Application of Polarisation and Phase in Quantum Information

A thesis submitted in partial fulfilment of

the requirements for the degree of

Doctor of Philosophy

by

Anju Rani

(Roll No. 18330002)

Under the supervision of

Prof. R. P. Singh

Professor

Atomic, Molecular and Optical Physics Division

Physical Research Laboratory, Ahmedabad, India

DISCIPLINE OF PHYSICS

INDIAN INSTITUTE OF TECHNOLOGY GANDHINAGAR

2023

To

My Father

DECLARATION

I declare that this written submission represents my ideas in my own words and where others' ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Signature

Name: Anju Rani

(Roll No: 18330002)

Date: 01/04/2024

CERTIFICATE

It is certified that the work contained in the thesis titled **"Application of Polarisation and Phase in Quantum Information"** by Ms. Anju Rani (Roll No. 18330002) has been carried out under my supervision and that this work has not been submitted elsewhere for a degree.

I have read this dissertation, and in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.

Prof. R. P. Singh
Professor
Atomic, Molecular and Optical Physics Division,
Physical Research Laboratory,
Ahmedabad, India.

(Thesis Supervisor)

Date: 01/04/2024

Thesis Approval

The thesis entitled

Application of Polarisation and Phase in Quantum Information

by

Anju Rani

(Roll No. 18330002)

is approved for the degree of

Doctor of Philosophy

Examiner	Examiner
Supervisor	Chairman

Date: _____

Place: _____

Acknowledgments

It's been five years since the day I joined PRL and the journey of my PhD comes to its end. My time in PRL is grateful to a number of people and the completion of my research would not have been possible without the contribution of each of them. I take this opportunity to extend my sincere gratitude to each of them.

First and foremost, I want to express my eternal gratitude to my Papa, Shri Rohtash Sharma. Whatever I am today and whatsoever I have achieved in my life is all because of you. Your countless efforts, hard work, and never-ending faith in me make this day happen. I really don't know how to put my words to express my gratitude and respect for you. I can just say, thank you Papa for everything and I Love you, Papa.

It brings me immense joy to express my eternal gratitude to my supervisor, Prof. R. P. Singh for his continuous guidance and encouragement throughout my research journey. Having you as my supervisor has been a true blessing. Your simplicity in both personal and professional aspects of life has been a great inspiration. Throughout my journey, you have been more than just a thesis supervisor; you have been a mentor, a guide, and a friend. Though there were many tough times, but you always believed in me. Your valuable suggestions and critical comments have helped me to improve in all aspects of my life. Your constant guidance, inspiration, encouragement, and motivation during this entire period helped me at various stages of this research journey. Your impact on my life and research is truly immeasurable, and I am forever grateful to have had you by my side.

I am also immensely grateful to Prof. Goutam K. Samanta, Prof. Mudit K. Srivastava, and Prof. Partha Konar for their valuable contributions as members of my Doctoral Supervisory Committee (DSC). Their insights, suggestions, and constructive criticisms have greatly enhanced the quality of this thesis. Their expertise and scholarly guidance have been instrumental in shaping my research. I am thankful to all DSCs for providing me with unending support and their friendly behavior, which always kept me motivated for my thesis work.

I am also thankful to all the Academic Committee members for their insightful comments and encouragement during my research period. I express my sincere gratitude to all the faculty members of PRL who had taught me during the course work and inspired me to pursue research. They provided an overall view of research works carried out in PRL, which helped me to have a brief knowledge about different fields of sciences. I am very grateful to the Di-

rector, Prof. Anil Bhardwaj; Dean, Prof. D. Pallamraju; and Head of Academic Services, Dr. Bhushit Vaishnav for their constant assistance during my Ph.D. tenure. I would take this opportunity to also thank the people from accounts, purchase, library, computer center, administration, canteen, CMD, dispensary, transport, and housekeeping sections for all the help they have provided me during my Ph.D. tenure. I also take this moment to express my gratitude to the academic and administrative staff members of IIT Gandhinagar for helping with the registration procedures. I would also like to extend my special regards to all my teachers who taught me at different stages of my career. Because of their teaching, it is possible for me to reach a stage where I could write this thesis.

I would like to thank my group members Ali, Nijil, Anindya, Ayan, Sarika, Satyajeet, Pravin, Suryansh, Tanya, Vardaan, Shashi, Unnati, and Rachita for all the discussions. They were always present for moral support and helped in creating a fun-loving working atmosphere. I thank our engineers' team Pooja Chandravanshi, Jayanth R., Rutuj Gharate, and Jaya Krishna Meka who have closely worked with me and helped me in troubleshooting the challenges in experiments. I thank Varun, Subith, Anirban, Vimlesh, Sandeep, Soumya, and Chahat for all the constructive discussions. I thank Dr. Rupesh for the discussion and the time he took out for me. I thank my collaborator Madhusudan P. for the discussions and the times we worked together. I thank the visitors in our group Pranav Tiwari, Raghu, and Parvatesh for their help.

I am grateful to Dayanand Mishra, Naval, Deva, Vikas, Sunil, Akanksha, Pranav, Namita, and Yash for their friendship and positive support throughout my Ph.D. journey. Their companionship, encouragement, and understanding have made this experience more enjoyable and fulfilling.

To Yogesh, Meghna, Deepak Gaur, Nabo, Deepak Kumar Rai, Harish, Shivani, Partha, Shanvali, Sana, and Monika, I express my gratitude for being wonderful friends who have provided unwavering support and shared many memorable moments. I would like to acknowledge Chahat, Arti, Mehul, Subhender, and Neha for being cool and friendly.

Besides, I would like to acknowledge my friend from Panjab University, Prawal Sharma. Thank you for your constant support and love for me. I feel pleasure to thank Munish for his companion and continuous support throughout the journey. I thank Priya and Kittu for their love and support.

When it comes to family, words are never enough to express the feeling of love, gratefulness, and regard. Still, I want to express my eternal gratitude to my parents, Shri. Rohtash Sharma and Smt. Sunita Sharma. You are my entire world, my motivation, encouragement, and everything. Thanks for your endless efforts, love, and care. My thesis will be incomplete if I don't express my love and thanks to the most beloved person in my life my brother Vishal and sister Manju. You are not only my brother and sister but my best friends ever. Without your support, it would not be easy for me to reach this point in my life. Your love and encouragement have given me the strength to persevere.

Last but certainly not least, I would like to extend my sincere thanks to all those individuals whom I may have inadvertently omitted from this acknowledgment. Your contributions, support, and positive impact on my journey have been truly invaluable. Please know that your involvement and assistance have played a significant role in shaping the successful completion of this Ph.D. thesis. Thank you all for your invaluable contributions and for being part of this significant milestone in my academic career.

Anju Rani

Abstract

This thesis explores the field of quantum communication and focuses on Quantum Key Distribution (QKD) protocols. As technology and computer science advancements continue to revolutionize communication, the need for secure communication has become more pressing. Classical cryptography faces challenges in providing provable security. Quantum communication, specifically QKD, offers an alternative approach to ensure unconditional security and track eavesdroppers in real-time.

The thesis delves into both discrete variable (DV) QKD using polarization and continuous variable (CV) QKD protocols using phase. The entanglement-based DVQKD protocols are proven to be more secure than the prepare and measure protocols but require more resources than a typical BB84. To strike a balance between security and resources, the thesis implements the BB84 protocol using a heralded single-photon source, requiring fewer resources and providing enhanced security. Our method uses a single-photon source, making the approach more efficient and secure than using weak coherent pulses. The protocol eliminates the need for an external random number generator for random polarization state preparation, instead, a beam splitter (BS) performs the random selection task. However, DVQKD protocols suffer disadvantages in the form of the requirement for single photon sources and detectors. These limitations restrict the rate of key exchange as well as open the QKD protocols to various attacks by an eavesdropper.

In contrast, CVQKD protocols bypass such stringent requirements by exchanging single photons with weak coherent states and single photon detectors with photodiodes. The CVQKD approach offers several evident advantages. These advantages include cost reduction, higher secure key generation rates, and scalability. The thesis

explores various classes of CVQKD protocols over free space, motivated by free space advantages such as reduced optical losses, and polarization insensitivity.

In this thesis, we have implemented various classes of CVQKD protocols over free space which include, discrete modulation and Gaussian modulation CVQKD. Free space offers various advantages over fiber, as the optical losses are less in free space compared to fiber. In addition, the free space channel is insensitive to polarization compared to fiber, which results in light polarization being nearly unchanged during propagation. The presence of Eve in the line of sight could be detected easily. In addition to this, compared to fiber CVQKD, atmospheric link offers the possibility of broader geographical coverage and more flexible transmission.

The work involves characterizing the CVQKD setup, accounting for imperfections that can impact the key rate, and conducting both laboratory and field demonstrations. Simulation results are used to verify experimental values, and free space field studies assess the feasibility of CVQKD for satellite-based applications. Despite challenges faced in the field, the results demonstrate the potential of CVQKD as an efficient and secure quantum communication solution.

Overall, this thesis contributes to the growing field of quantum communication by implementing and analyzing various QKD protocols, paving the way for practical applications in secure communication systems.

Keywords: Quantum Cryptography, Quantum Communication, Quantum Key Distribution, Discrete Variable, Continuous Variable, Discrete Modulation, Gaussian Modulation, BB84 Protocol, Heralded Photons, Balanced Homodyne Detection.

Abbreviations

BS	Beam Splitter
EB QKD	Entanglement Based Quantum Key Distribution
DV QKD	Discrete Variable Quantum Key Distribution
CV QKD	Continuous Variable Quantum Key Distribution
DM CV QKD	Discrete modulation Continuous Variable Quantum Key Distribution
GM CV QKD	Gaussian modulation Continuous Variable Quantum Key Distribution
OHT	Optical Homodyne Tomography
BHD	Balanced Homodyne Detection
PD	Photodetectors
EPS	Entangled Photon Source
EC	Error Correction
FC	Fiber Coupler
FPGA	Field Programmable Gate Array
HWP	Half Wave Plate
MI	Mutual Information
PA	Privacy Amplification
PBS	Polarizing Beam Splitter
PE	Parameter Estimation
P&M QKD	Prepare & Measure Quantum Key Distribution
QKD	Quantum Key Distribution
QBER	Quantum Bit Error Rate
QWP	Quarter Wave Plate
RNG	Random Number Generator
SPDC	Spontaneous Parametric Down Conversion
SPCM	Single Photon Counting Module
SPS	Single Photon Source
SLM	Spatial Light Modulator
PSE	Post Selection Efficiency
AM	Amplitude Modulator
PM	Phase Modulator

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Nature encompasses a wide range of scales, each with its own set of questions to explore. When we look at extremely small scales, smaller than the Compton wavelength, we enter the realm of Quantum Mechanics (QM). Despite significant advancements in our understanding of QM through both theory and experiments, we are still in the process of fully comprehending it. At the quantum level, things can get quite complicated. The way physical quantities behave here is very different from our everyday experiences. Some of the surprising predictions of QM include the uncertainty principle, which says we can't know certain properties of particles with complete accuracy and entanglement, where particles can be connected in ways that seem impossible based on our classical intuition. In the quantum world, individual particles can act in peculiar ways, and this is one of the unique features of QM.

Quantum physics possesses unique characteristics that lay the foundation for Quantum Key Distribution (QKD), which is one of its most ubiquitous applications. Alongside quantum mechanics, quantum information theory has rapidly expanded, giving

birth to the fields of quantum information and quantum computation. This thesis focuses on exploring different classes of QKD protocols and their practical implementations. Chapter-1 delves into the necessity for secure communication and the limitations of classical cryptographic methods, leading to a detailed exploration of various QKD protocols. By exploring into these cutting-edge concepts, the thesis aims to contribute to the growing field of quantum communication and information.

1.1 Classical Cryptography

As technology and computer science advancements continue to revolutionize communication, the need for secure communication has become more pressing. With the digitization of information, ensuring data security has become crucial for everyone [1]. The internet has brought together various computer networks, facilitating communication across the globe for private, public, academic, business, and government entities, making information confidentiality a top priority in real-life situations [2].

