown that, coherent states prepared by Alice can be used for QKD protocols instead of an entangled source [90]. The equivalence between using these two type of sources for QKD applications is know as *virtual entanglement* and described earlier in section 5.3.1. Each EOM was driven by an independent function generator, providing a broadband white noise signal up to 10 MHz. The magnitude of the white noise was set to provide almost the same displacement on each quadrature.
The outputs of function generators were divided into two. One part was sent to drive the EOMs and the other to data acquisition system (DAQ) to be recorded, as shown in Fig 7.1. This modulation record, after calibration was considered as Alice's data since she had control over the source. Here, calibration means determining the relationship between the function generator output and the phase space displacement as

measured before transmission. I will describe the calibration more, shortly. This is to produce the virtual entanglement which was explained earlier (see section 5.3.1).
An electronic delay was introduced to Alice's and Bob's data to gain the maximum correlation between them at 3.5-4.5 MHz.
When the homodyne detector was locked to the phase quadrature there was 30 dB of suppression of cross correlation between orthogonal quadratures and when it was locked to the amplitude quadrature the suppression was around 37 dB. But this effect worsened as the modulation depth increased as is seen from the experimental results presenting in section 7.4.
A pair of photo-detectors using the Uni-PD circuits with a combination of the *Epitax ETX-500* photodiodes were used for the homodyne detection. The photodiode's quantum efficiency was estimated to be around 97%. Our pair of detectors were balanced electronically, providing 30 dB of common mode rejection.
The homodyne efficiency was estimated using the relationship $\eta_{Hom} = \eta_M . \eta_{QE}$ [39], as described in subsection 3.7.4. Here η_{Hom} is the overall efficiency of the homodyne, η_M denotes the degree of mode matching and η_{QE} is the quantum efficiency of the detector. Hence our homodyne efficiency was around 93% with fringe visibility of 98%, limited by the mode distortions introduced by the EOMs.

7.2.1 Calibration of function generator outputs

As mentioned before, the output of function generators need to be calibrated in order to provide the corresponding phase-space displacement. One way to calibrate the output of function generators, is to keep the channel transmission value to "1", and scan the voltage of function generators over a certain range. For each value of voltage, Bob should measure the corresponding quadrature amplitude of his received state. The slop of the plot showing the variation of the quadrature amplitudes measured by Bob which are normalized to quantum-noise, versus the output of function generators on Alice's side, will give the calibration factor.
Another way that I used, is to infer the calibration factor from the elements of the covariance matrix, built from the experimental data. Our experiment can be described by the simple picture shown schematically in Fig 7.2. Only one quadrature is illustrated in this picture. I assume that $\tilde{S}_a$ are the numbers saved from the function generator, and $S_a = \tilde{S}_a/k$ are the corresponding phase-space displacement, with k being the calibration factor. x_v is the vacuum input to the EOM, x_B is the output of homodyne measurement performed by Bob, and η is the channel transmission.

This experiment can be described mathematically as follows:

$$x_B = (x_v + S_a)\sqrt{\eta} + \sqrt{1-\eta} \tag{7.1}$$

It can be inferred easily that $< x_B\, S_a >= \sqrt{\eta}\ < S_a^2 >$, where $< S_a^2 >$ is the variance of S_a and $< x_B\, S_a >$ are the covariance or off-diagonal elements of the covariance matrix built from the Alice's data and the output of Bob's measurement (see section 2.6 on description on the covariance matrix). Hence, the channel transmission can be

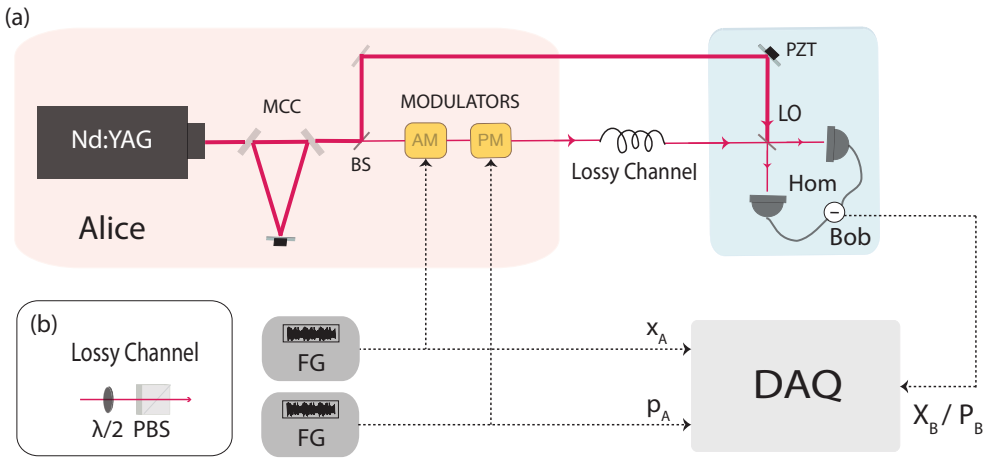


Figure 7.1: Schematic diagram of experimental setup implementing P&M scheme. A Nd:YAG 1064 nm laser was used as the light source. Here MCC is the mode-cleaning cavity which provided a quantum-noise limited laser field. AM and PM are electro-optic modulators (EOMs) driven by function generators (FG), which in turn provided Gaussian distributed displacement of the vacuum state in amplitude and phase quadratures. The resulting coherent states were sent to Bob's detection stations where he performed homodyne measurement (Hom), alternating between conjugate quadratures. DAQ is the digital data acquisition system. x_A and p_A are the outputs of function generators and X_B and P_B are the outcomes of the homodyne measurement. Inset (b) shows the combination of half waveplate ($\lambda/2$) and the polarizing beamsplitter (PBS) which were used to simulate the lossy channel. Red lines corresponds to the optical paths, while the dashed lines refer to the direction of the electrical signals.

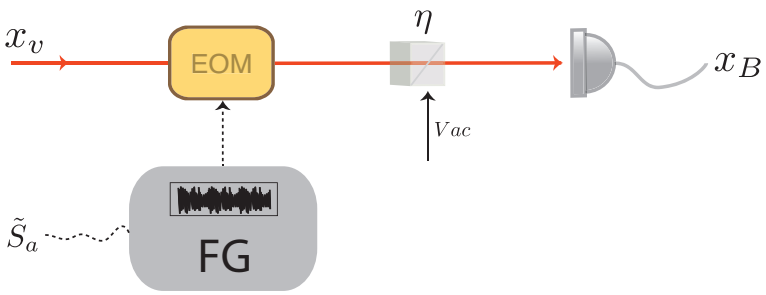


Figure 7.2: Simple diagram of P&M scheme showing only one quadrature.

written as:

$$\eta = \frac{cov(x_B, S_a)^2}{var(S_a)^2} \tag{7.2}$$

This helps to infer the calibration factor when $\eta = 1$ as (considering $S_a = \tilde{S}_a/k$) :

$$k = \frac{var(\tilde{S}_a)}{cov(x_B, \tilde{S}_a)} \tag{7.3}$$

7.3 Control System and Data Acquisition

This experiment was controlled digitally utilizing field programmable gate arrays (FPGAs). The digital control has the advantage of integration of the control loops and data acquisition together. The control loops and data acquisition codes programmed using National Instruments Lab VIEW. These codes were developed previously in our group by Dr. B. M. Sparkes et al [137], and further modified by Dr. Syed Assad. We used this system to lock the mode-cleaning cavity of the 1064nm laser field and a homodyne station.
In order to lock the homodyne station to the desired quadrature, a phase modulation at 21.25 MHz and an amplitude modulation at 30 MHz were imposed on the signal beam using electro-optic-modulators. After demodulation at the right frequency, an error signal was extracted enabling us to lock to any quadrature. The locking scheme of the homodyne station is illustrated schematically in Fig 7.3.

Utilizing this digital data acquisition system, 4×10^6 data points were sampled at 25×10^6 samples per second . The process was repeated five times in order to provide sufficient statistics for each data points. These data were then digitally filtered to 3.5-4.5 MHz.

7.4 Results

Here I present the result of the experimental implementation of the P&M scheme. In this experiment as described in section 7.2, Alice who was trusted and controlled the source, generated coherent states and Bob performed a homodyne measurement. In this protocol, Alice and Bob are also connected by a variable lossy channel of transmission T. The synchronization is local in this experiment and no finite size effects is taken into account. In addition, no parameter estimation errors due to the calibration imprecisions (see subsection 7.2) was calculated. I present the results as a function of the applied loss in dB scale.

In order to find the maximum range over which the protocol provides secure communication, we wish to find the optimal modulation variance for each value of the applied loss. Hence, we scanned the modulation variance over a range of 2 to 19 times the shot noise. The key rates were calculated using Equation 5.34, with reconciliation coefficient set to 0.95 for each modulation variance and loss setting. This is

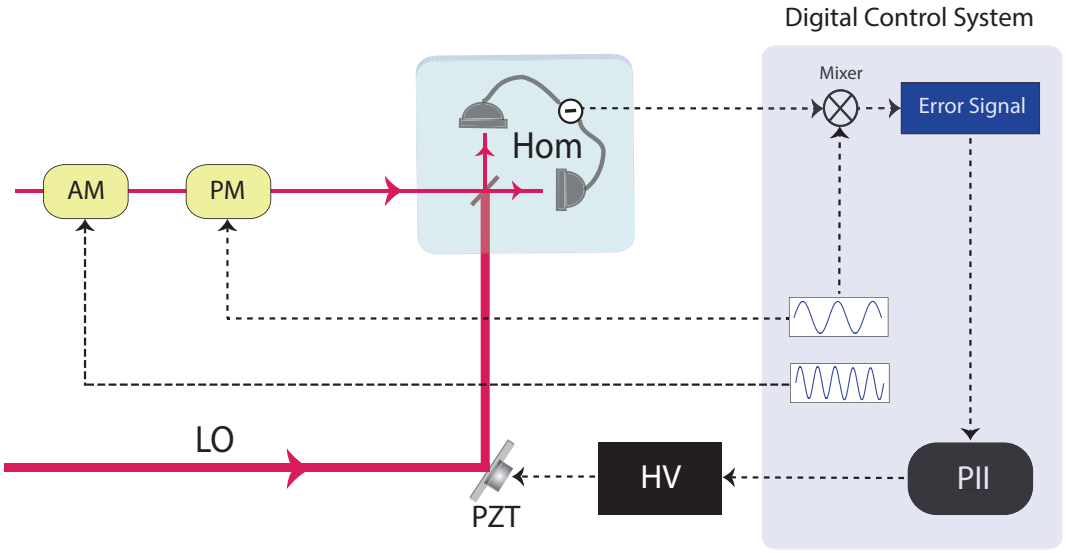


Figure 7.3: Schematic diagram of the homodyne lock utilized in P&M experiment. The input signal was modulated in both quadratures using electro-optic modulators. The two photocurrents coming from the two detectors of homodyne detection were subtracted, and was sent to the FPGA card. The error signal was extracted digitally, providing a proper feedback signal after being passed through a digital PII (proportional-double integral) controller.

an achievable value for CV-QKD [135, 10, 132]. Assuming it to be constant makes the comparison between different protocols possible. The result of these measurements is illustrated in Fig 7.4.