Cryptology is the science of secure communication. Cryptology comprises two main fields: cryptography and cryptanalysis [3–5]. Cryptography is a technique used to send information securely so that only the intended recipient can read it. It involves encoding (encryption) and decoding (decryption) messages to hide the information they carry, making it ideal for sending secret or confidential information. Cryptography focuses on creating codes and ciphers to protect the information. On the other hand, cryptanalysis deals with the technique of breaking these codes within a specific timeframe. By understanding how to break codes, cryptanalysis plays a vital role in ensuring the security of a given cryptosystem. The combination of code-making and code-breaking forms a secure cryptosystem within cryptology [4].

Initially, cryptography served military purposes, but with advances in telecommu-

nication, secure communication has become essential for everyone, not just nations but also individuals communicating with each other. To understand the communication process, we introduce three main characters: Alice and Bob, who want to communicate securely, and Eve, a third party who could eavesdrop on the information.

The message Alice wants to send is called plaintext (P). To protect it, she combines it with a **key** to create ciphertext or cryptogram (C) through encryption (E). Bob, the recipient, performs a decryption operation (D) using a corresponding key to retrieve the original message. The security of a cryptosystem relies on the key; without it, the cryptogram should be impossible to unlock. The goal is to protect the message as long as its information is valuable. Further, cryptography is classified into two types: symmetric key cryptography and asymmetric key cryptography, based on whether the same or different keys are used for encoding and decoding.

1.1.1 Symmetric Key Cryptography

In symmetric key cryptography, we use the same key 'K' for both encryption and decryption. Alice encrypts her plaintext into ciphertext by combining it with the key 'K'. The encrypted message is then securely transmitted to Bob through channels like WiFi-protected access (WPA) or local area network (LAN). Bob, in turn, decrypts the ciphertext using the same key 'K' to retrieve the original message. The process of key distribution in the symmetric algorithm is illustrated in Figure 1.1.

The encryption and decryption algorithm can be written as,

$$E_K(P) = C \implies \text{Encryption} \tag{1.1}$$

$$D_K(C) = P \implies \text{Decryption} \tag{1.2}$$

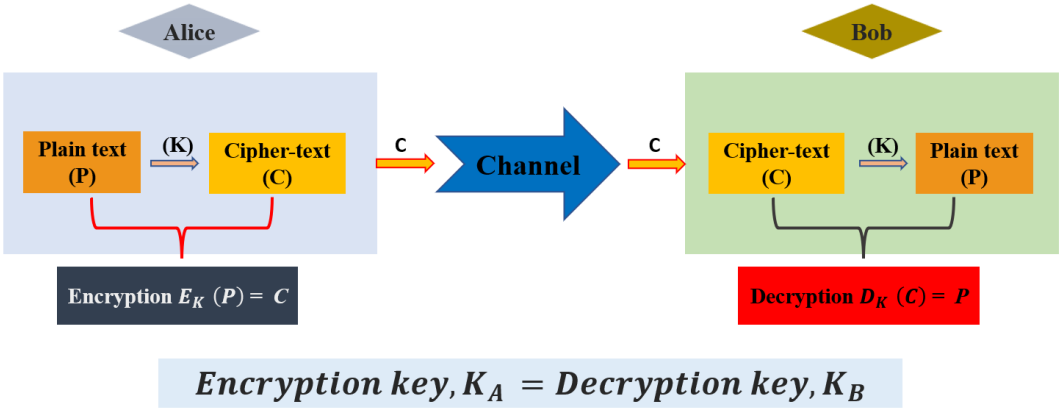

Figure 1.1: Symmetric key distribution. Alice encrypts his plaintext P, using key K, and gets the ciphertext C, which is transmitted through the classical channel. Bob decrypts the ciphertext using the same key K, and retrieves the plaintext P.

The one-time pad (OTP), also known as Vernam ciphers, was initially proposed by Gilbert Vernam of AT&T in 1926 and falls under the category of symmetric key distribution. The encryption and decryption algorithms are publicly known, and the security of the cryptogram relies entirely on the secrecy of the key [3, 4]. For OTP to be secure, the key must consist of a sequence of randomly chosen, sufficiently long bits of string.

Later, Shannon proved that OTP is information-theoretically secure [6], meaning its security remains intact regardless of the computing power available to potential eavesdroppers. If the key is truly random, never reused, and kept secret, OTP can offer perfect secrecy. However, despite Shannon's proof of its security, OTP has significant drawbacks in practical applications;

- It requires a perfectly random key.
- Secure key generation and exchange of the key must be at least as long as the message itself.

The OTP's requirement to renew the key for every message makes key distribution

prohibitively expensive. As a result, in most applications, absolute secrecy is not feasible, and less expensive and less secure systems are used. For critical applications, OTP may be employed due to its perfect secrecy, but for routine use like e-commerce, more practical approaches are favored.

Symmetric cryptosystems, such as the data encryption standard (DES), use shorter keys, typically 64 bits, along with complicated permutations and nonlinear functions to produce ciphertext from plaintext divided into blocks [5, 7]. Other cryptosystems like IDEA and advanced encryption standards (AES) follow similar principles, providing secure encryption for various applications [4, 8].

1.1.2 Asymmetric Key Cryptography

Asymmetrical cryptosystems involve the use of different keys for encryption and decryption. They are commonly known as public-key cryptosystems. The two main public-key cryptography techniques; the Diffie-Hellman key exchange protocol [9] and the RSA encryption system [10], are used currently. The key distribution using an asymmetric algorithm is shown in Fig. 1.2. Public-key cryptography allows communi-

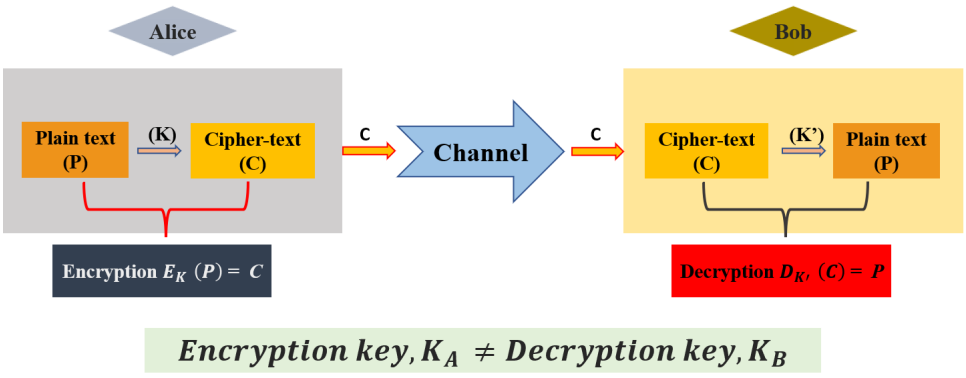

Figure 1.2: Asymmetric key distribution. Alice and Bob use different keys K and K' for encryption and decryption.

cating parties to exchange messages without prior agreement on a secret key. Instead, each party has a public key and a private key. The concept is analogous to a secure safe - anyone can lock it using the public key, but only the owner with the private key can unlock it. This system underpins the security of the Internet, acting like a mailbox where anyone can deposit a letter, but only the rightful owner can access it by using their private key. The security of public-key cryptosystems relies on the computational complexity of the algorithm. For instance, RSA encryption is based on the difficulty of prime factorisation for large integers. As the number of digits increases, the time required to factorise the number becomes significantly more challenging. Thus, increasing the number of digits renders the task computationally infeasible [1, 4, 5].

Despite its elegance, public-key cryptography faces a significant challenge. Currently, there is no definitive proof regarding the difficulty of factoring large integers, leaving open the possibility of the existence of a fast factorisation algorithm. Peter Shor's discovery of a polynomial algorithm for fast factorisation using a quantum computer adds uncertainty to the nonexistence of a similar algorithm for classical computers [11–14]. Likewise, all public key cryptosystems rest on unproven assumptions that may be weakened or overcome by theoretical or practical advances. In other words, the security of asymmetric cryptosystems is not mathematically proven, posing a serious threat to their reliability and making them susceptible to potential future breakthroughs [1, 15, 16].

Quantum cryptography [17] brings an entirely new way of solving the key distribution problem. It provides a better secure key distribution because, unlike classical cryptography, the security of quantum cryptography relies on the laws of Quantum Mechanics rather than the complexity of the mathematical algorithms.

1.2 Quantum Key Distribution

The increasing need for secure communication has led to the rise of quantum communication in recent decades [18, 19]. The laws of Quantum Mechanics make it strong evidence of practical application in quantum cryptography and ensure the security of the information transfer between the communicating parties. Quantum key distribution (QKD) represents the future of secure communication, incorporating both quantum and classical communication. QKD utilizes quantum states to encode information, offering not only unconditional security [20, 21] but also real-time detection of eavesdroppers [12, 21]. Compared to conventional cryptography [17, 22], QKD's information-theoretic security, rather than relying on computational hardness, makes it more resilient against attacks and information leakage during communication [15, 23].

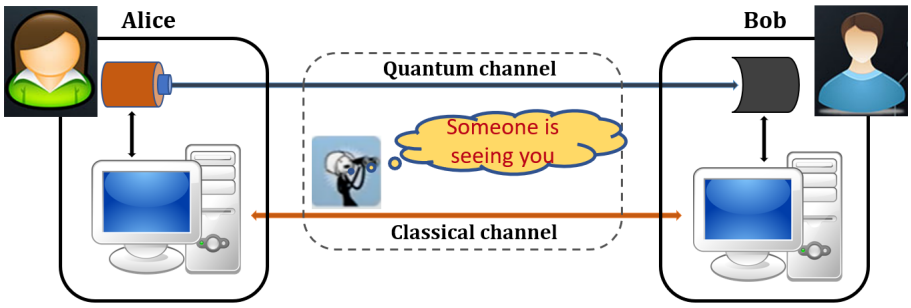

Figure 1.3: General layout of a quantum key distribution protocol.

The QKD protocol follows a general layout as depicted in Fig. 1.3. The process begins with Alice and Bob exchanging quantum bits or **Qubits**. The key information is encoded using a prescribed set of quantum states of a single particle. The transmission of qubits occurs through an insecure quantum channel. Eavesdropping, in this context, involves an eavesdropper performing measurements on the transmitted qubits. Upon

receiving the quantum state, Bob retrieves the key information by conducting measurements. The actual key exchange occurs through a quantum channel, and afterward, the key is further processed using an authenticated classical channel. This QKD approach ensures secure communication through quantum principles and authenticated classical channels.

1.2.1 Properties of Quantum System

In quantum communication, the information is stored in the form of quantum bits or qubits, representing quantum states. Therefore, we consider the quantum states and their measurements in detail [24, 25].

- **Quantum State**

  Any degree of freedom can be used to encode or represent bits. Some of the examples are polarisation, orbital angular momentum (OAM), time, frequency of photons, or the field quadratures of the electromagnetic field. The qubit in horizontal polarisation is represented as $|H\rangle$ while in vertical polarisation $|V\rangle$. One can also have a superposition of $|H\rangle$ & $|V\rangle$ polarisation, which is represented as $c_1|H\rangle + c_2|V\rangle$. Where c_1 and c_2 are the probability amplitudes (can be complex numbers) of $|H\rangle$ & $|V\rangle$ states, respectively.

  In addition, we can have different states of the electromagnetic oscillator, like the quadrature states. The single-mode system allows for the definition of position- and momentum-like operators as follows: $\hat{q} = \frac{1}{\sqrt{2}}(\hat{a}^\dagger + \hat{a})$ and $\hat{p} = \frac{i}{\sqrt{2}}(\hat{a}^\dagger - \hat{a})$. The canonical conjugate variables $\hat{q}$ and $\hat{p}$ satisfy the commutation relation, $[\hat{q}, \hat{p}] = i$. The coherent state $|\alpha\rangle$ can be written in terms of quadrature states $|q + ip\rangle$.

- **Projective Measurement**

  Measuring qubits on a corresponding basis will project them in one of the eigen-basis of the measurement operators. The below example makes the statement clear.

  Measuring in $\{H,V\}$ basis means the projectors are $\mathbb{P}_H = |H\rangle\langle H|$ & $\mathbb{P}_V = |V\rangle\langle V|$ indicates projection of the states on the corresponding polarisation. Let the initial state of the system be $|\psi\rangle_{in} = |H\rangle$ then the measurement result leads to

$$|\psi\rangle_f = \frac{\mathbb{P}|\psi\rangle_{in}}{{}_{in}\langle\psi|\mathbb{P}|\psi\rangle_{in}}, \tag{1.3}$$

  $|\psi\rangle_f$, final state after measurement. The subscript in $\mathbb{P}$ can either be H or V based on the projection used in the measurement. Here, $|\psi\rangle_f$ in $\mathbb{P}_H$ will be $|H\rangle$ and in $\mathbb{P}_V$, it will be 0. If initial state is in superposition $|\psi\rangle_{in} = c_1|H\rangle + c_2|V\rangle$ then, the probability of the final state in H is $\frac{{c_1}^2}{c_1^2+c_2^2}$ and in V is $\frac{{c_2}^2}{c_1^2+c_2^2}$. This indicates that measurement of state in the wrong basis will give random results [15, 17].

- **Quantum Entanglement**

  According to quantum entanglement, if two systems are entangled, then they share a strong non-local correlation (quantum correlation), which will be maintained even when they are separated by vast distances. The essence of entanglement is that measurement performed on one particle directly affects the state of the other particle even when they are far apart. Mathematically, an entangled state can be represented as two states which are non-separable.

  Consider two photons, a and b, whose combined state is written as,

$$|\psi\rangle_{ab} = |\psi\rangle_a \otimes |\psi\rangle_b, \tag{1.4}$$

where $|\psi\rangle_a$ and $|\psi\rangle_b$ are the individual quantum states of each photon. Eq. 1.4 is not an entangled state because the combined state can be written as a direct product of the two photons. Therefore, measuring the state of photon a, will not affect the state of photon b.

A pair of photons is said to be entangled if the quantum state of each particle can not be described independently but only the quantum state as a whole. Mathematically,

$$|\psi\rangle_{ab} \neq |\psi\rangle_a \otimes |\psi\rangle_b \,. \tag{1.5}$$

Here, the state, $|\psi\rangle_{ab}$, is a non-separable state and shows the non-local correlations.

The aforementioned properties serve as the foundation of quantum computing and quantum information [18, 19]. A more detailed mathematical explanation of these concepts is provided in Chapter-2.

1.2.2 Basic Security

The basic principles that guide the ideas of security in any QKD protocols are as follows.

No-cloning Theorem

It is impossible to construct a universal machine that can copy an arbitrary quantum state [26, 27]. The laws of quantum mechanics prevent copying an unknown quantum state. This makes QKD protocols robust against eavesdropping while exchanging information.

Consider a machine performing unitary operations clones a state $|\psi\rangle$.

$$|\psi\rangle|b\rangle|U_o\rangle = |\psi\rangle|\psi\rangle|U_\psi\rangle \tag{1.6}$$

Here, $|b\rangle$ is the blank state of the machine, and $|\psi\rangle$ is the state to be copied. $|U_o\rangle$ and $|U_\psi\rangle$ are the initial and the final states of the machine. This is true for any arbitrary state $|\phi\rangle$ as well.

Now, if we want to copy an arbitrary state of the form, $\alpha|\psi\rangle + \beta|\phi\rangle$, where α, β are complex numbers. Then, we get,

$$(\alpha|\psi\rangle + \beta|\phi\rangle)|b\rangle|U_o\rangle = \alpha|\psi\rangle|\psi\rangle|U_\psi\rangle + \beta|\phi\rangle|\phi\rangle|U_\phi\rangle \tag{1.7}$$

However, the state that should be obtained after copying is desired to be

$$(\alpha|\psi\rangle + \beta|\phi\rangle) \otimes (\alpha|\psi\rangle + \beta|\phi\rangle) \tag{1.8}$$

So, the state that the copying machine gives is not the desired state that one should obtain. So, from the unitary transform, one can never clone an unknown arbitrary quantum state. This principle prevents an interceptor (or eavesdropper) from copying the state exactly.

Uncertainty Principle

One cannot measure two canonically conjugate variables, such as position and momentum $(X,\ P)$, with arbitrary accuracy simultaneously. In general, the uncertainty

principle between two conjugate variables is

$$\triangle q \triangle p \geq \frac{h}{4\pi}. \tag{1.9}$$

This property provides an advantage in ensuring security in any QKD protocol. When a measurement is performed on one basis, it randomizes the result on a conjugate basis. Consequently, the uncertainty principle limits the maximum information that can be revealed to a third party, such as Eve, without creating any disturbance. This feature ensures that eavesdropping is impossible without detection, making QKD inherently secure.

Entanglement Monogamy

In quantum physics, if the two particles or systems are entangled with each other, then there is no way a third party can be correlated with any one of them. This is explained in Fig. 1.4. The monogamy of entanglement is a fundamental principle in Quantum

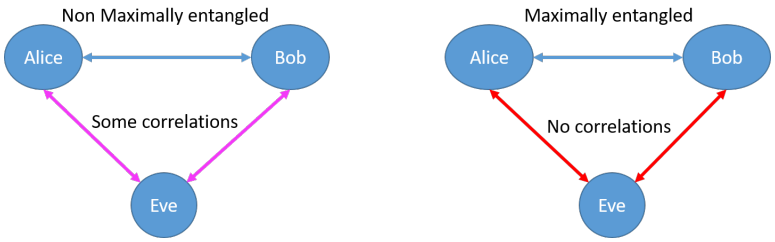

Figure 1.4: Schematics for entanglement monogamy.

Mechanics, which states that quantum entanglement cannot be simultaneously shared by an unlimited number of systems [28]. This unique property plays a crucial role in enhancing the security of entanglement-based QKD protocols.

In entanglement-based QKD, the security of the key exchange relies on the use of

entangled quantum states between the communicating parties, Alice and Bob. When they share a maximally entangled pair, which serves as the basis for the final secret key, the monogamy of entanglement ensures that the potential eavesdropper, Eve, cannot have correlations with both Alice and Bob simultaneously. This property makes it impossible for Eve to gain any information about the secret key during the transmission.

1.2.3 Classification of QKD

In QKD, the key information is encoded in the quantum state of light, which is then transmitted through a quantum channel [29]. The receiver performs a prescribed set of measurements on the received quantum state. Based on the techniques of state preparation and detection, QKD has been classified broadly into two categories [30] i.e., discrete variable (DV) and continuous variable (CV) QKD. In DVQKD, the key

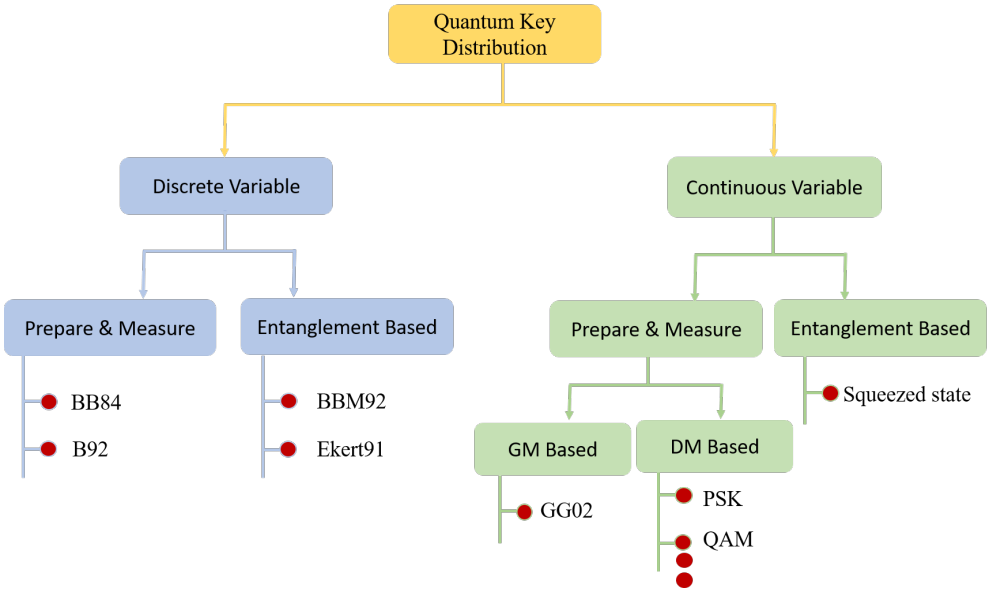

Figure 1.5: Classification of QKD; GM: Gaussian Modulation; DM: Discrete Modulation; GG02: Grosshan and Grangier; QPSK: Quadrature Phase Shift Keying; QAM: Quadrature Amplitude Modulation.

information is encoded in discrete properties of light, such as the polarisation state, time of arrival, or phase [12, 31]. On the other hand, in CVQKD, the key information is encoded in continuous properties of light, like the field quadratures of the electromagnetic oscillator [32]. DVQKD uses single-photon detectors for detection [33, 34], while CVQKD employs homodyne/heterodyne detectors [35–37].

The classification of QKD on the basis of state preparation and measurement is shown in Fig. 1.5. DVQKD and CVQKD protocols are further divided into prepare and measure, and entanglement-based protocols. There are various classes of protocols that belong to prepare and measure [38, 39] and entanglement-based DVQKD protocols [28, 40–42]. The first proposed protocol BB84 [43] and B92 [31], belongs to the class of prepare and measure protocols. Whereas BBM92 [44] & Ekert-91 [41] belong to entanglement-based protocols [42].

Based on the techniques of modulation, the prepare and measure CVQKD protocols are classified further into Gaussian modulation (GM) [45, 46] and discrete modulation (DM) protocols [47, 48]. The Gaussian modulation coherent state (GMCS) CVQKD and GG02 belong to the earlier case. Quadrature phase shift keying (QPSK) and quadrature amplitude modulation (QAM) [49], belong to the latter case. The entanglement-based CVQKD includes the squeezed state protocols that also use Gaussian modulation [32].

The details of quadrature states and squeezed states will be discussed in Chapter-2.

1.3 Discrete Variable QKD

Prepare & Measure Protocol (BB84 Protocol)

Charles H. Benett and Gilles Brassard proposed the first QKD protocol in 1984, [23] named BB84. The protocol execution includes the following steps.

1. Alice encodes her key information in the polarisation state of the photon. She randomly chooses a basis ($\{H,V\}$, or $\{D,A\}$) from a set of mutually unbiased basis. She assigns the bit values to the polarisation states as $H \rightarrow 0, V \rightarrow 1, D \rightarrow 0, A \rightarrow 1$.

2. She sends the encoded state to Bob through a quantum channel, which can be either a free space or a fiber-optic channel.

3. Bob randomly chooses his measurement basis and records the data.

4. Once sufficient bits are collected, Alice and Bob use the authenticated classical channel to disclose their basis choice.

5. They keep the results for which the basis are compatible. They are left with the raw key. This process is called sifting.

6. They announce the results of a small fraction of the key over a public channel to estimate the errors. If the error is above a threshold, they abort the protocol, and if the error is below the threshold value, they further do the post-processing to get a secure key.

7. Furthermore, they perform the error correction (to make the key identical) and the privacy amplification (to make the key secure against eavesdropper) to ex-

tract the secure key. A fraction of the key is used in this process, which is removed from the final key.

A schematic of the protocol is shown in Fig. 1.6. This protocol was first demonstrated

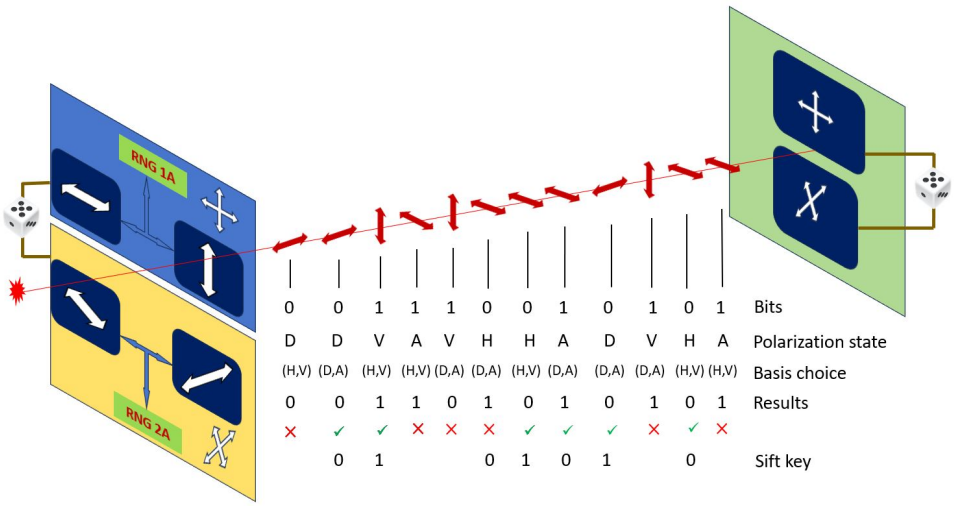

Figure 1.6: Schematics of BB84 protocol.

experimentally in 1992 [31]. Later, a similar protocol, B92 was proposed, which tells how one can do QKD with just two non-orthogonal states [39].