Fig.7.5 depicts the results obtained for the DR coherent state protocol for optimum modulation variances. We show that secure key can be generated after applying 0.6 ± 0.047 dB of loss, in good agreement with our theoretical model, which predicts our current setup would be secure up to applying 0.9 dB of loss. With the P&M protocol, we have much more freedom to vary the modulation variance and hence the virtual entanglement in order to optimize the secret key rate for each loss setting. As such, we could achieve a loss tolerance superior to the EB DR protocol, whilst using only the cheapest and most readily available quantum optical resources.

7.5 Error Estimation

In order to estimate the errors in calculating the key rates and other variables all variables $(A, B, ...)$ are considered to be independent and the error propagation formula is applied as follows:

$$\Delta Z = \sqrt{(\frac{\partial Z}{\partial A})^2 \Delta A^2 + (\frac{\partial Z}{\partial B})^2 \Delta B^2 + \cdots} \tag{7.4}$$

Here ΔA and ΔB etc represent the standard deviation of the variables. Key rates

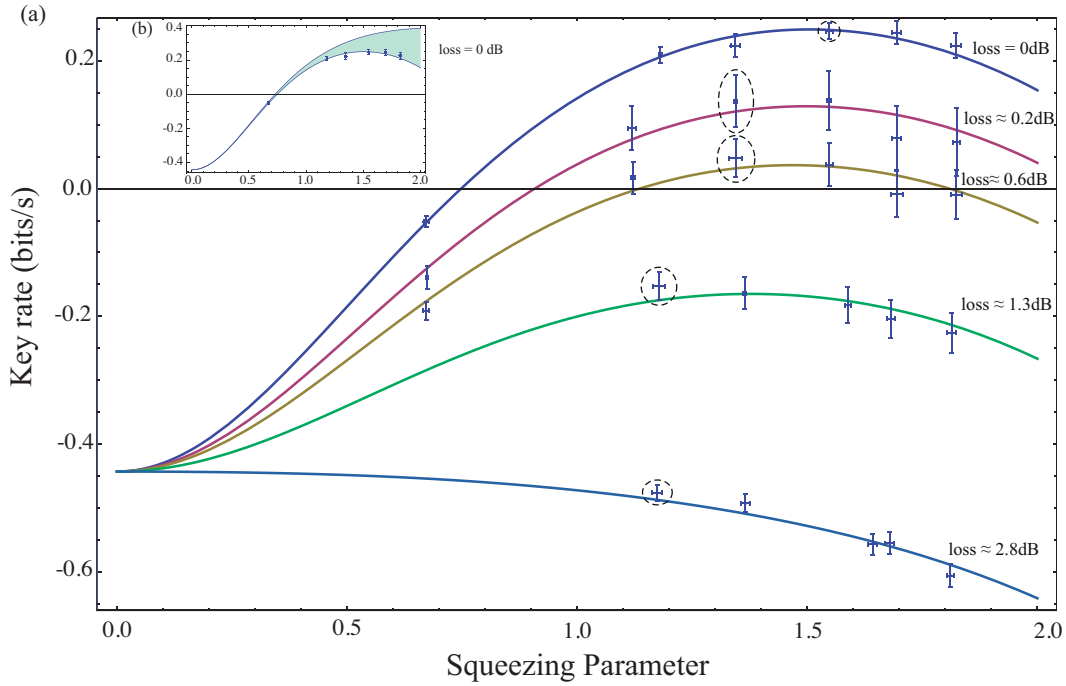


Figure 7.4: (a) variation of key rates versus effective modulation squeezing parameter for 5 different values of the applied loss. A theory line with the average value of the applied loss is fitted on the experimental data points. Data points surrounded by dashed circles correspond to the optimum modulation squeezing parameters which resulted the highest key rate for each loss setting. The key rates resulting from these optimum modulation variances are shown separately in Fig 7.5. (b) demonstrates the gap between the theoretical model and the realistic model which captures the experimental imperfections and matches well with the experimental results for the case of the zero applied loss. The model is described in section 7.6.

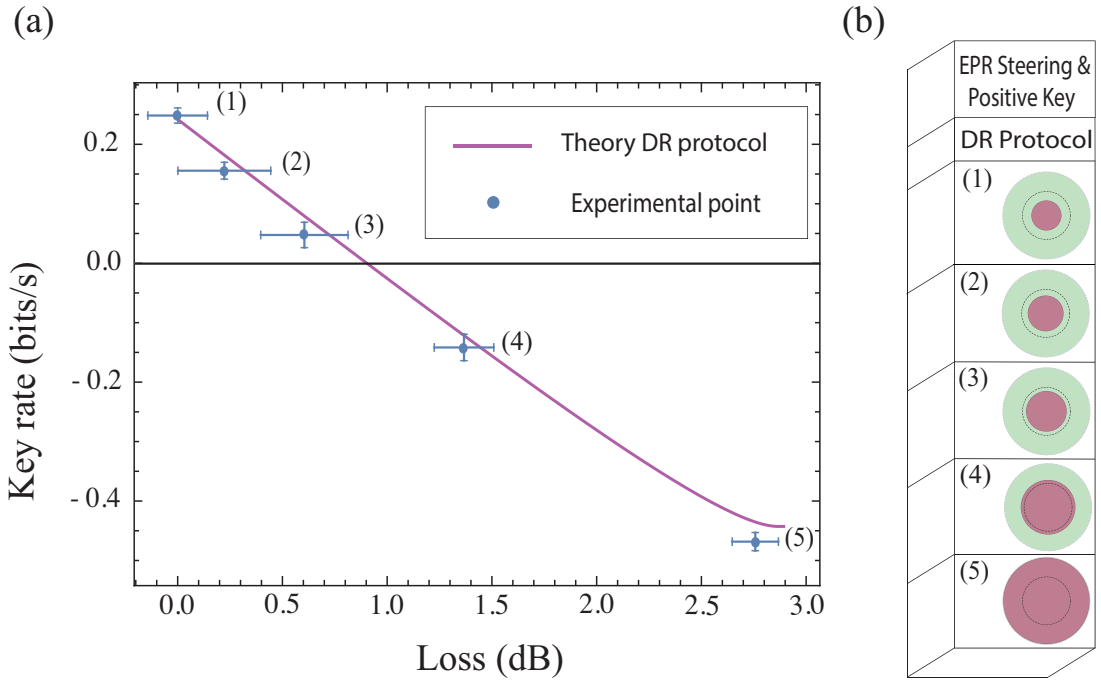


Figure 7.5: (a) key rates versus loss in dB scale for P&M coherent state DR protocol. Experimental error bars were estimated using error propagation of uncertainties. Panels (b) show the connection between the measured values of EPR steering and generation of the positive key rates, are as described in Fig 6.8.

are functions of the variances and covariances of the collected data. Each measurement was repeated 5 times for the this scheme, which provided us sufficient data to estimate the error.

7.6 Computer Modeling

To model the P&M experiment, I benefit from the equivalent EB picture and begin with $\sigma_{\text{in}} = \text{EPR(S)}$ given as follows :

$$\text{EPR}(s) = \begin{pmatrix} \cosh(2s) & 0 & \sinh(2s) & 0 \\ 0 & \cosh(2s) & 0 & -\sinh(2s) \\ \sinh(2s) & 0 & \cosh(2s) & 0 \\ 0 & -\sinh(2s) & 0 & \cosh(2s) \end{pmatrix} \tag{7.5}$$

where s is the squeezing parameter and is related to the modulation variance via $\cosh(2s) = V_S + 1$.

Recall that one part of the equivalent EPR state was sent to Bob through a lossy channel where he performed a homodyne detection, and on the other part Alice performed a heterodyne detection. To model the heterodyne detection a vacuum state was introduced to the first mode (Alice's mode) and mixed with it on a 50:50 beam splitter. Although much more flexible, the coherent state setup naturally still suffers from imperfections which in turn determine the optimum modulation. These imperfect correlations arise partly from cross correlation between orthogonal quadratures and partly from our limited ability to maximize the correlation between Alice and Bob's modes using electronic delay. Both phenomena can be thought of as an unknown rotation in the system. Hence, a rotation operator with small angles is applied to both quadratures of the second mode (Bob's mode) to model the imperfect correlation between Alice and Bob's modes.

To model the lossy channel, a thermal state with the variance of $1 + \chi$ was introduced to the system and mixed with the second mode on a beamsplitter of transmission T. Here χ is the excess noise entering to the system through the transmission channel. The excess noise χ was very small compared to decoherence effects caused by cross correlation between orthogonal quadratures. Hence, it has negligible impact on the key rate calculations. The transmission can again be determined directly by taking the ratio of the correlation at a particular setting with the correlation at full transmission. Here again all the states and operators were assumed to be Gaussian. Therefore, the final covariance matrix can be described by symplectic transformation (see subsection 2.6.1 and equation 6.2) as follows:

$$\sigma_{out} = S[\sigma_{in} \bigoplus V_\chi(B) \bigoplus diag(1,1)]S^{\text{T}}, \tag{7.6}$$

where $V_\chi = diag(1+\chi_x, 1+\chi_p)$, and $\chi_{x(p)}$ is the excess noise introduced to $\hat{x}(\hat{p})$

quadratures. The operator S is given by :

$$S = RT(\theta_x, \theta_p)BS_{1,4}(1/2)BS_{2,3}(T). \tag{7.7}$$

where RT is the rotation operator described by the matrix 8.17 and BS is the beam-splitter operator defined by matrix 8.18.

The variation of key rates versus the equivalent modulation squeezing parameter for 5 different transmission was previously shown in Fig 7.4. As is clear from Fig 7.4, using coherent states provides a much greater range over which to tune the equivalent squeezing. When using actual EPR states the maximum achievable value for s is around 0.8, well short of the optimum.

As the modulation was increased, so too was the detrimental effect on the correlations, leading to a smaller value for the optimal modulation parameter which for an ideal experiment would depend only upon β. In inset(b) of Fig 7.4 the gap between the ideal case without cross correlation and the realistic case is shown for the case of zero applied loss.

The key rate resulting from optimum modulation variances for each loss setting is chosen and plotted versus the applied loss in Fig 7.5. (a). In addition, our model predicts that if the cross correlation between Alice and Bob's modes was zero, the loss tolerance of the system would extend from 0.9 dB to 1.3 dB as depicted in Fig 7.6. This would result the extension of the range of secure communication for this protocol.