Entanglement-based DVQKD

In 1991, Arthur Ekert proposed another type of QKD protocol, which was based on the principle of quantum entanglement known as the Ekert-91 protocol [41]. In Ekert's protocol, instead of Alice sending particles to Bob, there is a central source creating entangled particles and sending one to Alice and one to Bob. The protocol is briefly described below.

- A common sender 'Charlie' prepares an entangled state $|\psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ and sends the state to Alice and Bob through a quantum channel (fiber or free

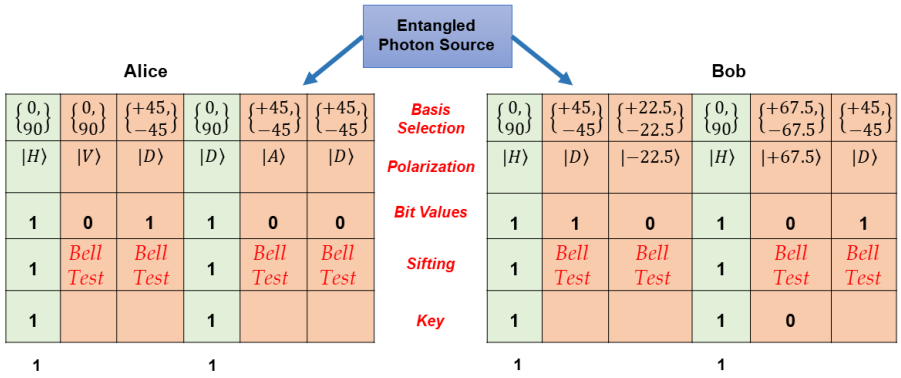

Figure 1.7: Schematics of Ekert (E91) Protocol. *Image credit-Ayan Biswas.*

space).

- Alice and Bob independently make their measurements in random basis.
- The measurement bases of Alice are ({**22.5/-22.5**},{**67.5/-67.5**},{**0/90**}) where as Bob's bases are({**0/90**},{**45/-45**})
- After the measurement process, both Alice and Bob declare their basis choices through the public channel.
- Alice and Bob will form the key when they choose the same bases for their measurements (i.e., when both of them measure in {**0/90**} basis).
- The rest of the measurement results will be used to check the Bell's parameter for the security of the protocol.

The schematic of the protocol is shown in Fig. 1.7.

The security of these protocols is based on the monogamy of entanglement, i.e., the entanglement between two systems decreases when a third system interacts with

the entangled photons. The protocols are secure against any eavesdropping strategy. The Bell's parameter for the maximally entangled state is $2\sqrt{2}$ if the particle is not disturbed by the eavesdropper. If a maximally entangled state is used for a key generation, then the Bell parameter (S) below $2\sqrt{2}$ (for ideal channel) will be considered insecure [41, 50–53]. For real situations both S, and quantum bit error rate (QBER) are measured, if S is less than $2\sqrt{2}$ and there is QBER in the generated keys, then one goes for error correction and privacy amplification to distill the secret keys [54–56]. The advantage of working with entanglement-based DVQKD is that it does not require random number generators. Randomness is inherent in the process of the generation of entangled photons. However, the price of entanglement-based DVQKD is a lower key generation rate due to the limited brightness of contemporary entangled photon-pair sources.

Another similar type of protocol used for entanglement-based DVQKD is BBM92 protocol [57]. It avoids the need to measure Bell's inequality violation. The key is formed only from the compatible basis on both Alice's and Bob's sides. This increases the key rate but makes it less secure.

1.4 Continuous Variable QKD

The demonstration of continuous-variable quantum teleportation in [58] has made significant interest in the field of CVQKD. The first protocol of CVQKD proposed by F. Grosshans and P. Grangier was based on the Gaussian modulation of the squeezed states [59]. The idea of Gaussian-modulation CVQKD with coherent states was subsequently explored in [60, 61]. CVQKD utilizes the quadrature modulation and measurement of amplitude and phase from a bright laser to distribute the secret key. These protocols have various practical advantages over DVQKD protocols. In CV quantum

processing, the bandwidth of the homodyne detection is significantly higher ($\sim$ GHz) compared to that of the avalanche photodetectors used in DVQKD. Homodyne detection is far more efficient than single-photon detection, achieving higher detection efficiency [62, 63]. The key rate obtained in CV is much higher than DV for a certain distance as one can encode the key information in the quadrature states that can have infinite basis values [64–66]. The major advantage of CVQKD is that it uses only telecommunication components that are much more mature from a technological point of view and, hence, compatible with available classical infrastructure.

In DVQKD protocols, we obtained the key directly in binary form, which has direct applicability in the field. But for CVQKD protocols, we get the key in continuous form. We perform the homodyne detection at the receiver ends. So, instead of getting a binary number, the obtained key is in the form of the Gaussian key elements. Secret key distillation could be performed to extract the binary key from these continuous key elements [67, 68]. We will be discussing different classes of CVQKD protocols in the following sections.

Prepare & Measure Protocol (A Protocol with Coherent State)

The more general schematic of the prepare and measure protocol is shown in Fig. 1.8. The quantum key establishment includes state preparation and measurement. In particular, we encode the information in a weak coherent signal that carries the amplitude and phase quadrature of the beam. These are analogous to position and momentum for a light mode and, hence, are continuous, conjugate variables. We do the amplitude and the phase modulation of the light. Based on the modulation techniques, CVQKD is classified into Gaussian modulation and discrete modulation CVQKD. The modulation techniques involved in both protocols are further discussed in the upcoming

section. The encoded state is transmitted through the quantum channel to Bob. Bob

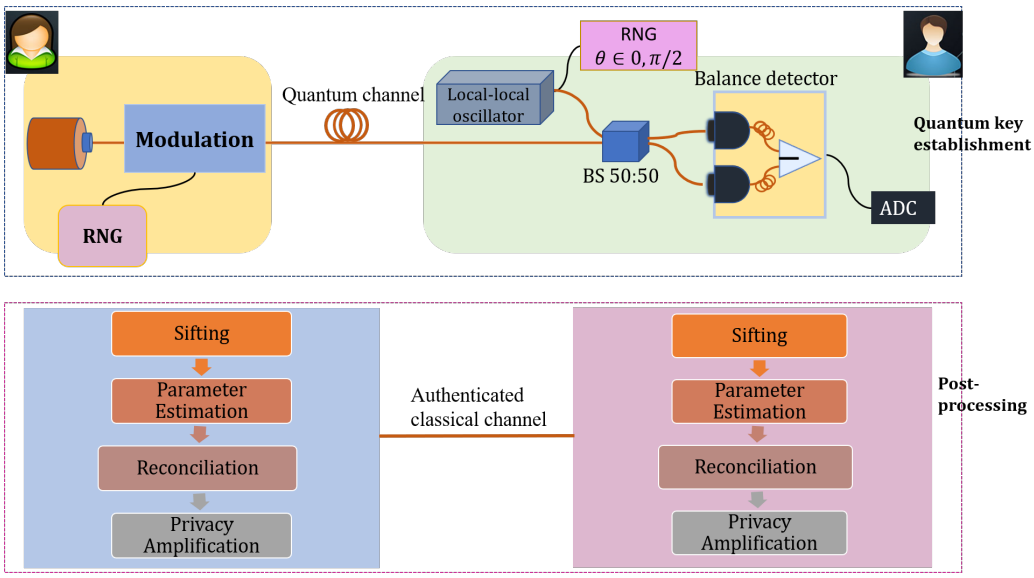

Figure 1.8: Schematic for prepare and measure CVQKD.

performs the homodyne/heterodyne detection. The local oscillator (LO) is a strong classical beam, acts as a phase reference, and selects the random basis measurement q or p. LO can be transmitted along with the signal or can be created at the receiver's end called a local-local oscillator (LLO) [69, 70]. Once the key is established, we do further post-processing, which includes sifting, error reconciliation, parameter estimation, and privacy amplification to extract the secure key. The information that one obtains is strictly limited by the generalized uncertainty principle for simultaneous measurements of conjugate variables.

Gaussian Modulation CVQKD

The protocol was proposed by Grosshans and Grangier in 2002, where coherent states are modulated in both quadratures simultaneously, called GG02. It uses the idea of Gaussian modulation. Alice generates coherent states of light mode with Gaussian distributed quadratures, and Bob's measurements are homodyne measurements. This

protocol allows for facilitated implementations and high secret key generation rates; this follows from the fact that homodyne detection can operate faster than the photon detectors used for BB84. The protocol includes the following steps.

- Alice prepares a large number of coherent states $|\alpha_1\rangle, |\alpha_2\rangle, ..., |\alpha_N\rangle$. Where, α_i are complex variables selected from two identical and independent normal distributions $N(0, V_{\text{mod}})$ with variance V_{mod}.
- Alice transmits the state through a quantum channel that could be fiber or free space.

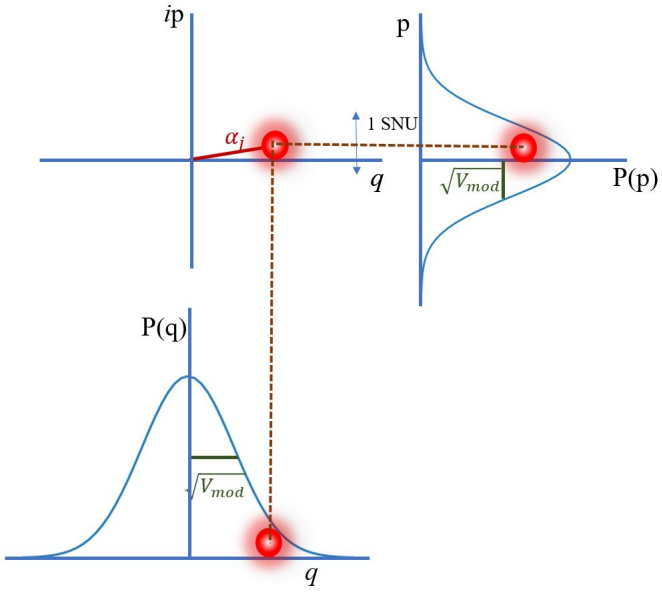

Figure 1.9: Gaussian modulation protocol for continuous variable QKD.

- Once the state is received by Bob, he performs homodyne (heterodyne) and measures a random quadrature q or p (q & p) for each state and informs Alice about his choices of both quadratures.
- After sifting, Both Alice and Bob are left with N or 2N real-valued numbers corresponding to their measurement outcomes (homodyne or heterodyne). De-

noting the sequence for Alice and Bob symbols, $x = (x_1, ..., x_n)$ and $y = (y_1, ..., y_n)$.

- Alice and Bob perform error reconciliation (direct or reverse reconciliation) and use classical error-correction techniques to correct the errors in their raw key formed after sifting.

- They perform parameter estimation to calculate the channel transmittance and excess noise present in the system and calculate the covariance matrix. This puts an upper bound on Eve's information. Once this estimate is obtained, Alice and Bob can compute a secure key of a certain length.

- At the end, they perform privacy amplification to the obtained key using universal Hash functions to their respective corrected strings and obtain a final secure key.

Discrete Modulation CVQKD

The other class of CVQKD is known as discrete modulation CVQKD. In such protocols, we do the discrete modulation of the coherent state [71–74]. The advantage of the protocol is that it simplifies the modulation scheme and key extraction task, which are a bit more complicated in GG02 protocols, where one extracts the key from continuous random values. The other benefit of implementing discrete modulation CVQKD is its long-distance applicability. In these protocols, reconciliation efficiency remains remarkably high even at very low SNR, and these protocols can be applied for long-distance applications.