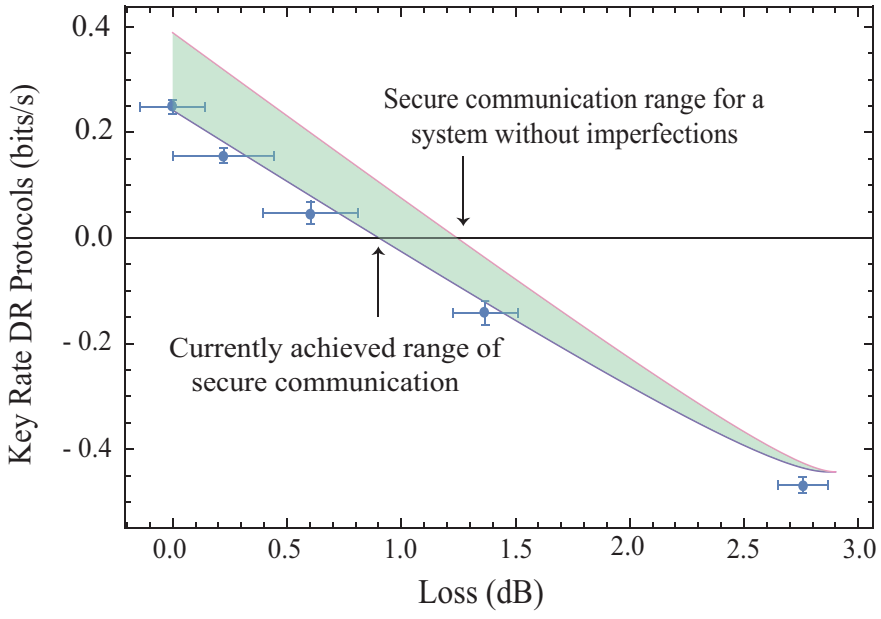


Figure 7.6: Comparison of the key rates resulted from optimum modulation variances versus the applied loss in dB scale for our experimental system and an ideal system with out any imperfections. The reconciliation efficiency is taken as 0.95 for both cases. These theoretical lines are produced using the model described in the text.

7.7 Summary

In this chapter I detailed our experimental implementation of one-sided device-independent quantum key distribution using coherent states. I started by giving the overall view of our experiment then I described the way I calibrated the function generator outputs. I explained our control and data acquisition system and presented our experimental results. I detailed the computer modelling I perform to understand the setup better and the way to improve it.

Chapter 8

Bell-like Correlations for Continuous-Variables

8.1 Introduction

In the early 1930s, Albert Einstein, Boris Podolsky and Nathan Rosen (EPR) in their seminal paper[3] pointed out the quantum entanglement to demonstrate that Quantum Mechanics was incomplete. They hoped that a more comprehensive and less troubling theory could replace it one day. Their argument was based on two assumptions of realism (that physical objects have real properties determining the outcome of a measurement) and locality (that the physical reality in one location is not influenced instantaneously by measurements conducted at a distant location), together called "local realism" or "local hidden variables". However, EPR did not provide any test to prove local realistic theories. These concepts were first quantified in 1964 by John Bell [5] through his famous inequalities. Bell assumes that a pair of particles have interacted and separated, where two distant observers perform measurement on them. If local realistic theories are correct, the correlations between different outcomes of measurements should obey certain constraints defined by Bell's inequalities. While the violation of the Bell's inequalities disprove all local realistic theories.

In addition, it has particular implication in quantum key distribution where the violation of the Bell's inequality will rule out any tampering of the quantum source leading to the development of device-independent QKD as described earlier in chapter 4.
In this chapter I review the Bell's inequality and show how it can be extended to the continuous-variables scheme. Then I will discuss the computer simulation I performed to model two experiments proposed in ref [1, 2] that can violate the Bell's inequality in continuous varaibles. The feasibility of these experiments open the door for real-life implementation of device-independent CV-QKD.

8.2 Mathematical Description of Bell's Inequality

In order to derive the original inequality Bell considered the EPR argument promoted by Bohm and Aharonov [138], where an entangled pair of spin one-half particles

formed in the singlet state can move freely in opposite directions. Measurements are performed employing Stern-Gerlach magnets on the selected components of the spins, where spins of particles 1&2 are defined by $\vec{\sigma_1}$ and $\vec{\sigma_2}$ respectively. Considering $\vec{a}$ as a unit vector in a certain direction, then the measurement of the spin component in that direction which is described by $\vec{\sigma_1} \,.\, \vec{a}$, yields the value $+1$. Hence the measurement of the spin of the other particle on the same direction $\vec{\sigma_2} \,.\, \vec{a}$ must yield -1 according to the laws of quantum mechanics. Now we can imagine that the two measurement apparatuses are placed far from each other in a way that the orientation of one Stern-Gerlach magnet does not affect the result of the other measurement setup. Since the result of measuring any chosen spin component of of particle 2, can be predicted by previously measuring the same component of the spin of particle 1, it suggests that the result of any such measurement should be predetermined. Since according to the quantum mechanics the result of any measurement cannot be determined in advance, this predetermination may lead to the possibility of the more complete description of quantum mechanics by including the so-called *hidden variables* [5].

To include the hidden variables, a single continuous parameter λ was assumed in a way that the result A of measuring $\vec{\sigma_1}.\vec{a}$ is determined by $\vec{a}$ and λ, and the result B of measuring $\vec{\sigma_2}.\vec{b}$ in the same time is determined by $\vec{b}$ and λ. The outcomes of these measurements are as follows [5]:

$$A(\vec{a},\lambda) = \pm 1,\ B(\vec{b},\lambda) = \pm 1. \tag{8.1}$$

The important assumption is that the result B for particle 2 is not affected by the measurement setting of the particle 1 or vice versa.

Considering $\rho(\lambda)$ as the probability distribution of λ, then the quantum correlation which is defined as the expectation value of the product of the two components $\vec{\sigma_1}.\vec{a}$ and $\vec{\sigma_2}.\vec{b}$ is given by [5] :

$$P(\vec{a},\vec{b}) = \int d\lambda\, \rho(\lambda) A(\vec{a},\lambda) B(\vec{b},\lambda) \tag{8.2}$$

If the description using the hidden variables is correct, the expectation value defined above should be equal to the quantum mechanical expectation value [5] :

$$< \vec{\sigma_1} \,.\, \vec{a}\ \vec{\sigma_2} \,.\, \vec{b} >= -\vec{a} \,.\, \vec{b} \tag{8.3}$$

However, Bell showed through developing his famous inequality that it is not possible to have the quantum mechanical expectation value defined above, by including the hidden variables. His original proposed inequality is as follows [5] :

$$1 + P(\vec{b},\vec{c}) \leq |P(\vec{a},\vec{b}) - P(\vec{a},\vec{c})|. \tag{8.4}$$

here $\vec{a}$, $\vec{b}$ and $\vec{c}$ denote the unit vectors in the direction of three arbitrary measurement settings, and Ps are the correlation functions defined by relation 8.2. Nevertheless, this inequality is restricted to the case in which the outcomes of both sides of the

experiment should be anti-correlated when the analyzers are parallel. This makes the real implementation of this inequality very hard. Hence other inequalities were developed which are experimentally more feasible.

8.3 CHSH Inequality

"in 1969, John Clauser, Michael Horne, Abner Shimony and Richard Holt generalized Bell's original inequality to the famous CHSH inequality " [139]. As the original Bell's inequality it introduces constraints on the correlations of the outcomes of the measurements performed by the two different parties. Though, no assumption of perfect correlation or anti-correlation at equal detector settings was taken into account to derive this inequality. The CHSH inequality is defined as follows [139]:

$$|E(a,b) - E(a,b') + E(a',b) + E(a',b')| \leq 2 \tag{8.5}$$

where a and a' are two different detector settings on side A, and b and b' are different detector settings on side B. The $E(a,b)$ etc. are the quantum correlations of the pair of particles defined as the expectation value of the product of the "outcomes " of the experiment, as previously described by equation (8.2):

$$E(a,b) = \int d\lambda\, \rho(\lambda) A(a,\lambda) B(b,\lambda) \tag{8.6}$$

where λ again is the "hidden variable" drawn from a fixed distribution with density function $\rho(\lambda)$, and A and B are the average values of the outcome of the measurements made by two parties as described previously by relation 8.1. However, in relation 8.1 two outcomes ± 1 was denoted for the outcome of the measurements, while for CHSH inequality which was derived based on the use of "two-channel" detectors, $+1$ is coded for "+" and -1 for the "-" channel. As performing a real experiment at that time meant utilizing of polarized light and single-channel polarizers, where they interpreted "-" as "no detection" and "+" as the "detection" of the single photon. In fact, most of the experiments performed so far employed properties of light like its polarization, as in the well-known experiment by Aspect et al. [140] rather than spins of the electrons as Bell thought in the first place. Schematic diagram of this kind of experiments is shown in Fig 8.1.

Quantum mechanics predicts maximum violation of $2\sqrt{2}$ for CHSH inequality which is greater than 2. Therefore, experimental verification of violation of this inequality proves that the nature cannot be described by local hidden variables theories.

For experiments utilizing single photons, simultaneous observations or coincidences are recorded and categorized as "+ +","+ -","- +" and "- -", where "+" implies the detection of a single photon and "-" to non-detection of a photon. The numbers of coincidences for each detection settings (a,b) are registered as N_{++} etc. The

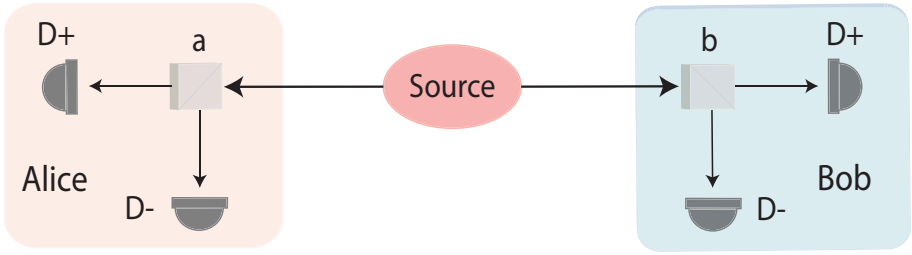


Figure 8.1: Schematic diagram of a two channel CHSH Bell experiment. Pairs of photons are produced by an entangled source. They are sent through two different directions. Each photon encounters a two-channel detection station where two parties Alice and Bob perform measurement by setting the orientation of their polarizer.

experimental estimation for correlation functions $E(a,b)$s are calculated as [139]:

$$E(a,b) = \frac{N_{++} - N_{+-} - N_{-+} + N_{--}}{N_{++} + N_{+-} + N_{-+} + N_{--}} \tag{8.7}$$

Four separate subexperiments should be performed corresponding to the four terms of $E(a,b)$ in CHSH inequality. The settings a, a', b, b' are generally set to the angles 0, $\pi/4$, $\pi/8$ and $3\pi/8$ respectively. These angles which are known as the "Bell test angles" result the greatest violation of the inequality. When all the correlation functions are estimated, equation (8.5) will be used to calculate the CHSH Bell's inequality. If the number is bigger than 2, it will prove quantum mechanics to be correct excluding all the hidden variable theories.
One of the most important assumptions in the derivation of the CHSH inequality was fair sampling. It assumes that the detected pairs are a fair samples of the emitted photons.

8.4 CHSH Inequality for Continuous Variables

Optics has been a platform for experimental demonstration of bell's inequality for a long time, in a way that polarization of single photons were used in the experiment by Aspect et al. [140]. However, due to the improvements in the field of quantum information using optical systems based on the continuous variables, developing a Bell type inequality for these systems is of significant importance. T. C. Ralph et al. in ref [1] proposed a method for observing Bell type correlations with continuous variables. They suggested that EPR states created by squeezed light beams can be utilized to violate a Bell's type inequality. In their first proposal they suggested to use four independent squeezing sources to generate two pairs of EPR states [1]. Although using four squeezing sources would provide higher correlation, it is experimentally challenging to implement. Hence, a simpler systems were proposed later by E. H. Huntington and T.C.Ralph in ref [2] based on only two bright squeezed sources with moderate levels of amplitude squeezing.