The protocol we are going to analyse consists of the following steps:

- Alice prepares a quantum state $|S\rangle$, which is randomly chosen out of four coherent states $|\pm\alpha\rangle$, $|\pm i\alpha\rangle$ of a given mode. Here, $\alpha > 0$.
- She then transmits the state to Bob over a quantum channel.
- Bob performs homodyne detection on the received signal and randomly decides to measure the $\hat{q}$ quadrature or the $\hat{p}$ quadrature.

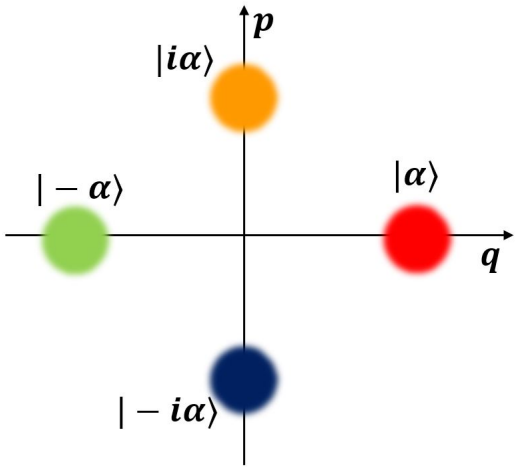

Figure 1.10: Discrete modulation protocol for continuous variable QKD.

- Alice and Bob repeat the processes mentioned above sufficiently many times.
- Alice reveals which basis she used in each process through a classical channel. She also randomly chooses a part of the process and reveals the state she sent.
- Bob estimates the parameters of the quantum channel using the data revealed by Alice. Then, he selects the data to be used for key generation in accordance with his measurement and the estimated channel parameters. He uses only the processes for which he made a correct choice of measurement basis. Here, the correct basis refers to the q-basis for $|\pm\alpha\rangle$, whereas the p-basis for $|\pm i\alpha\rangle$. Bob informs Alice which process was selected. In the theoretical analysis, we assume that Bob also reveals the absolute value $|m|$ of his outcome m.

- Bob makes a bit string by assigning 0 for the negative m and 1 for the positive m of the selected measurement, respectively.
- Alice makes a bit string by assigning 0 for $|-\alpha\rangle$, $|-i\alpha\rangle$, whereas, 1 for $|\alpha\rangle$, $|i\alpha\rangle$.
- Alice and Bob share a secure key by applying error correction and privacy amplification to the bit strings obtained.

Entanglement Based CVQKD (A Squeezed State Protocol)

The entanglement-based protocols involved entangled beams of light and showed EPR correlations [75] of quadratures. The CVQKD protocols based on entangled states of light [76, 77] are proved to be more secure against adversaries. The security of such protocols is given against the strongest collective attacks that are optimal under certain symmetries of the protocol [78–80].

The protocol execution involves the following steps. Alice generates Gaussian key elements randomly and independently, denoted by a variable X_A. Alice chooses two different encoding rules, which may require different variances,

$$X_{A,i} \sim N(0, \Sigma_{A,i}\sqrt{N_o}) \tag{1.10}$$

where $X_{A,i}$ decide that the state is squeezed in q for $i = 1$ or in p for $i = 2$. The idea of the protocol is as follows. The Heisenberg Uncertainty principle implies that it is impossible to measure with absolute accuracy both the quadrature of a single-mode, $\mathbf{q}$, and $\mathbf{p}$. Let us now detail the two encoding rules.

- In case 1, Alice prepares a squeezed vacuum state such that the fluctuations of

q are squeezed with parameter $s_1 < 1$ and applies a displacement of q by an amount equal to $X_{A,1}$ i.e., such that $\langle \mathbf{q} \rangle = X_{A,1}$. Hence, Alice's encoding rule is $X_{A,1} \rightarrow |X_{A,1,s_1}\rangle$.

- In case 2, Alice sends a squeezed state $\mathbf{p}$ squeezed with parameter $s_2 > 1$, and applies a displacement of $\mathbf{p}$ by an amount equal to $X_{A,2}$, i.e., such that $\langle \mathbf{p} \rangle = X_{A,2}$. Hence, Alice's encoding rule is $X_{A,2} \rightarrow |X_{A,2,s_2}\rangle$.

- On his side, Bob measures either $\mathbf{q}$ or $\mathbf{p}$, yielding the result $Y_{B,\mathbf{q}}$ or $Y_{B,\mathbf{p}}$, choosing at random which quadrature he measures.

- After sending a predefined number of squeezed states, Alice reveals to Bob the encoding rule for each squeezed state. They keep only the useful transmissions over the quantum channel; that is, they discard the key elements for which Alice used case 1 (or case 2), and Bob measured $\mathbf{p}$ (or $\mathbf{q}$). The remaining key elements corresponding to Bob's measurements are denoted by Y_B.

- They reconstruct the distributions corresponding to correct measurements and do the classical post-processing to get the secret key.

The QKD techniques mentioned above appear to be secure and effective in addressing the key distribution problem. Ideally, all these QKD techniques offer unconditional security from an information-theoretic perspective. However, achieving this level of security in practical implementations presents challenges. The main hurdle lies in constructing a QKD system that balances minimalistic resources with maximum security. Currently, there are numerous protocol implementations in the literature [81, 82]. However, some of these implementations may suffer from either low key generation rates or reduced security levels. Striking the right balance between key generation rate and protocol security becomes a soft trade-off in QKD system design. The recent

work in the field of QKD is directed in two directions: implementing the protocols and giving more advanced security proofs for the existing protocols [20, 40, 83, 84].

Various DVQKD protocols have been implemented since the discovery of BB84 protocol [12, 31, 85–87]. Ground-to-satellite link has been established successfully [88]. The rigorous security proofs are developed for finite size key analysis [89–92] for DVQKD protocols. A lot of work has been done to account for the various imperfections present in a QKD experiment, and security proofs are given [93, 94]. To eliminate the source imperfection and increase the key rate with the same security a decoy state protocol is implemented [95–97]. In addition, measurement device independent (MDI) QKD is implemented, which removes the fear of side channel attack at the detection end [98]. That is, the scope of QKD applications is expanding every year, as well as the number of approaches to its implementation.

Certainly, QKD systems are not meant to replace existing infrastructures but rather be integrated into them. As a result, a significant portion of current and prospective research in quantum communications focuses on finding practical solutions to various challenges. One such solution involves utilizing coherent detection methods in QKD systems, which use devices already employed in classical fiber-optical communication systems, rather than relying on single-photon detectors, which are both complex and expensive. These QKD systems based on coherent detection methods are referred to as CVQKD systems [60, 99–102]. The CVQKD approach offers several evident advantages. These advantages include cost reduction, high secure key generation rates, and scalability. Embracing CVQKD can pave the way for more efficient and feasible quantum communication systems. By exploring CVQKD, we can discover a faster and more reliable QKD approach that optimizes resources and operates efficiently within the constraints of classical infrastructure.

1.5 Objective of the Thesis

QKD is a promising method to achieve secure communication resistant against adversaries between two parties, the sender (Alice) and the receiver (Bob). The increase in demand for secure communication at a very high speed has given origin to various classes of QKD protocols. The two major families of QKD protocols are DVQKD and CVQKD protocols. Such protocols have been the subject of wide research and have been experimentally implemented over long distances. A successful demonstration of satellite-to-ground quantum communication has been done. India has initiated efforts in this direction by setting it as one of the objectives of the National Quantum Mission (NQM). This NQM is expected to accelerate quantum technology (QT) led economic growth, nurture the ecosystem in the country, and make India one of the leading nations in the development of Quantum Technologies and Applications (QTA).

Being less resource-intensive QKD promises to integrate with the current communication setup within the coming years. The entanglement-based DVQKD protocols are proven to be more secure than the prepare and measure protocols but require more resources than a typical BB84. Keeping this in mind, to get a trade-off between resources and security, we have implemented the BB84 protocol using heralded single-photon source. The proposed method uses less resources, i.e., five detectors, compared to BBM92, which uses eight detectors and is more secure than weak coherent pulses. Since we use a single-photon source, it does not require an external random number generator to prepare various polarisation states randomly. Instead, a beam splitter (BS) does the job of random selection.

DVQKD protocols suffer disadvantages in the form of the requirement for single-photon sources and detectors. These limitations restrict the rate of key exchange as

well as open the QKD protocols to various attacks by an eavesdropper. Compared to DVQKD protocols, CVQKD protocols bypass such stringent requirements by exchanging single-photons with weak coherent states and single-photon detectors with photodetectors.

In this thesis, we have implemented various classes of CVQKD protocols over free space, which include, discrete modulation and Gaussian modulation CVQKD. This is the first time we have demonstrated this class of protocols in our lab in India. Free space offers various advantages over fiber, as the optical losses are less in free space compared to fiber. In addition, the free space channel is insensitive to polarisation compared to fiber, which results in light polarisation being nearly unchanged during propagation. The presence of Eve in the line of sight could be detected easily. In addition to this, compared to fiber CVQKD, atmospheric link offers the possibility of broader geographical coverage and more flexible transmission.

We performed the field demonstration of discrete modulation and Gaussian modulation CVQKD over an atmospheric channel. Along with this, we have worked on the various experimental parameters affecting the key rate of the protocols. We have highlighted the imperfections present in the initial characterisation of the setup. These imperfections could lead to security threats in CVQKD and could have a strong impact on the achievable key rate. We have performed both theoretical and experimental studies of these parameters.

1.6 Organisation of Thesis

This thesis is organized into eight Chapters. Chapter-1, is dedicated to understanding the basic concepts, which will help to follow the protocols described in the upcoming Chapters. In this Chapter, we discussed the need for QKD protocols for se-

cure communication. This Chapter includes various classes of QKD that are currently used in practice. The study includes both prepare & measure and entanglement-based QKD protocols.

Chapter-2, is divided into two sections. Section-I is based on the formalism of quantum mechanics, and Section II includes the study of the tools needed for the execution of a QKD protocol. In Section I, the concept of quantum state measurement, the idea of quantum entanglement, and density matrix formalism are described in brief. We discuss the electromagnetic harmonic oscillator and its possible states. We further study the mathematical treatment of the balanced homodyne detection in detail, which is used to measure the field quadratures of the electromagnetic field. Section-II describes details of the post-processing of the CVQKD. Further, we calculate the mutual information and the secure key rate for CVQKD protocols.

In Chapter-3, we describe the implementation of BB84 QKD protocol using a heralded single-photon. Where these photons are produced by the Spontaneous Parametric Down-Conversion (SPDC) process. Further, We discuss the experimental results and the measured security parameters.

In Chapter-4, we do the initial characterisation of the setup for CV applications, which deals with measuring the shot noise. We accounted for various imperfections present in the detection system and gave a theoretical and experimental understanding of the same.

In Chapter-5, we have demonstrated a discrete modulation CVQKD protocol in a controlled environment of the lab. We have proposed a noise model to account for the channel losses and done the simulation to see the effects of various parameters on the secure key rate. These simulated results would help in the certification of the

experimental results.

In Chapter-,6 we have implemented the Gaussian modulation CVQKD protocol over free space in laboratory settings. We have performed a careful characterisation of the setup including electronic noise, shot noise, detection efficiency, and delay measurements. We have extracted the various experimental parameters and the mutual information for the protocol.

In Chapter-7, we have performed the field demonstration of discrete and Gaussian modulation CVQKD over atmospheric channels and simultaneously studied the effect of environmental parameters on the secure key rate.

Finally, the summary of the thesis and the future scope are given in Chapter-8.

Chapter 2

Theoretical Background

QKD is a broad field that requires a basic knowledge of quantum mechanics, classical and quantum information theory, fundamental quantum optics, computation, and other branches of physics. In the previous Chapter, we considered the broad perspective of discrete and continuous variable QKD. Before the execution of QKD, we need a theoretical background that would help us in understanding the work presented in the thesis. In this Chapter, we will study the mathematical background required to understand the DV and CV QKD. It involves the definitions of various types of quantum states and the mechanism for preparing them. This Chapter is organized into two major sections; Section I describes the basic concepts of Quantum Mechanics, and Section II gives the details of the tools required for the practical implementation of QKD.

Section I - Basic Concepts

2.1 Light as Quanta of ElectroMagnetic (EM) Field

Light shows both wave and particle aspects. It considers various phenomena such as interference and diffraction, dispersion, polarisation, etc. All these are the classical aspects of light. On the other hand, light appears as a click in the detector, called the photon. This aspect of light is considered in the photo-electric effect, Compton scattering, etc. The reason for this strange behavior of light is not known, but it has been formulated within the framework of the quantum theory of light. To understand this better, we will start with the classical description of the EM field, then quantise it.