The Bell-type correlation experiment suggested in [1, 2] is shown schematically

in Fig 8.2. A quantum optical source S generates four-mode (two spatial and two polarization) correlated beams of light denoted by $\hat{A}_h$, $\hat{A}_v$, $\hat{B}_h$ and $\hat{B}_v$, where two modes $\hat{A}_h$ and $\hat{A}_v$ are sent to Alice and the other two modes $\hat{B}_h$ and $\hat{B}_v$ to Bob. By using a combination of polarizing optics, such as a half-waveplate and polarizing beamsplitter, they mix their modes and separate them to two polarization basis "+", "-" at an angle θ_A and θ_B. This is given by the following transformation [2] :

$$\hat{A}_+(\theta_A) = cos\theta_A\,\hat{A}_h + sin\theta_A\,\hat{A}_v \tag{8.8}$$
$$\hat{A}_-(\theta_A) = cos\theta_A\,\hat{A}_v - sin\theta_A\,\hat{A}_h \tag{8.9}$$
$$\hat{B}_+(\theta_B) = cos\theta_B\,\hat{B}_h + sin\theta_B\,\hat{B}_v \tag{8.10}$$
$$\hat{B}_-(\theta_B) = cos\theta_B\,\hat{B}_v - sin\theta_B\,\hat{B}_h \tag{8.11}$$

Then Alice performs one of the measurements $\{\theta_A, \theta'_A\}$ on her mode and Bob performs one of the measurements $\{\theta_B, \theta'_B\}$ on his mode. The result of the measurements are shown by two outcomes R^+ and R^-, where +1 is coded for R^+ and -1 for R^- in the Bell experiment.

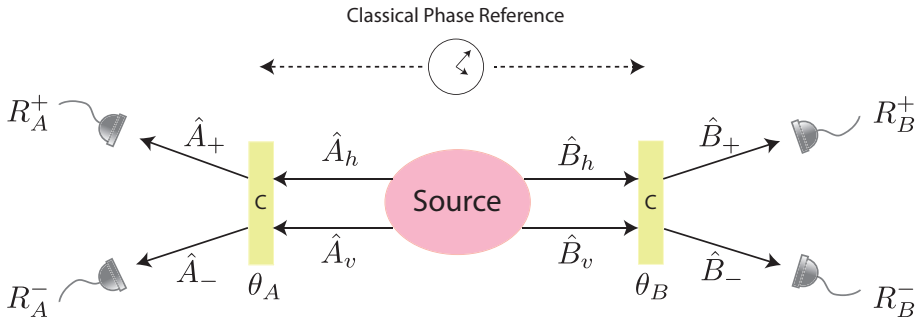


Figure 8.2: Schematic diagram of a quantum optical system that can be used to demonstrate the violation of Bell's inequality. Here $\hat{A}_h$, $\hat{A}_v$, $\hat{B}_h$ and $\hat{B}_v$ are the four-mode (two spatial and two polarization) of the system generated by the source. Polarizing optics are used to decompose the two spatially distinct beams $\hat{A}$ and $\hat{B}$ into a polarization basis set $+,-$ at an angle θ to the original h, v basis. Photo detection in the $+$ and $-$ basis on each beam can be made. The classical phase reference refer to the local oscillator that is used for homodyne measurement.

The photon number correlation can be constructed by repeating the experiment several times and using the correlation statistics between Alice and Bob's measurement outcomes as follows [1, 2]:

$$\begin{aligned}\langle R^{ij}(\theta_A\theta_B)\rangle &= \langle R_A^i(\theta_A) R_B^j(\theta_B)\rangle \\ &= \langle \hat{A}_i^\dagger(\theta_A)\hat{A}_i(\theta_A)\hat{B}_j^\dagger(\theta_B)\hat{B}_j(\theta_B)\rangle\end{aligned}$$

where $i, j = +, -$. The R^{ij} correspond to the numbers of coincidences for each detection settings defined as N_{++} etc. in section 8.3. Hence, the correlation function

corresponding to relation 8.7 can be built using these photon number correlations as follows[1, 2]:

$$E(\theta_A,\theta_B)=\frac{\langle R^{++}(\theta_A,\theta_B)\rangle+\langle R^{--}(\theta_A,\theta_B)\rangle-\langle R^{+-}(\theta_A,\theta_B)\rangle-\langle R^{-+}(\theta_A,\theta_B)\rangle}{\langle R^{++}(\theta_A,\theta_B)\rangle+\langle R^{--}(\theta_A,\theta_B)\rangle+\langle R^{+-}(\theta_A,\theta_B)\rangle+\langle R^{-+}(\theta_A,\theta_B)\rangle}. \tag{8.12}$$

here also the measurement settings can be chosen as $\{0,\pi/4\}$ for $\{\theta_A,\theta'_A\}$ and $\{\pi/8,3\pi/8\}$ for $\{\theta_B,\theta'_B\}$, which are the "Bell test angles" introduced in section 8.3 and were also used for settings a, a', b, b' in section 8.3. Any local realistic description of the correlations can be bounded using CHSH Bell's inequality as [1, 2]:

$$B=|E(\theta_A,\theta_B)+E(\theta'_A,\theta'_B)+E(\theta'_A,\theta_B)-E(\theta_A,\theta'_B)|\leq 2. \tag{8.13}$$

Here again four separate subexperiments corresponding to the four combination of measurement settings should be performed to build the four terms of $E(\theta_A,\theta_B)$s in CHSH inequality.
In order to extend this result to continuous variable measurements, it was shown in ref [1] that the photon number correlations can be decomposed into a series of quadrature amplitude measurements using the equivalence [1, 2]:

$$\hat{A}_i^\dagger\hat{A}_i\equiv 4(\hat{A}_i^\dagger\hat{A}_i-\hat{V}_i^\dagger\hat{V}_i)=(\hat{X}^i_{A;1})^2+(\hat{X}^i_{A;2})^2-(\hat{X}^i_{V;1})^2-(\hat{X}^i_{V;2})^2 \tag{8.14}$$

where $\hat{X}_{F;1}=\hat{F}+\hat{F}^\dagger$ corresponds to amplitude quadrature operator and $\hat{X}_{F;2}=i(\hat{F}-\hat{F}^\dagger)$ corresponds to phase quadrature operator. They can be measured experimentally using homodyne detection technique (see section 2.8.1). $\hat{V}_i$ is a vacuum mode where $\langle\hat{V}_i^\dagger\hat{V}_i\rangle=0$. Using equation (8.14) and assuming that the fields having Gaussian statistics, correlation functions R^{ij} can be written as [1, 2] :

$$\begin{aligned}R^{ij}=\frac{1}{16}[&2(\langle\hat{X}^i_{A;1}\hat{X}^j_{B;1}\rangle^2+\langle\hat{X}^i_{A;2}\hat{X}^j_{B;2}\rangle^2+\langle\hat{X}^i_{A;2}\hat{X}^j_{B;1}\rangle^2+\langle\hat{X}^i_{A;1}\hat{X}^j_{B;2}\rangle^2)\\&+V^i_{A;1}V^j_{B;1}+V^i_{A;2}V^j_{B;2}+V^i_{A;2}V^j_{B;1}+V^i_{A;1}V^j_{B;2}-2V_v(V^i_{A;1}+V^j_{A;2})\\&l-2V_v(V^i_{B;1}+V^j_{B;2})+4V_v^2]\end{aligned}$$

where $V_{F;k}=\langle(\hat{X}_{F;k})^2\rangle$ for $k=1,2$.
This shows that the correlation function defined by equation 8.12 and hence the CHSH inequality given by equation 8.13, can be built from the photon correlations R^{ij} developed for continuous variables introduced above. The violation of CHSH inequality for continuous variables suggests the presence of strong correlation between the subsystems of a quantum system and excludes all the hidden variable theories.
In the next section I will describe the computer simulation I conducted to model the experimental setups suggested in [1, 2].

8.5 Computer Modeling of two systems showing Bell type correlation using continuous variables

I simulated two of the experimental setups suggested in [1, 2] and calculated the possible outcomes of those experiments. The first setup was the scheme using four squeezing sources named as $S1$ in [1]. The second one, was the similar scheme in which two squeezing sources are used instead of four. This scheme is called $S2$ in [2]. These two experimental setups are shown schematically in figures 8.3 and 8.4.

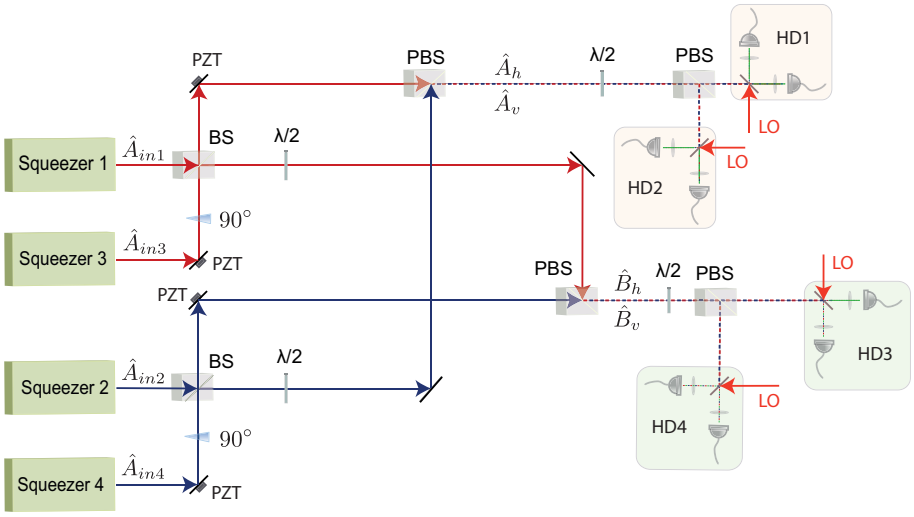


Figure 8.3: Schematic diagram of system $S1$ using four squeezing sources proposed in ref [1]. Four horizontally polarized bright amplitude-squeezed beams are produced. The third and forth beams ($\hat{A}_{in3}, \hat{A}_{in4}$) experienced 90^o phase shift and then combined on a 50:50 beamsplitters with the first and second beams ($\hat{A}_{in1}, \hat{A}_{in2}$) respectively to generate two EPR states. The polarizations of the transmitted outputs from the beamsplitters are rotated by 90^o. The reflected outputs from each beamsplitter are combined with the transmitted beams from the other beamsplitter on a polarizing-beamsplitter (PBS) to form the output modes $\hat{A}_h, \hat{A}_v, \hat{B}_h, \hat{B}_v$. A combination of half-waveplate and polarizing-beamsplitter are used to decompose the two spatially distinct beams to the new polarization basis. Each output is sent to a homodyne detection station in order to perform the quadrature amplitude measurements. Here PZT is piezo-electric crystal, BS is beamsplitter, $\lambda/2$ is half-waveplate, 90^o refers to the 90^o phase shift, PBS is polarizing beamsplitter and HD refers to homodyne detection.

To model the experiments showing the Bell type correlation from continuous variables, all the states and operators were assumed to be Gaussian. Hence, the states can be described by their mean values and covarinace matrices (CMs), where symplectic transformations are used to describe the effect of the Gaussian operations on the Gaussian states as described in subsection 2.6.1 . This simulation is very similar to the theoretical modelling of 1SDI-QKD experiment which was described in sections 6.7. Except that in Bell type correlation experiments four modes are involved.