Classically the dynamics of the EM field are given by Maxwell equations. In the vacuum, these equations are:

$$\nabla \times \mathbf{E} = -\varepsilon_0 \frac{\partial \mathbf{H}}{\partial t}, \tag{2.1}$$

$$\nabla \cdot \mathbf{E} = 0, \tag{2.2}$$

$$\nabla \times \mathbf{H} = \mu_0 \frac{\partial \mathbf{E}}{\partial t}, \tag{2.3}$$

$$\nabla \cdot \mathbf{H} = 0, \tag{2.4}$$

where μ_0 and ε_0 are the permeability and the permittivity of free space. It satisfies the relation, $\mu_0 \varepsilon_0 = c^2$, c being the speed of light. The EM field follows the wave equation, which is given by

$$\nabla^2 \mathbf{E} - \frac{\partial^2 \mathbf{E}}{\partial t^2} = 0. \tag{2.5}$$

It has a plane wave solution moving with the speed of light, which is given by

$$\mathbf{E}(r,t) = \sum_i E_i \varepsilon_i^{(\lambda)} \left[\alpha_{i,\lambda} e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_i t)} + \alpha_{i,\lambda}^* e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega_i t)} \right]. \tag{2.6}$$

Here, $\mathbf{E}(r,t)$ is a complex vector function called spatial-temporal mode. It includes all classical wave aspects, including polarisation. i is mode index, λ is polarisation, ω_i is frequency of the i^{th} mode, and $\alpha_{i,\lambda}$ and $\alpha_{i,\lambda}^*$ are complex constants. E_i is a real constant. A similar structure can be seen for the magnetic field; for further details, see [103].

Quantisation of EM field

The quantised EM field [25] can be identified by replacing the complex scalar $\alpha_{i,\lambda}$ and $\alpha_{i,\lambda}^*$ with the annihilation and creation operators $\hat{a}_{i,\lambda}$ and $\hat{a}_{i,\lambda}^\dagger$. These operators further satisfy the commutation relations

$$\begin{aligned} \left[\hat{a}_{i,\lambda}, \hat{a}_{i',\lambda'}^\dagger\right] &= \delta_{ii'}\delta_{\lambda\lambda'}, \\ \left[\hat{a}_{i,\lambda}, \hat{a}_{i',\lambda'}\right] &= 0, \text{ and } \left[\hat{a}_{i,\lambda}^\dagger, \hat{a}_{i',\lambda'}^\dagger\right] = 0 \end{aligned} \tag{2.7}$$

Hence, the quantised electric field can be expressed as

$$\mathbf{E}(r,t) = \sum_i E_i \varepsilon_i^{(\lambda)} \left[\hat{a}_{i,\lambda} e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_i t)} + \hat{a}_{i,\lambda}^\dagger e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega_i t)} \right]. \tag{2.8}$$

2.2 Representation of States

There are different possible representations of states.

2.2.1 Fock States

The single-mode states of the EM oscillator are known as Fock states, denoted by $|n\rangle$, also referred to as number states. These states are the eigenstates of the number operator $\hat{n}$, with the corresponding eigenvalue n. It is given by

$$\hat{n}|n\rangle = n|n\rangle. \tag{2.9}$$

The Fock states $|n\rangle$ are eigenstates of the Hamiltonian

$$H|n\rangle = \hbar\omega(n+1/2)|n\rangle = E_n|n\rangle, \tag{2.10}$$

with eigenvalue, E_n. Further, these states can be written as the excitation of the vacuum state,

$$|n\rangle = (\hat{a}^\dagger)^n/(\sqrt{n!})|0\rangle, \tag{2.11}$$

The number states, $|n\rangle$, have a definite and fixed photon number equal to n. These states being the eigenstates of the number operator, satisfy the orthonormality condition and form the complete basis of orthogonal states.

$$\text{Orthogonality relation: } \langle m|n\rangle = \delta_{m,n} \tag{2.12}$$

$$\text{Completeness: } \sum |n\rangle\langle n| = I \tag{2.13}$$

Therefore, an arbitrary state, $|\psi\rangle$, which is a superposition of energy eigenbasis, is

$$|\psi\rangle = \sum C_n |n\rangle . \tag{2.14}$$

In general, the density operator is used for describing any state of one mode of light,

$$\hat{\rho} = \sum_{m,n=0}^{\infty} p_{m,n} |m\rangle \langle n| , \tag{2.15}$$

where $\hat{\rho}$ is a positive Hermitian operator with $tr(\hat{\rho}) = 1$. The trace of the squared density operator, $tr(\hat{\rho}^2)$, can be used in measuring the purity of a state. It yields a value between $1/n$ and 1, where 1 represents a pure state and n is the dimension of the Hilbert space.

This single-mode formalism for the EM field can be extended to the multi-mode formalism by redefining the basis $|n_i\rangle$ as

$$|n_i\rangle = |n_1\rangle \otimes |n_2\rangle \otimes ... \otimes |n_i\rangle \tag{2.16}$$

where $|n_1\rangle$ represents the n_1 photons in the first mode and similar for others. This basis is the tensor product of different modes present.

2.2.2 Quadrature States

For a single-mode, the quantised electric field, Eq. (2.8) can be expressed as

$$\mathbf{E}(r,t) = E_0 \varepsilon(\lambda) \Big[\hat{q} \cos(\mathbf{k}\cdot\mathbf{r} - \omega t) + \hat{p} \sin(\mathbf{k}\cdot\mathbf{r} - \omega t) \Big]. \tag{2.17}$$

Here the operators $\hat{p}$ and $\hat{q}$ are defined as the quadratures of the EM field. These are given by

$$\hat{q} = \frac{1}{\sqrt{2}}(\hat{a}^\dagger + \hat{a}), \text{and} \tag{2.18}$$

$$\hat{p} = \frac{i}{\sqrt{2}}(\hat{a}^\dagger - \hat{a}) \tag{2.19}$$

These operators satisfy the commutation relation

$$[\hat{q}, \hat{p}] = i, \tag{2.20}$$

and the Uncertainty principle,

$$\Delta q \Delta p = 1/4, \tag{2.21}$$

where $\Delta q = \langle \hat{q}^2 \rangle - \langle \hat{q} \rangle^2$ and $\Delta p = \langle \hat{p}^2 \rangle - \langle \hat{p} \rangle^2$ are defined as the variances of the observables $\hat{q}$ and $\hat{p}$ respectively.

These operators can be considered analogous to the position and the momentum operators, even though they are not directly related to the position and momentum of the photons. Instead, they are associated with the harmonic oscillator linked to the single optical mode.

The quadrature states are the eigenstates of the corresponding operators

$$\begin{aligned} \hat{q}|q\rangle &= q|q\rangle \\ \hat{p}|p\rangle &= p|p\rangle. \end{aligned}$$

Forming the orthonormality conditions

$$\langle q|q'\rangle = \delta(q-q'), \text{ and} \tag{2.22}$$

$$\langle p|p'\rangle = \delta(p-p'), \tag{2.23}$$

for the complete orthogonal basis

$$\int_{-\infty}^{\infty} |q\rangle \langle q| = I \tag{2.24}$$

$$\int_{-\infty}^{\infty} |p\rangle \langle p| \quad = \quad I \tag{2.25}$$

Both of these states are related via the Fourier transformation relation.

$$|q\rangle = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} dq e^{-iq\cdot p} |p\rangle \,, \text{ and } |p\rangle = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} dp e^{iq\cdot p} |q\rangle \tag{2.26}$$

It is to be noted that the quadrature states cannot be measured directly. So, we need to find the probability distribution for these states. One can measure them using the well-known technique called homodyne detection; further details are discussed in 2.7.2.

We can write the Fock states in the coordinate representation also. $|n\rangle$ in the coordinate representation is

$$\psi_n(q) = \langle q|n\rangle \tag{2.27}$$

One can calculate the $\psi_0(q)$ by using the annihilation operator on the vacuum and solving the differential equation. For details, see textbooks such as [36]. Hence, the eigenstates of the harmonic oscillator can be obtained as follows:

$$\psi_n(q) = \frac{1}{\sqrt{2^n n! \sqrt{\pi}}} H_n(q) \exp\left(-q^2/2\right), \tag{2.28}$$

where $H_n(q)$ are defined as the Hermite polynomials [104]. The probability distribution of the q quadrature, $|\psi_n(q)|^2$, is found to be Gaussian in nature.

2.2.3 Coherent States

Though the Fock states are useful for the representation of states, they are difficult to generate experimentally. Alternatively, lasers are commonly used as sources of

light, generating coherent states. Hence, it is important to understand the properties of coherent states. The coherent state, also known as Glauber states, denoted as $|\alpha\rangle$, is the eigenstate of the annihilation operator, $\hat{a}$,

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle\,. \tag{2.29}$$

It is to be noted that since $\hat{a}$ is not a hermitian operator, the eigenvalue of $\hat{a}$ is complex ($\mathbb{C}$) in nature. Hence, the coherent states have well-defined amplitude, $|\alpha|$, and phase, $\arg\alpha$. One can further note that the vacuum is a coherent state as well since it verifies Eq. (2.29) for $\alpha = 0$. Therefore, the mean energy of the coherent state is

$$\langle H\rangle = \langle\alpha|\left(\hat{a}^{\dagger}\hat{a} + 1/2\right)|\alpha\rangle = |\alpha|^2 + 1/2. \tag{2.30}$$

It is the sum of vacuum energy and the intensity of classical waves. It can also be seen that the shift in the phase angle of the coherent state is given by

$$\hat{U}(\theta)\,|\alpha\rangle = \exp\left(-i\theta\right)|\alpha\rangle\,. \tag{2.31}$$

Further, The coherent state can be viewed as a displaced vacuum state. It is expressed as

$$|\alpha\rangle = D(\alpha)|0\rangle = \exp\left(\alpha\hat{a}^{\dagger} - \alpha^{*}\hat{a}\right)|0\rangle, \tag{2.32}$$

where $D(\alpha)$ is the displacement operator [104]. We stress that the coherent states are not physically similar to the vacuum states. They only have some quantum noise properties in common. In order to understand it better, we can compute the quadrature wave functions $\psi_{\alpha}(q)$ and $\psi_{\alpha}(p)$. First, we write the displacement operator in terms of quadratures q and p by decomposing the complex amplitude, α, into real and

imaginary parts, i.e., $\alpha = 2^{-1/2}(q_0 + ip_0)$, as

$$\hat{D} = \exp(ip_0\hat{q} - iq_0\hat{p}) = \exp\left(\frac{ip_0q_0}{2}\right)\exp(-iq_0\hat{p})\exp(ip_0\hat{q}) \tag{2.33}$$

Here, we have used the Baker-Campbell-Hausdorff formula

$$\exp(A+B) = \exp(A)\exp(B)\exp\left(-\frac{1}{2}[A,B]\right), \tag{2.34}$$

provided $[A,B]$ commutes. These states have both wave-like aspects as well as particle-like aspects. Above, we considered the displacement operator in terms of quadratures q and p, and hence the wave aspects. The probability distribution for both the quadrature wave function comes out as Gaussian.

$$\psi_\alpha(q) = \pi^{-1/4}\exp\left[-\frac{(q-q_0)^2}{2} + ip_0q - \frac{ip_0q_0}{2}\right] \tag{2.35}$$

It is the position wave function and a similar equation can be obtained for the momentum wave function [36]. On the other hand, in the particle picture, we express the displacement operator in terms of annihilation and creation operator.

$$\hat{D} = \exp\left(-\frac{1}{2}|\alpha|^2\right)\exp(\alpha\hat{a}^\dagger)\exp(-\alpha^*\hat{a}) \tag{2.36}$$

Again we have used the Baker-Campbell-Hausdorff formula to obtain this relation. Further, using Eq. (2.36) and Baker-Campbell-Hausdorff formula

$$\exp(-\alpha\, A)\; B\; \exp(\alpha\, A) = B - \alpha[A,B] + \alpha^2/2[A,[A,B]] + \ldots, \tag{2.37}$$

The displacement operator acted on the annihilation operator, a, and displaced it by the complex number α. It is given as

$$D^{\dagger}(\alpha)\hat{a}D(\alpha) = \hat{a}+\alpha. \tag{2.38}$$

A similar expression can be obtained for the quadratures of the field

$$D^{\dagger}(\alpha)\hat{q}D(\alpha) = \hat{q}+\sqrt{2}\mathbb{R}(\alpha), \tag{2.39}$$

$$D^{\dagger}(\alpha)\hat{p}D(\alpha) = \hat{p}+\sqrt{2}\mathbb{I}(\alpha). \tag{2.40}$$

Hence, the coherent state $|\alpha\rangle$ can be obtained by displacing the vacuum state, $|0\rangle$, in the phase space by $\sqrt{2}\mathbb{R}(\alpha)$ along the $\hat{q}$ axis and by $\sqrt{2}\mathbb{I}(\alpha)$ along the $\hat{p}$ axis.