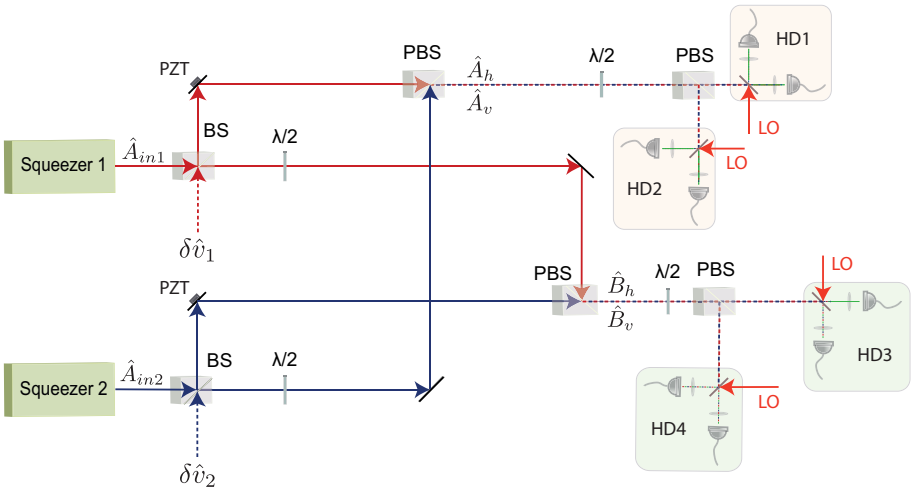


Figure 8.4: Schematic diagram of system *S*2 using two squeezing sources proposed in ref [2]. This system is very similar to system *S*1 shown and described in figure 8.3. Except, instead of squeezed beams $\hat{A}_{in3}$ and $\hat{A}_{in4}$, vacuum modes $\delta\hat{v}_1$ and $\delta\hat{v}_2$ are introduced and mixed on beamsplitters with squeezed modes $\hat{A}_{in1}$ and $\hat{A}_{in2}$ respectively.

The CM of a four-mode squeezed vacuum state with squeezing in quadrature of modes *i*,*j*,*k* and *l* is given by applying the following symplectic operator:

$$SQ_{i,j,k,l}(s_1,s_2,s_3,s_4) = \begin{pmatrix} e^{s_1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & e^{-s_1} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & e^{s_2} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & e^{-s_2} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & e^{-s_3} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & e^{s_3} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & e^{-s_4} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & e^{s_4} \end{pmatrix} \tag{8.15}$$

where s_1, s_2, s_3 and s_4 are the squeezing parameters applied on the modes 1 to 4 or i^{th}, j^{th}, k^{th} and l^{th} respectively. I assumed modes 1&2 to be squeezed on the same quadrature and modes 3&4 to be squeezed on the orthogonal quadrature, so later modes 1&3 and 2&4 can be mixed on a 50:50 beamsplitter to create two EPR states. This is equivalent to applying the 90^o phase shifts to the output of the squeezers 3th and 4th in Fig 8.3.
In order to model the loss of each squeezer, a vacuum mode is introduced and mixed with the squeezed mode by applying a beamsplitter operator of transmittance η_A for the first squeezed mode and vacuum, η_B for the second squeezed mode and vacuum, η_C for the third squeezed mode and vacuum and η_D for the forth squeezed mode and vacuum. The beamsplitter transformation between any two modes is given by :

$$BS(\eta) = \begin{pmatrix} \sqrt{\eta} & 0 & -\sqrt{1-\eta} & 0 \\ 0 & \sqrt{\eta} & 0 & -\sqrt{1-\eta} \\ \sqrt{1-\eta} & 0 & \sqrt{\eta} & 0 \\ 0 & \sqrt{1-\eta} & 0 & \sqrt{\eta} \end{pmatrix} \tag{8.16}$$

As shown in Fig 8.3, the squeezed modes 1 & 3 and 2 & 4 are mixed on the 50:50 beamsplitter to create EPR states. Before mixing these modes, a rotation operator was applied to modes 1 and 2 to model the phase shift due to the imperfect locking point. The applied operator is given by :

$$RT(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \tag{8.17}$$

After that beamsplitter operators with transmittance of $1/2$ were applied on modes 1 & 3 and 2 & 4.
To model the transformations defined by 8.11, a beamsplitter operation with the transmittance of $cos^2(\theta_A)$ is applied on modes 2 & 3 and another beamsplitter operation with the transmissivity of $cos^2(\theta_B)$ is applied on modes 1&4. A two-mode beamsplitter operator with the transmissivity of $cos^2(\theta)$ is given by :

$$BS(cos^2\theta) = \begin{pmatrix} cos\theta & 0 & -sin\theta & 0 \\ 0 & cos\theta & 0 & -sin\theta \\ sin\theta & 0 & cos\theta & 0 \\ 0 & sin\theta & 0 & cos\theta \end{pmatrix} \tag{8.18}$$

The loss of the four homodyne stations was simulated by applying a beamsplitter operator of transmittance η_{D_A}, η_{D_B}, η_{D_C} and η_{D_D}, which are equal to the homodyne efficiencies, while the other mode was in a thermal state of variance $V_{\Delta_{A(B,C,D)}} = 1 + \Delta_{A(B,C,D)}/(1 - \eta_{D_{A(B,C,D)}})$, to model the detector dark noise of magnitude $\Delta_{A(B,C,D)}$. The correlation functions and Bell's inequality were calculated using the equation mentioned in section 8.13.

Modelling of the system $S2$ proposed in [2] and shown in Fig 8.4, which uses two squeezers instead of four was the same as described above. Except the squeezing operator was not applied on modes 3&4. Hence each of the 1st and 2nd modes was mixed with a vacuum on a 50:50 beamsplitter.

The results of this simulation is shown in Fig 8.5, which suggests that both of the experimental setups $S1$ and $S2$ can violate the Bell's inequality. It is obvious that the system $S1$ that uses four squeezers show higher correlation and higher violation of Bell's inequality. However, the correlation generated from two squeezers also show the violation of Bell's inequality while being experimentally more feasible.

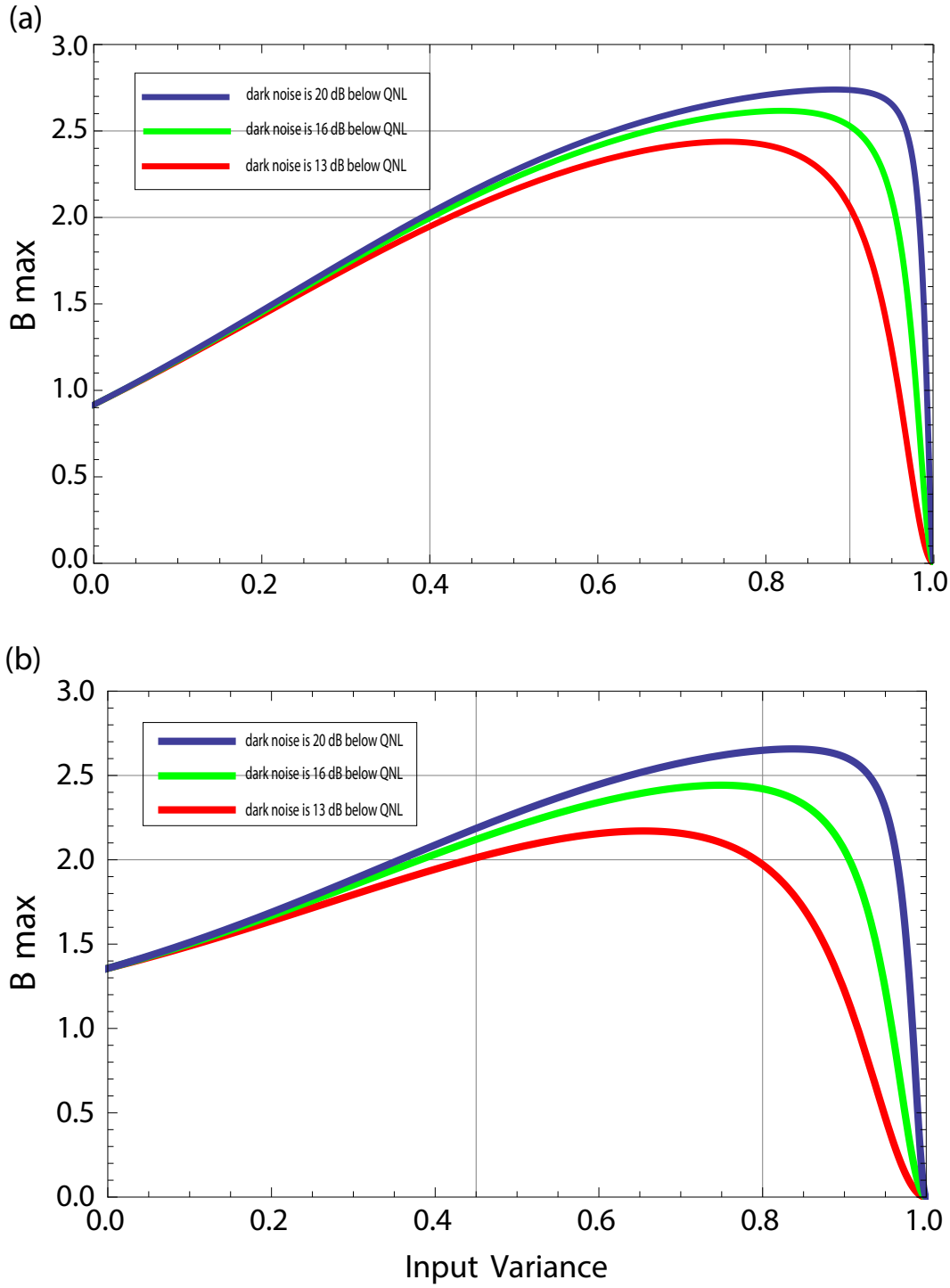


Figure 8.5: Plots showing the maximum violation of Bell's inequality (B_{max}) as a function of the variance of the input state for (a) an experimental setup using four squeezing sources suggested in [1] and named as system $S1$ and (b) the experimental setup using two squeezing sources suggested in [2] and named as system $S2$. Bell test angles were used to calculate the (B_{max}). Three levels of detectors' electronic noise variances of 13 dB, 16 dB and 20 dB below quantum noise limit were considered for each system.

8.6 Summary

I this chapter I introduced briefly the Bell's inequality, a fundamental inequality in physics which proves quantum mechanics to be correct and ruling out the hidden variable theories. I described CHSH inequality and showed how it can be extended to continuous-variables. I illustrated two experimental schemes for the measurement of the Bell-type correlation from continuous variables proposed in [1, 2]. I elaborated the computer simulation I performed to model these two experiments and presented its results which shows that both schemes which are experimentally feasible can violate Bell's inequality. The violation of Bell's inequality for continuous-variables quantum systems, despite having the fundamental importance, opens new horizons for secure quantum communication through the development of device-independent QKD, as is described in chapter 4.

Chapter 9

Conclusion

In this thesis I covered our studies on different types of quantum correlations; Quantum Discord, EPR-steering and Bell-type correlation.