Now, using Eq. (2.36), we can write the coherent state in the form of the number of states

$$|\alpha\rangle = \exp\left(-\frac{1}{2}|\alpha|^2\right)\sum_{n=0}^{\infty}\frac{\alpha^n(\hat{a}^{\dagger})^n}{n!}|0\rangle \tag{2.41}$$

which provides a coherent state as

$$|\alpha\rangle = \exp\left(-\frac{1}{2}|\alpha|^2\right)\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle \tag{2.42}$$

The probability of getting n photons in $|\alpha\rangle$ would be,

$$p_n = |\langle n|\alpha\rangle|^2 = \frac{|\alpha|^{2n}}{n!}\exp(-|\alpha|^2) \tag{2.43}$$

that comes out to Poissonian in nature with mean and variance equal to $|\alpha|^2$. Classical particles obey the same statistical law when they are taken at random with an average

of $|\alpha|^2$ each time. Hence, the coherent states are often referred to as quasi-classical states since, in addition to exhibiting Poisson distribution statistics, they also minimise the product of uncertainties in phase and amplitude, as governed by the uncertainty principle shown in Eq. (2.21). These properties are justified since the coherent states follow a wave-like nature. The statistics would lead to fluctuation in the source.

Another essential property of coherent states is that they are not orthogonal to each other because they are not eigenstates of a Hermitian operator.

$$\begin{aligned} \langle \alpha' | \alpha \rangle &= \langle 0 | \hat{D}^{\dagger}(\alpha') \hat{D}(\alpha) | 0 \rangle , \\ &= \langle 0 | D(\alpha' - \alpha) | 0 \rangle = \exp(-|\alpha' - \alpha|^2/2). \end{aligned} \tag{2.44}$$

These states may become orthogonal when their amplitudes differ sufficiently. Consequently,

$$|\langle \alpha' | \alpha \rangle|^2 = \exp(-|\alpha' - \alpha|)^2. \tag{2.45}$$

This falls to zero when the difference between the amplitudes α' and α is large compared to the quadrature noise level of the vacuum. Moreover, it is noted that the set of these states satisfies the completeness relations, which is given by

$$\frac{1}{2\pi} \int |\alpha\rangle \langle \alpha| \, dq_0 dp_0 = I. \tag{2.46}$$

Due to lack of orthogonality, the coherent states are even over-complete.

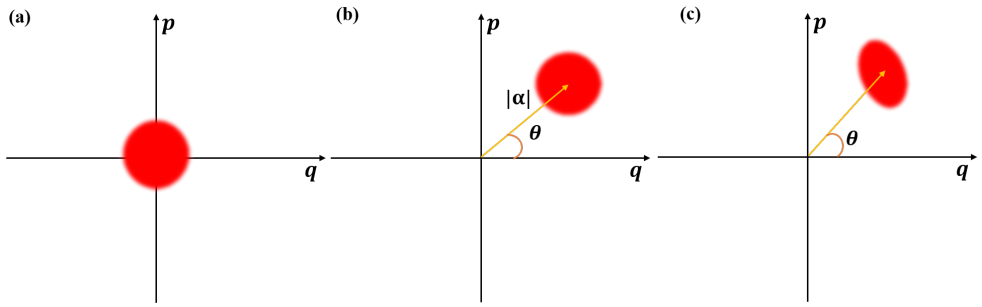

Figure 2.1: Phasor diagram of a (a) vacuum state, (b) coherent state, and (c) squeezed state.

2.2.4 Squeezed States

We have understood the properties of coherent states. They have only as much theoretical uncertainty in the quadrature amplitudes as the vacuum. A valid question then can be asked; Are the coherent states minimum uncertainty states? It is to be noted that the minimum uncertainty states act as displaced states, and contain Gaussian wave functions well like the coherent states. The minimum uncertainty states differ from the coherent state in a way that the former does not necessitate the variance, $\Delta^2 q$ to be $1/2$ like the latter. Hence, the variances in q and p are not required to be equal and $1/2$ to follow the Heisenberg uncertainty principle. Consequently, the statistical uncertainty of the quadrature, q, may be squeezed below the vacuum level $1/2$ at the cost of enhancing the uncertainty in the quadrature, p, and vice versa.

Therefore, squeezed states are defined as the quantum state with minimum uncertainty, and they hold the uncertainty relation defined for coherent states but with unequal uncertainty in both quadratures. These states can be generated by first applying the squeezing operator, denoted as $S(\varepsilon)$, with the squeezing parameter $\varepsilon = re^{2i\theta}$, and then applying the displacement operator to a vacuum state. The squeezing operator is

defined as

$$\hat{S}(\varepsilon) = \exp\big(\frac{1}{2}(\varepsilon^* \hat{a}^2 - \varepsilon \hat{a\dagger}^2)\big). \tag{2.47}$$

The squeezing operator applied directly to a vacuum state produces a state known as the squeezed vacuum state, represented as $S(r)|0\rangle$. For a squeezing factor $r > 0$, the variance of the squeezed quadrature decreases below shot noise unit ($e^{-2r} < 1/2$). In order to satisfy the Heisenberg uncertainty relation, the variance of conjugate quadrature must increase with the squeezing ($e^{2r} > 1/2$). In a Fock state basis, squeezed vacuum state is given by,

$$S(r)|0\rangle = \frac{1}{\sqrt{\cosh r}} \sum_{n=0}^{\infty} \frac{\sqrt{(2n)!}}{2^n n!} \tanh^n r |2n\rangle \tag{2.48}$$

The mean number of photon $\langle \hat{N} \rangle$ in a squeezed state is calculated by using the definition of the number operator,

$$\langle \hat{N} \rangle = \frac{1}{2}\big[\langle (\hat{x}^2 + \hat{p}^2) \rangle - 1\big] = \sinh^2 r \tag{2.49}$$

When the squeezing operator is applied to a coherent state, it results in the scaling of the quadratures, characterised by the squeezing factor r, and a rotation by θ. The state is called squeezed coherent state. The variance of both quadratures is defined by

$$\begin{aligned} \Delta q &= e^{-r}, \\ \Delta p &= e^{r} \end{aligned} \tag{2.50}$$

A more straightforward approach to creating the squeezed coherent states is achieved by applying a displacement operator $D(\alpha)$ to a squeezed vacuum state, denoted as

$(D(\alpha)S(r)|0\rangle)$.

2.3 Quantum States and its Measurement

With this brief idea of various representations of states of the EM field, we now understand how these states are used in the language of QKD.

2.3.1 Quantum State

In the classical picture, information is encoded in bits [105], which is composed of a two-level system. One of the examples is a coin with a head and tail as a two-level system. On the other hand, in the quantum picture, a qubit, analogous to a bit, is used. It describes a two-level system, including the superposition state between the two. In principle, the quantum state is described by a state vector in the Hilbert space. The Hilbert space is an infinite dimensional complex vector space with an inner product having the property that it is complete or closed. Hence, an arbitrary qubit state can be written in terms of orthogonal basis $|0\rangle, |1\rangle$ as

$$|\Phi\rangle = a|0\rangle + b|1\rangle, \tag{2.51}$$

with the normalization of the state: $\langle\Phi|\Phi\rangle = 1$, where $\langle\Phi|$ is defined as a dual of $|\Phi\rangle$.

The evolution of a quantum state is governed by the Schrödinger equation:

$$i\hbar\frac{d|\Phi\rangle}{dt} = \hat{H}|\Phi\rangle. \tag{2.52}$$

In the above equation, $\hbar$ represents Planck's constant, and $\hat{H}$ is the Hamiltonian operator, which is Hermitian (i.e., $\hat{H}^\dagger = \hat{H}$). Further, this equation can be simplified in

terms of $|\Phi'(t')\rangle = \mathscr{U}(t',t)\,|\Phi(t)\rangle$, where $\mathscr{U}(t,t')$ is defined as the evolution operator stating the evolution of state from t to t'. The evolution of the quantum state is provided by two interpretations: the Heisenberg picture and the Schrodinger picture. The former picture involves the time evolution of the operator, whereas the latter involves the time evolution of the state vector. For discrete variables, the Schrodinger picture is found to be useful. On the other hand, the Heisenberg picture is found to be useful for continuous variables.

2.3.2 Measurement

In quantum mechanics, the description of a quantum state involves a set of measurement operators denoted as $\hat{M}_m$, where "m" represents the index of possible measurement outcomes. Let's consider the example from Eq. (2.51) with a family of measurement operators: $\hat{M}_1 = |1\rangle\langle 1|$ and $\hat{M}_0 = |0\rangle\langle 0|$. It should be noted that in QM, the state of a system is not predetermined, but the measurement operators determine the probabilities associated with obtaining measurement results of either 1 or 0.

$$\begin{aligned} p(1) &= \langle\phi|\hat{M}_1^\dagger \hat{M}_1|\phi\rangle = |b|^2 \\ p(0) &= \langle\phi|\hat{M}_o^\dagger \hat{M}_o|\phi\rangle = |a|^2 \end{aligned} \tag{2.53}$$

Upon performing a measurement, the quantum state undergoes a transformation based on the obtained result, resulting in a modified state given by

$$\frac{\hat{M}_m\,|\phi\rangle}{\sqrt{\langle\phi|\hat{M}_m^\dagger \hat{M}\,|\phi\rangle}} \tag{2.54}$$

If we obtain a measurement result of 0, the quantum state will collapse to $|0\rangle$. Similarly, if the measurement outcome is 1, the state will collapse to $|1\rangle$.

2.4 Entanglement

Entanglement is a fundamental concept in quantum mechanics, arising when composite quantum systems interact and become inseparable, leading to the formation of entangled states. Mathematically, entangled states are described as a superposition of product states, given by $|\psi\rangle = \sum_{i,j} C_{i,j} |i\rangle \otimes |j\rangle$, where $C_{i,j}$ represents the complex coefficients and $|i\rangle$ and $|j\rangle$ denote the individual states of the constituent systems. These entangled states defy a separable representation and exhibit nontrivial correlations that transcend classical boundaries.

The entanglement of composite states is quantified using various measures, such as entanglement entropy, concurrence, or entanglement negativity [52]. These measures provide a quantitative assessment of the amount of entanglement present in a given state, highlighting the degree of correlation and nonlocality between the constituent systems. Entanglement plays a pivotal role in many aspects of quantum information processing. For instance, in quantum computing, entanglement enhances computational power by allowing quantum operations on the entire entangled system. In quantum cryptography, entanglement-based protocols, such as quantum key distribution, provide secure communication channels that are inherently resistant to eavesdropping due to the entanglement-based detection of any unauthorized interference.

2.5 Linear Operations

In the upcoming section, we will provide a comprehensive explanation of the set of linear and Gaussian operations [32] applicable to a multi-mode optical field. Building upon the states discussed in Sec. 2.2, these states can be combined with other states through the utilization of unitary operators. By employing these operations, the optical

field can be manipulated in a manner that preserves linearity and Gaussian characteristics. Here we will discuss two important operations that will be used in the thesis, phase shift operation and beam splitter operation.