I have introduced our simple experimental technique to verify quantum discord in continuous-variable quantum states. This method can be applied to unknown bipartite Gaussian states and certain type of non-Gaussian states which can be produced by exposing statistical mixtures of coherent states to one port of a beam-splitter and the vacuum state to the other port. We implemented this technique experimentally by producing a thermal state and subjecting it to a beam-splitter to prepare a separable but correlated bipartite state. Three different non-Gaussian states were also prepared; the first one was a uniform statistical mixture of vacuum and a thermal state, the second was a mix of coherent and the vacuum state and the last one was generated using asynchronous detection. This corresponds to the stroboscopic observation of the quadrature of a harmonic oscillator. Our technique successfully proved nonzero quantum discord in all the prepared Gaussian and non-Gaussian states. Since our method provides an easy way to confirm the presence of quantum discord in a bipartite quantum state, it can open the door for practical implementation of quantum discord as a resource for quantum computations and communications.

In the second part of this thesis, I have looked at the EPR-steering, the intermediary scheme between general entanglement and the Bell-type correlation. I have discussed its application in the quantum cryptographic scenario known as "one-sided device independent QKD" where the apparatuses of one of the communicating parties are only trusted. I have presented our theoretical and experimental investigations on the complete family of the Gaussian CV-QKD protocols from the perspective of one-sided device independence and its connection to EPR-steering. We have demonstrated theoretically that only 6 of the 16 possible Gaussian CV-QKD protocols are device-independent, and implemented 5 of those 6 protocols experimentally. We have used both entanglement-based (EB) and prepare and measure (P&M) schemes. I have detailed the experimental implementations and the results in this thesis. One of the highlights of our research was the first demonstration of a 1SDI-QKD protocol employing only the coherent states. This surprising result and the fact that producing coherent states is a lot cheaper and easier than entangled states makes them an elegant candidate for the short range metropolitan quantum networks.

In the last part of this thesis I looked at the Bell-like correlations for continuous-

variables. It was based on the theoretical proposal of ref [1, 2]. This completes my study on quantum correlations. We are implementing experimentally this proposal in our group. The experiment is not completed yet. Here, I only presented the result of my computer simulation.

9.1 Future Work

Our research on 1SDI CV-QKD can be improved further experimentally and theoretically. As suggested by my computer modelling presented in section 6.7 for EB scheme and section 7.6 for (P&M) scheme, by improving the experimental setup we can boost the range of secure communication considerably. For example, in (EB) scheme by decreasing the the level of noise reduction (squeezing) to -10 dB and improving the locks the applied loss can be increased from 1.6 dB to more than 3.2 dB which in turn will expand the range of the secure quantum communication. This effect is captured in figure 6.10. There is a little room to improve the secure range using the coherent states. However, still by omitting the effect of cross-correlation it can be increased as shown in figure 7.6.

Another way to further extend the range of these 1SDI-QKD protocols, would be employing the noiseless linear amplifier [109, 141], especially the measurement based version of these scheme which has been recently demonstrated [142]. However, this could only be applied to the RR protocols.

From theoretical point of view, we need to include finite size effects [143] into our security proof.

After implementing all the improvements mentioned above, it is possible to apply our 1SDI-QKD protocols practically between two nodes connected with fibre optics. This can be done for example between ANU and UNSW-ADFA in Canberra where the fibre optics link is already available.

Completing the Bell's test using continuous variables; itself is of special interest. It can provide the tool for implementation of device-independent quantum key distribution in continuous-variables. In addition, since the violation of the Bell's test guarantees the existence of quantum entanglement in the system under measurement, the output of the measurement is assured to be random and not predetermined. This makes it possible to generate random numbers [144] from the output of the homodyne measurements in the experiment.

References

1. T. C. Ralph, W.J. Murno and R. E. S. Polkinghorne, *Proposal for the Measurement of Bell-Type Correlations from Continuous Variables*, Phys. Rev. Lett. **85**, 2035 (2000). (cited on pages x, xvi, 2, 5, 101, 104, 105, 106, 107, 110, 111, and 114)

2. E. H. Huntington and T. C. Ralph, *Continuous-variable Bell-type correlations from two bright squeezed beams*, Phys. Rev. A. **65** 012306 (2001). (cited on pages x, xvi, 2, 5, 101, 104, 105, 106, 107, 108, 109, 110, 111, and 114)

3. A. Einstein, B. Podolsky and N. Rosen, *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*, Phys. Rev. **47**, 777 (1935). (cited on pages 1, 26, 28, and 101)

4. W. Heisenberg, Zeitschrift für Physik. **43**, 172-198 (1927). (cited on pages 1, 14, 61, and 62)

5. J. S. Bell, *On The Einstein Podolsky Rosen Paradox* , Physics **1**, 195 (1965). (cited on pages 1, 31, 50, 53, 101, and 102)

6. V. Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dusek, Nobert Lütkenhaus, Momtchil, *The security of practical quantum key distribution*, Rev. Mod. Phys. **81**, 1301-1350 (2009). (cited on pages 1 and 49)

7. N. Gisin, G. Ribordy, W. Tittle and H. Zbinden, *Quantum cryptography*, Rev. Mod. Phys. **74**, 145-196 (2002). (cited on pages 1 and 49)

8. C. Bennet & G. Brassard, *Public Key Distribution and Coin Tossing*, Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, New York,1984, pp.175-179. (cited on pages 1, 49, 51, and 52)

9. A. K. Ekert, *Quantum Cryptography Based on Bell's Theorem*, Phys. Rev. Lett. **67**, 661 (1991). (cited on pages 1, 49, 52, and 53)

10. P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier and E. Diamanti, *Experimental demonstration of long-distance continuous-variable quantum key distribution*, Nature Photonics. **7**,378-381 (2013). (cited on pages 1, 50, 84, and 95)

11. M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, J.F. Dynes, S.Fasel, S. Fossier, M. Fürst, J-D Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G.Humer, T. Länger, M. Lergé, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J-B Page, A. Poppe, E.

Querasser, G. Ribordy, S. Robyr, L. Salvail, A.W.Sharpe, A.J.Shields. D. Stucki, M. Suda, C. Tamas, T. Themel, R.T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R.Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden and A. Zeilinger ,*The SECOQC quantum key distribution network in Vienna*, New J. Phys. **11**,075001 (2009). (cited on pages 1 and 50)

12. M.Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M.Peev and A. Zeilinger ,*Field test of quantum key distribution in the Tokyo QKD Network*, Opt. Express. **11**, 10387-10409 (2011). (cited on pages 1 and 50)

13. D. Mayers & A. Yao, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science, Palo Alto, 1998* (IEEE, Washington, DC,1998), p. 503. (cited on pages 1, 53, and 61)

14. A. Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio and Valerio Scarani, *Device-Independent Security of Quantum Cryptography against Collective Attacks*, Phys. Rev. Lett. **98**, 230501 (2007). (cited on pages 1, 54, and 61)

15. B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin and P. G. Kwiat,*Detection-Loophole-Free Test of Quantum Nonlocality, and Applications* , Phys. Rev. Lett. **111**, 130406 (2013). 28. (cited on pages 1 and 50)

16. M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, Jörn Beyer, A. Lita, B. Calkins, T. Gerrits, S. W. Nam, R. Ursin and A. Zeilinger, *Bell violation using entangled photons without the fair-sampling assuption*, Nature **497**, 227-ĂŞ230 (2013). (cited on pages 1 and 50)

17. H. M. Wiseman, S. J. Jones and A. C. Doherty,*Steering, Entanglement, Nonlocality, and the Einstein-Podolsky-Rosen Paradox*, Phys. Rev. Lett. **98**, 140402 (2007). (cited on pages 1, 58, 69, and 70)

18. M. Tomamichel & R. Renner, *The Uncertainty Relation for Smooth Entropies*, Phys. Rev. Lett. **106**, 110506 (2011). (cited on pages 1, 58, and 61)

19. C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani and H. M. Wiseman, *One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering*, Phys. Rev. A. **85**, 010301(R) (2012). (cited on pages 1, 58, 61, 71, and 72)

20. M.Berta, M. Christandl, R. Colbeck, J. M. Renes and R. Renner, *The Uncertainty Principle in the Presence of Quantum Memory*, Nature. Phys **6**, 659 (2010). (cited on pages 1, 56, 61, 62, and 63)

21. I. Bialynicki-Birula & J.Mycielski, *Uncertainty Relations for Information Entropy in Wave Mechanics*, Commun. Math. Phys. **44**, 129-132(1975). (cited on pages 2, 61, and 62)

22. D. Deutsch, *Uncertainty in Quantum Mechanics*, Phys. Rev. Lett. **50**, 631-633 (1983). (cited on pages 2, 61, and 62)

23. K.Kraus, *Complementary observables and uncertainty relations*, Phys. Rev. D. **35**, 3070-3075 (1987). (cited on pages 2, 61, and 62)

24. H. Maassen & J.B. Uffink, *Generalized Entropic Uncertainty Relations*, Phys. Rev. Lett. **60**,1103-1106 (1988). (cited on pages 2, 61, and 62)

25. M. Hall. Phys. Rev. Lett. **74**, 3307-311 (1995). (cited on pages 2, 61, and 62)

26. F. Furrer, M. Berta, M. Tomamichel, V. B. Scholz and M. Chirstandl,*Position-Momentum Uncertainty Relations in the Presence of Quantum Memory*, Journal of Mathematical Physics **55**, 122205 (2014). (cited on pages 2, 61, and 63)

27. R. L. Frank & E. H. Lieb. Communications In Mathematical Physics **323**, 487-495 (2014). (cited on pages 2, 61, and 63)

28. A. Ferenczi, *Security proof methods for quantum key distribution protocols*, PhD Thesis, University of Waterloo (2013). (cited on pages 2 and 63)

29. L. Henderson & V. Vedral, *Classical, quantum and total correaltions*, J.Phys. A: Math. Gen **34**, 6899-6905 (2001). (cited on pages 2, 24, 25, and 33)

30. H. Ollivier & W. H. Zurek, *Quantum Discord: A Measure of the Quantumness of Correlations* , Phys. Rev. Lett. **88**, 017901 (2001). (cited on pages 2, 24, 25, 29, and 31)

31. Mark Fox. *Quantum Optic,An Introduction*, (Oxford University Press, Oxford, 2006). (cited on pages xvii, 7, 9, 12, 13, and 14)

32. G. Adesso, S. Ragy and A. R. Lee, *Continuous Variable Quantum Information: Gaussian States and Beyond* , Open Syst.Inft.Dyn.**21** 1440001 (2014). (cited on pages 9, 15, 16, and 17)

33. Gerardo Adesso, *Entanglement of Gaussian States*. PhD Thesis, Universitá Degli Studi Di Salerno (2006). (cited on pages 17, 26, 27, and 28)

34. H-A. Bachor & T.C. Ralph, *A Guide to Experiments in Quantum Optics*, WILEY-VCH (2003). (cited on page 22)

35. Paolo Giorda and Matteo G A Paris, *Gaussian quantum discord*, Phys. Rev. Lett. **105**, 020503 (2010). (cited on pages 17, 32, 33, and 34)

36. N. Brunner, N. Gisin and V. Scarani, *Entanglement and non-locality are different resources*, New J. Phys. **7**, 88 (2005). (cited on page 26)

37. J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics*, (Cambridge University Press, Cambridge, 1987). (cited on page 26)

38. D.F. Walls & G.J. Milburn. *Quantum Optics*, (Springer-Verlag Berlin Heidelberg, 1994). (cited on pages 7, 8, 10, 11, 12, and 13)

39. U. Leonhardt, *Measuring the Quantum State of Light* (Cambridge University Press, Cambridge, 1997). (cited on pages 9, 10, 12, 13, 14, 15, 19, 20, 35, 43, and 92)

40. W. B. Case, *Wigner functions and Weyl transformations for pedestrians* , Am. J. Phys. **76**, Issue 10, pp.937-946 (2008). (cited on page 14)

41. G. Adesso & F. Illuminati, *Entanglement in continuous-variable system: recent advances and current perspectives* , J. Phys. A: Math. Theor. **40**, 7821 (2007).

42. M. Nielson and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2010). (cited on pages 18, 22, 23, 24, 26, and 27)

43. Oldrich Vasicek, *A Tast for Normality Based on Sample Entropy*, Journal of the Royal Statistical Society, Series B, **38** (1), (1976). (cited on page 23)

44. K. Modi, A. Brodutch, Hugo Cable, Tomasz Paterek, Vlatke Vedral , *The classical-quantum boundary for correlations: Discord and related measures* , Rev. Mod. Phys. **84**, 1655-1707 (2012). (cited on pages 24, 25, and 31)

45. K. Modi & V. Vedral, *Unification of quantum and classical correlations and quantumness measures* , AIP Conf. Proc. 1384, 69-75 (2011). (cited on page 23)

46. M. D. Reid and P. D. Drummond, *Quantum Correlations of Phase in Nondegernerate Parametric Oscillation* , Phys. Rev. Lett. **60**, 2731 (1988). (cited on page 28)

47. M. D. Reid, *Demonstration of the Einstein-Podolsky-Rosen paradox using nondegenerate parametric amplification*, Phys. Rev. A **40**, 913 (1989). (cited on pages 28, 64, 70, and 81)

48. L. M. Duan, G. Giedke, J. I. Cirac and P. Zoller, *Inseparability Criterion for Continuous Variable Systems*, Phys. Rev. Lett **84**, 2722 (2000). (cited on page 28)

49. J. Janousek, *Investigation of non-classical light and its application in ultrasensitive measurements*. PhD Thesis, Technical University of Denmark (2007). (cited on pages 28, 76, and 81)

50. E. Knill & R. Laflamme, *Power of One Bit of Quantum Information* , Phys. Rev. Lett. **81**, 5672 (1998). (cited on page 31)

51. A. Datta, S.T. Flammia and C. M. Caves, *Entanglement and the power of one qubit*, Phys. Rev. A **72**, 042316 (2005). (cited on page 31)

52. A. Datta, A. Shaji and C. M. Caves, *Quantum Discord and the Power of One Qubit*, Phys. Rev. Lett. **100**, 050502 (2008). (cited on page 31)

53. V. Madhok & A. Datta, *Interpreting quantum discord through quantum state merging*, Phys. Rev. A **83**, 032323 (2011). (cited on page 31)

54. D. Cavalcanti, L. Aolita, S. Boixo, K. Modi, M. Piani and A. Winter, *D. Cavalcanti, L. Aolita, S. Boixo, K. Modi, M. Piani, and A. Winter* , Phys. Rev. A **83**, 032324 (2011). (cited on page 31)

55. M. Gu, H. M. Chrzanowski, S. M. Assad, T. Symul, K. Modi, T. C. Ralph, V. Vedral and P.K. Lam, *Observing the operational significance of discord consumption* ,Nature Phys. **8**, 032324 (2011). (cited on page 31)

56. B. Dakić, Y. O. Lipp, X. Ma, M. Ringbauer, S. Kropatschek, S. Barz, T. Paterek, V. Vedral, A. Zeilinger, C. Brukner, P. Walther, *Quantum discord as resource for remote state preparation* , Nature Phys. **8**, 666-670 (2012). (cited on page 31)

57. G. Adesso & A. Datta, *Quantum versus Classical Correlations in Gaussian States* , Phys. Rev. Lett. **105**, 030501 (2010). (cited on pages 32 and 33)

58. R. Tatham, L. Mista, Jr., G. Adesso and N. Korolkova, *Nonclassical correlations in continuous-variable non-Gaussian Werner states*, Phys. Rev. A **85**, 022326 (2012). (cited on page 32)

59. C. Weedbrook, S. Pirandola, J. Thompson, V. Vedral, M. Gu, *Discord Empowered Quantum Illumination* , arXiv:1312.3332v1 (2013). (cited on page 32)

60. D. Girolami, A. M. Souza, V. Giovannetti, T. Tufarelli, J. G. Filgueiras, R. S. Sarthour, Diogo O. Soares-Pinto, Ivan S. Oliveira, and Gerardo Adesso, *Quantum Discord Determines the Interferometric Power of Quantum States* , Phys. Rev. Lett. **112**, 210401 (2014). (cited on page 32)

61. S. Pirandola, *Quantum discord as a resource for quantum cryptography* , Sci. Rep. **4**, 6956 (2014). (cited on page 32)

62. J. Ma, B. Yadin, D. Girolami, V. Vedral, M. Gu, *Converting Coherence to Quantum Correlations* , arXiv:1510.06179v1 (2015). (cited on page 32)

63. B. Yadin, J. Ma, D. Girolami, M. Gu, V. Vedral, *Quantum processes which do not use coherence* , arXiv:1512.02085v1 (2015). (cited on page 32)

64. R. Rahimi & A. SaiToh, *Single-experiment-detectable nonclassical correlation witness* , Phys. Rev. A **82**, 022314 (2010). (cited on page 32)

65. B. Bylicka & D. Chruściński, *Witnessing quantum discord in* $2 \times N$ *systems* , Phys. Rev. A **81**, 062102 (2010). (cited on page 32)

66. B. Dakić, V. Vedral & C. Brukner, *Necessary and Sufficient Condition for Nonzero Quantum Discord* , Phys. Rev. Lett. **105**, 190502 (2010). (cited on page 32)

67. L. Chen, E. Chitambar, K. Modi & G. Vacanti, *Detecting multipartite classical states and their resemblances*, Phys. Rev. A **83**, 020101 (2011). (cited on page 32)

68. Chengjie Zhang, Sixia Yu, Qing Chen, and C. H. Oh, *Detecting the quantum discord of an unknown state by a single observable*, Phys. Rev. A **84**, 032122 (2011). (cited on page 32)

69. D. Girolami & G. Adesso, *Observable Measure of Bipartite Quantum Correlations* , Phys. Rev. Lett. **108**, 150403 (2012). (cited on page 32)

70. J. Maziero & R. M. Serra, *Classicality Witness for two-qubit states* , Int. J. Quant. Inf. **10**, 1250028 (2012). (cited on page 32)

71. R. Auccaise, J. Maziero, L. C. Céleri, D. O. Soares-Pinto, E. R. deAzevedo, T. J. Bonagamba, R. S. Sarthour, I. S. Oliveira, and R. M. Serra, *Experimentally Witnessing the Quantumness of Correlations* , Phys. Rev. Lett. **107**, 070501 (2011). (cited on page 32)

72. G. Passante, O. Moussa, D. A. Trottier, and R. Laflamme, *Experimental detection of nonclassical correlations in mixed-state quantum computation* , Phys. Rev. A **84**, 044302 (2011). (cited on page 32)

73. G. H. Aguilar, O. Jiménez Farías, J. Maziero, R. M. Serra, P. H. Souto Ribeiro, and S. P. Walborn, *Experimental Estimate of a Classicality Witness via a Single Measurement* , Phys. Rev. Lett. **108**, 063601 (2012). (cited on page 32)

74. S. Rahimi-Keshar, C. M. Caves and T. C. Ralph, *Measurement-based method for verifying quantum discord* , Phys. Rev. A **87**, 012119 (2013). (cited on pages 32, 33, 34, 35, 37, and 44)

75. R. Blandino, M. G. Genoni, J. Etesse, M. Barbieri, M. G. A. Paris, P. Grangier and R. Tualle-Brouri, *Homodyne Estimation of Gaussian Quantum Discord* , Phys. Rev. Lett. **109**, 180402 (2012).

76. U. Vogl, R. T. Glasser, Q. Glorieux, J. B. Clark, N. V. Corzo and P. D. Lett, *Experimental characterization of Gaussian quantum discord generated by four-wave mixing* ,Phys. Rev. A **87**, 010101 (2013).

77. L. S. Madsen , A. Berni, M. Lassen and U. L. Andersen, *Experimental Investigation of the Evolution of Gaussian Quantum Discord in an Open System*, Phys. Rev. Lett. **109**, 030402 (2012).

78. A. Meda, S. Olivares, I. P. Degiovanni, G. Brida, M. Genovese, and M. G. A. Paris, *Revealing interference by continuous variable discordant states*, Optics Letters **38**, 3099 (2013).

79. E. Prugovečki, *Information-theoretical aspects of quantum measurement* , Int. J. Theor. Phys. **16**, 321 (1977). (cited on page 34)

80. P. Busch, *Informationally complete sets of physical quantities*, Int. J. Theor. Phys. **30**, 1217 (1991). (cited on page 34)

81. M. D. Lang, C. M. Caves, A. Shaji, *Entropic measures of non-classical correlations*, Int. J. Quant. Inf. **9**, 1553 (2011).

82. M. S. Kim, W. Son, V. Buzek, and P. L. Knight, *Entanglement by a beam splitter: Nonclassicality as a prerequisite for entanglement* , Phys. Rev. A **65**, 032323 (2002). (cited on page 36)

83. W. Xiang-bin, *Theorem for the beam-splitter entangler* , Phys. Rev. A **66**, 024303 (2002). (cited on page 36)

84. R. J. Glauber, *Photon Correlations* , Phys. Rev. Lett. **10**, 84 (1963). (cited on page 37)

85. E. C. G. Sudarshan, *Equivalence of Semiclassical and Quantum Mechanical Descriptions of Statistical Light Beams* , Phys. Rev. Lett. **10**, 277 (1963). (cited on page 37)

86. R. W. P. Drever, J. L. Hall, F. V. Kowalski, J. Hough, G. M. Ford, A. J. Munley, H. Ward , *Laser phase and frequency stabilization using an optical resonator*, Appl. Phys. B: Photophys. Laser Chem. **31**, 97-105 (1983). (cited on page 39)

87. E. D. Black, *An introduction to Pound-Drever-Hall laser frequency stabilization*, Am. J. Phys. **69** (1), (2001). (cited on page 39)

88. J. W. Wu, P. K. Lam, M. B. Gray, and H.-A. Bachor, *Optical homodyne tomography of information carrying laser beams*, Optics Express **3**, 154 (1998). (cited on page 44)

89. Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón, Nicolas J. Cerf, Timothy C. Ralph, Jeffrey H. Shapiro, Seth LIoyd, *Gaussian quantum information*, Rev. Mod. Phys. **84**, 621, (2012). (cited on pages 50, 51, and 64)

90. F. Grosshans, N. J. Cerf, J. Wenger, R. Tualla-Brouri, P. Grangier, *Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables*, Quantum Inf. Comput. **3**, 535-552 (2003). (cited on pages 51, 64, and 91)

91. F. Grosshans & P. Grangier, *Continuous Variable Quantum Cryptography Using Coherent States*, Phys.Rev.Lett. **88**, 057902 (2002). (cited on pages 49 and 51)

92. P. W. Shor & J. Preskill, *Simple Proof of Security of the BB84 Quantum Key Distribution Protocol*, Phys.Rev.Lett. **85**, 441 (2000). (cited on page 49)

93. T. C. Ralph, *Continuous variable quantum cryptography*, Phys. Rev. A.**61**, 010303 (1999). (cited on pages 49 and 64)

94. G. Brassard, N. Lútkenhaus, T. Mor and B. C. Sanders, *Limitations on Practical Quantum Cryptography*, Phys. Rev. Lett. **85**, 1330 (2000).

95. C-H. F. Fung, B. Qi, K. Tamaki,and H-K. Lo, *Phase-remapping attack in practical quantum-key-distribution systems* , Phys. Rev. A. **75**,032314 (2007). (cited on page 50)

96. F. Xu, B. Qi and H-K Lo, *Experimental demonstration of phase remapping attack in a practical quantum key distribution system*, New J. Phys. **12**, 113026 (2010). (cited on page 50)

97. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar and Vadim Makarov, *Hacking commercial quantum cryptography systems by tailored bright illumination* , Nature Photonics. **4**, 686 (2010). (cited on page 50)

98. Y. Zhao, C-H. F. Fung, B. Qi, C. Chen and H-K Lo, *Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems*, Phys. Rev. A **78**, 042333 (2008). (cited on page 50)

99. S. Pironio , A. Acín, N. Brunner, N. Gisin, S. Massar and V. Scarani, *Device-independent quantum key distribution secure against collective attacks*, New J. Phys. **11**, 045021 (2009). (cited on pages 51, 52, 53, 54, and 55)

100. A. Acín, N. Gisin, and L. Masanes, *From Bell's Theorem to Secure Quantum Key Distribution*, Phys. Rev. Lett. **97**, 120405 (2006). (cited on pages 52 and 54)

101. J. Barrett, L. Hardy and A. Kent, *No Signaling and Quantum Key Distribution*, Phys. Rev. Lett. **95**, 010503 (2005). (cited on page 52)

102. J. Barrett, L. Hardy and A. Kent, *No Signaling and Quantum Key Distribution*, Phys. Rev. Lett. **95**, 010503 (2005). (cited on pages 53 and 54)

103. A. Acín, S. Massar and S. Pironio, *Efficient quantum key distribution secure against no-signalling eavesdroppers*, New J. Phys. **8**, 126 (2006). (cited on page 54)

104. V. Scarani, N. Gisin, N. Brunner, L. Masanes, S. Pino and A. Acín, *Secrecy extraction from no-signaling correlations* , Phys. Rev. A. **74**, 042339 (2006). (cited on page 54)

105. M. McKague. New J.Phys. **11**, 103037 (2009). (cited on page 54)

106. L. Masanes, S. Pironio and A. Acín, *Secure device-independent quantum key distribution with causally independent measurement devices*, Nature Comm. **2**, 238 (2011). (cited on page 54)

107. J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics*, Cambridge Univ. Press, Cambridge, (1987). (cited on page 55)

108. N. Gisin, S. Pironio and N. Sangouard, *Proposal for Implementing Device-Independent Quantum Key Distribution Based on a Heralded Qubit Amplifier*, Phys. Rev. Lett. **105**, 070501 (2010). (cited on page 55)

109. T.C.Ralph and A.P. Lund, *Nondeterministic Noiseless Linear Amplification of Quantum Systems* , in Quantum Measurement and Computing Proceedings of 9th International Conference, Ed. A. Lvovsky, pp 155 (AIP,New York 2009); arXiv:0809.0326. (cited on pages 55 and 114)

110. C. C. W. Lim, C. Portmann, M. Tomamichel, R. Renner, and N. Gisin, *Device-Independent Quantum Key Distribution with Local Bell Test* , Phys. Rev X. **3**, 031006 (2013). (cited on page 55)

111. U. Vazirani & Thomas Vidik, *Fully Device-Independent Quantum Key Distribution*, Phys. Rev. Lett. **113**, 140501 (2014). (cited on page 55)

112. C. J. Broadbent, K. Marshall, C. Weedbrook, J. C. Howell, *Device-independent quantum key distribution with generalized two-mode Schrödinger cat states* ,arXiv:1503.01688v1, (2015). (cited on page 55)

113. H-K. Lo, M. Curty and B. Qi, *Measurement-Device-Independent Quantum Key Distribution* , Phys. Rev. Lett. **108**, 130503 (2012). (cited on page 56)

114. S. Abruzzo, H. Kampermann and Dagmar BruSS, *Measurement-device-independent quantum key distribution with quantum memories*, Phys. Rev. A. **89**, 012301 (2014). (cited on page 56)

115. C. Panayi, M. Razavi, X. Ma and N. Lütkenhaus, *Memory-assisted measurement-device-independent quantum key distribution*, New. J. Phys. **16**, 043005 (2014). (cited on page 56)

116. M. Curty, F. Xu, W. Cui, C. C. W Lim, K. Tamaki and H-K. Lo, *Finite-key analysis for measurement-device-independent quantum key distribution* , Nature Comm. **5**, 3732 (2014). (cited on page 57)

117. Y. Liu, T-Y. Chen, L-J. Wang, H. Liang, G-L. Shentu, J. Wang, K. Cui, H-L. Yin, N-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C-Z. Peng, Q. Zhang and J-W. Pan, *Experimental Measurement-Device-Independent Quantum Key Distribution*, Phys. Rev. Lett. **111**, 130502 (2013). (cited on page 57)

118. Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian and H-K.Lo, *Experimental Demonstration of Polarization Encoding Measurement-Device-Independent Quantum Key Distribution*, Phys. Rev. Lett. **112**, 190503 (2014). (cited on page 57)

119. S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen and U. L. Andersen , *High-rate measurement-device-independent quantum cryptography* , Nature Photonics. **9**, 397-402 (2015). (cited on page 57)

120. M. Pawlowski & N. Brunner, *Semi-device-independent security of one-way quantum key distribution*, Phys. Rev. A. **84**, 010302(R) (2011). (cited on page 57)

121. A. Einstein, B. Podolsky and N. Rosen, *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*, Phys. Rev. **47**, 777-780 (1935).

122. N. Walk, S. Hosseini, J. Geng, O. Thearle, J. Y. Haw, S. Armstrong, S. M. Assad, J. Janousek, T. C. Ralph, T. Symul, H. M. Wiseman and P. K. Lam. *Experimental Demonstration of Gaussian Protocols for one-sided device independent quantum key distribution*. Optica **3**(6), 634-642 (2016). (cited on page 67)

123. I. Devetak & A. Winter, Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **461**, 207-235 (2005). (cited on page 63)

124. M. Berta, F. Furrer, V. B. Scholz, *The Smooth Entropy Formalism for von Neumann Algebras* , arXiv:1107.5460 (2011). (cited on page 63)

125. M. Hillery, *Quantum cryptography with squeezed states*, Phys. Rev. A **61**, 022309 (2000). (cited on page 64)

126. F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf and P. Grangier, *Quantum key distribution using gaussian-modulated coherent states*, Nature **421**, 238-241 (2003). (cited on page 64)

127. C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph and P. K. Lam, *Quantum Cryptography Without Switching*, Phys. Rev. Lett **93**, 170504 (2004). (cited on page 64)

128. R. Renner & J. I. Cirac, *de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography*, Phys. Rev. Lett **102**, 110504 (2009). (cited on page 65)

129. R. García-Patrón & N. J. Cerf, *Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution* , Phys. Rev. Lett **97**, 190503 (2006). (cited on page 65)

130. M. Navascués, F. Grosshans & A Acín, *Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography*, Phys. Rev. Lett **97**, 190502 (2006). (cited on page 65)

131. D. J. Saunders , S. J. Jones, H. M. Wiseman and G. J. Pryde, *Experimental EPR-steering using Bell-local states*, Nature Phys **6**, 845-849 (2010). (cited on page 70)

132. T. Gehring, V. Händchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R. F. Werner and R. Schnabel, *Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks*, Nature Comm. **6**, 8795 (2015). (cited on pages 74, 84, and 95)

133. G. D. Boyd & D. A. Kleinman, *Parametric Interaction of Focused Gaussian Light Beams* , J. Appl. Phys,39:3597 (1968). (cited on page 76)

134. S. Armstrong, *Experiments in Quantum Optics: Scalable Entangled States and Quantum Computation with Cluster States*. PhD Thesis, Australian National University (2014). (cited on page 84)

135. P. Jouguet, S. Kunz-Jacques and A. Leverrier, *Long-distance continuous-variable quantum key distribution with a Gaussian modulation* , Phys. Rev A. **84**, 062317 (2011). (cited on pages 84 and 95)

136. T. Eberle , S. Steinlechner, J. Bauchrowitz, V. Händchen, H. Vahlbruch, M. Mehmet, H. Müller-Ebhardt and R. Schnabel, *Quantum Enhancement of the Zero-Area Sagnac Interferometer Topology for Gravitational Wave Detection*, Phys. Rev. Lett. **104**, 251102 (2010). (cited on page 87)

137. B. M. Sparks, H. M. Chrzanowski, D. P. Parrain, B. C. Buchler, P. K. Lam, T. Symul, *A Scalable, Self-Analyzing Digital Locking System for use on Quantum Optics Experiments* , Rev. Sci. Instrum. 82, 075113 (2011). (cited on page 94)

138. D. Bohm & Y. Aharonov, *Discussion of Experimental Proof for the Paradox of Einstein, Rosen, and Podolsky*, Phys. Rev. **108**, 1070 (1957). (cited on page 101)

139. J. F. Clauser, M. A. Horne, A. Shimony and R. A. Holt, *Proposed Experiment to Test Local Hidden-Variable Theories*, Phys. Rev. Lett. **23** (15):880-4 (1969). (cited on pages 103 and 104)

140. Alain Aspect, Philippe Grangier and Gérard Roger, *Experimental Tests of Realistic Local Theories via Bell's Theorem*, Phys. Rev. Lett. **47** (7):460-3 (1981). (cited on pages 103 and 104)

141. G. Y. Xiang, T. C. Ralph, A. P. Lund, N. Walk and G. J. Pryde, *Heralded noiseless linear amplification and distillation of entanglement* , Nature Photon. **4**, 316-319 (2010). (cited on page 114)

142. H. M. Chrzanowski, N. Walk, S. M. Assad, J. Janousek, S. Hosseini, T. C. Ralph, T. Symul and P. K. Lam, *Measurement-based noiseless linear amplification for quantum communication* , Nature Photon. **8**, 333-338 (2014). (cited on page 114)

143. F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel and R. F. Werner, *Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks*, Phys. Rev. Lett. 109, 100502 (2012). (cited on page 114)

144. J. Y. Haw, S. M. Assad, A.M. Lance, N. H. Y. Ng, V. Sharma, P. K. Lam and T. Symul, *Maximization of Extractable Randomness in a Quantum Random-Number Generator*, Phys. Rev. Applied. **3**, 054004, (2015). (cited on page 114)