2.5.1 Phase Shift

The phase shift operator is parametrized by a parameter θ. The phase shifting operator is defined as,

$$\hat{U}(\theta) = exp(-i\theta\hat{n}) \tag{2.55}$$

As the name suggests, the phase shifting operator provides the amplitude $\hat{a}$ with a phase shift θ when acting on $\hat{a}$,

$$\hat{U}^{\dagger}(\theta)\hat{a}\hat{U}(\theta) = \hat{a}exp(-i\theta) \tag{2.56}$$

Phase shifting rotates the quadratures,

$$\hat{q}_{\theta} \equiv \hat{U}^{\dagger}(\theta)\hat{q}\hat{U}(\theta) = \hat{q}\cos\theta + \hat{p}\sin\theta \tag{2.57}$$

$$\hat{p}_{\theta} \equiv \hat{U}^{\dagger}(\theta)\hat{p}\hat{U}(\theta) = -\hat{q}\sin\theta + \hat{p}\cos\theta \tag{2.58}$$

We see that we can go from a position representation to a momentum representation via a phase shift θ of $\pi/2$.

2.5.2 Beam Splitter

A beam splitter is a fundamental and commonly used optical element in various optics experiments. It functions by combining or splitting a beam of light using a partially

transparent surface with a transmission parameter, $0 \leq T \leq 1$, and a reflectivity parameter, $R = 1 - T$. A beam splitter is a four-port device with two input ports and two output ports, as shown in Fig. 2.2. When a beam splitter with a transmission parameter T is applied to two optical fields with annihilation operators $\hat{a}_{\text{in}}$ and $\hat{b}_{\text{in}}$, the transformation is given by:

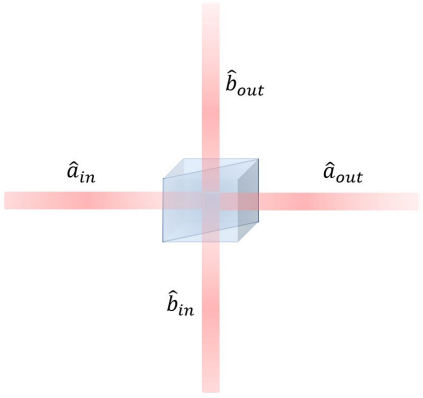

Figure 2.2: Beam splitter model. $\hat{a}_{\text{in}}$ and $\hat{b}_{\text{in}}$ are the input modes. $\hat{a}_{\text{out}}$ and $\hat{b}_{\text{out}}$ are the output modes.

$$\begin{pmatrix} \hat{a}_{\text{out}} \\ \hat{b}_{\text{out}} \end{pmatrix} = \begin{pmatrix} \sqrt{T} & \sqrt{1-T} \\ -\sqrt{1-T} & \sqrt{T} \end{pmatrix} \begin{pmatrix} \hat{a}_{\text{in}} \\ \hat{b}_{\text{in}} \end{pmatrix}. \tag{2.59}$$

The beam splitter operator is crucial in experimental modeling as it allows us to account for losses. In any experimental setup, there are various sources of loss, such as scattering from optical components, spatial mode matching, and inefficient detection. By using the beam splitter operator, we can effectively model these losses and understand how a vacuum or thermal state from the environment can couple into the signal mode.

2.6 Gaussian Operators

A Gaussian operation is a transformation that takes a Gaussian state and maps it to another Gaussian state, preserving the Gaussian characteristics of the input state. The corresponding operators for different cases are given here.

2.6.1 Displacement Operator

The displacement operator used to generate the coherent states simply translates the mean of the state,

$$\begin{aligned} \hat{x}|_{out} &= \sqrt{T}\hat{x}|_{in} + d_x \\ \hat{p}|_{out} &= \sqrt{T}\hat{p}|_{in} + d_p \end{aligned} \tag{2.60}$$

where, T is transmission coefficient, d is displacement in quadratures, x and p, i.e., $(d_x, d_p) = \sqrt{2}(\mathbb{R}(\alpha), \mathbb{I}(\alpha))$. Moreover, under the displacement operator, the covariance matrix of a Gaussian state remains invariant.

2.6.2 Symplectic Transform

In the context of Gaussian quantum information, symplectic operators correspond to unitary operators in Hilbert-space notation [45]. A matrix S is considered symplectic if it satisfies the relation

$$S\Omega S^T = \Omega \tag{2.61}$$

where, Ω is a fixed $2n \times 2n$ nonsingular, skew-symmetric matrix having form

$$\Omega = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}. \tag{2.62}$$

A symplectic operation transforms a Gaussian state as follows:

$$\hat{X} \to S\hat{X}, \quad \text{and} \tag{2.63}$$

$$\Sigma \to S\Sigma S^T. \tag{2.64}$$

In this context, the matrix S is a $2N \times 2N$ matrix with real elements. Moreover, the determinant of every symplectic matrix is $\det S = 1$. The symplectic operations corresponding to the passive operations described in Section 2.5 are provided below.

Phase Shift: The symplectic operator for a single-mode state undergoing a phase shift of θ corresponds to a rotation between the quadratures. It is given by:

$$S_{PS}(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \tag{2.65}$$

The symplectic operator for a beam splitter with transmission T is having form mentioned in Eq. (A.1).

Squeezing Operator: The symplectic operator for squeezing a single-mode state is expressed as follows:

$$S_{Sq}(r) = \begin{pmatrix} e^{-r} & 0 \\ 0 & e^{r} \end{pmatrix} \tag{2.66}$$

The unitary squeezed state operator, S_{Sq}, also acts as a phase shift on the input state.

Two Modes Squeezed States: By combining different symplectic operators, one can construct various Gaussian states. For instance, a two-mode squeezed state can be generated by combining two orthogonally squeezed states using a beam splitter. The symplectic operator is given by,

$$S_{\mathrm{BS}}(r) = \begin{pmatrix} \cosh(r)\mathbb{I} & \sinh(r)\sigma_z \\ \sinh(r)\sigma_z & \cosh(r)\mathbb{I} \end{pmatrix}. \tag{2.67}$$

where, $\mathbb{I}$ is 2×2 identity matrix. The superscript in the symplectic operator notation indicates the mode on which the operator is acting. The matrix σ_z is written as

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.68}$$

2.7 Generation & Detection of Light

Light is a wonderful object to perform experiments with [24]. Lasers can generate light of superb quality, optical devices can process light with great precision, and highly efficient detectors are available to measure the quantum properties of light. Classical optics is well well-established century-old theory, so we understand very well the classical features of light and can focus on the non-classical quantum effects. This is the reason that many fundamental concepts of quantum mechanics have been realized through quantum optics. So quantum optics has much to offer to those who are interested in practical demonstrations of fundamental quantum principles. Moreover, light is the most likely candidate for practical applications of state measurements. Light is a typical high-technology tool to investigate or to change various properties of matter. By gaining as much information as possible about, we can better explain the

behavior of material probes. Additionally, because light is used for communication, certainly worth studying is how to extract the maximal information allowed by the very principles of quantum mechanics.

2.7.1 Generation of Light

In order to prepare the quantum state for QKD protocols, one requires a single-photon source which is difficult to generate experimentally. One of the alternatives to the problem is to use weak coherent pulses (WCP) or SPDC sources (heralded single-photon sources). The details of both processes are given below.

Weak Coherent Pulses

WCP are attenuated laser pulses that are assumed to carry a single-photon in a given pulse. Many well-known QKD protocols use weak coherent laser pulses to encode the quantum state [106, 107]. These sources differ from the ideal single-photon sources and follow the Poisson statistics. A highly attenuated pulsed laser source is used to

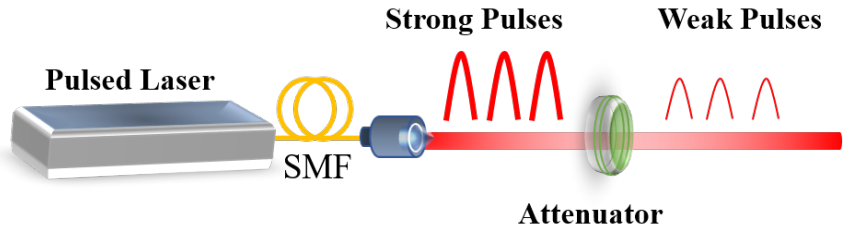

Figure 2.3: Generation of weak coherent pulses.

realize these weak coherent pulses. There is a non-zero probability, however low, to get more than a single-photon in a pulse.

Spontanoeus Parametric Down-Conversion (SPDC) Process

One of the methods of generating a single-photon is the SPDC process [108, 109]. This is a nonlinear process where an input 'pump' photon of high energy passing through a nonlinear second-order crystal creates two lower energy photons, signal, and idler, at the output. The process is called 'spontaneous' because both the photons are created

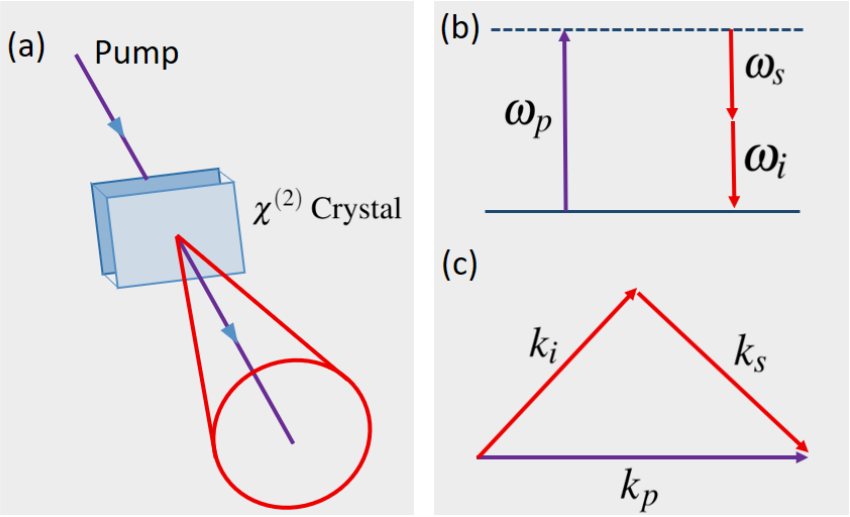

Figure 2.4: (a) Generation of entangled photon pair in spontaneous parametric down-conversion SPDC process. Phase matching condition in this process derives from (b) energy conservation and (c) momentum conservation.

spontaneously. There are no initial signal and idler fields to stimulate the generation of down-converted photons. They are generated from vacuum energy fluctuations. The term 'parametric' indicates that the nonlinear interaction between the photons and the crystal does not add or subtract energy or momentum. The term 'down-conversion' means that the generated signal and idler photon pairs must have a lower frequency than the pump photon according to energy conservation.

In a nonlinear medium, the dielectric polarisation vector is expanded as a power

series in terms of the electric field.

$$P(t) \propto \chi^{(1)}E(t) + \chi^{(2)}E^2(t) + \chi^{(3)}E^3(t) + ... \tag{2.69}$$

In this representation, the coefficients $\chi^{(n)}$ correspond to the n-th order susceptibilities of the medium. The linear optical transformations are captured by the $\chi^{(1)}$ term, while the higher-order terms account for the nonlinear effects in the medium. $\chi^{(2)}$ is the second-order susceptibility of the crystal which arises due to the dipole moment per unit volume (or polarisation) induced by the electric field of light propagating through the crystal.

Consider that the pump field is quantised. The SPDC process requires photon-crystal interaction. Therefore, the interaction Hamiltonian can be written as

$$\hat{H} \sim \chi^{(2)}\hat{a}_p\hat{a}_s^\dagger\hat{a}_i^\dagger + H.c. \tag{2.70}$$

where $H.c.$ is the Hermitian conjugate. $\hat{a}_p$ is the annihilation operator of the pump photon. $\hat{a}_s^\dagger$ and $\hat{a}_i^\dagger$ are the creation operator of the signal and idler photons respectively. Because of the 'spontaneous' nature of the process, the signal and idler are initially in vacuum states, and during the interaction with the crystal, the pump photon annihilates and gets converted into two photons, signal and idler,

$$|1\rangle_p|0\rangle_s|0\rangle_i \rightarrow \hat{a}_p\hat{a}_s^\dagger\hat{a}_i^\dagger|1\rangle_p|0\rangle_s|0\rangle_i = |0\rangle_p|1\rangle_s|1\rangle_i. \tag{2.71}$$

Both the photons, signal and idler, are assumed to be created simultaneously. Because of the simultaneous generation, the correlation between both the photons in various degree of freedom have been maintained. This correlation in various DoFs such as polarisation, OAM, path, time etc. leads to the entanglement between both the photons.

Phase-Matching: SPDC process follows energy and momentum conservation. According to the conservation law, the sum of the energy of the signal and idler must be equal to the energy of the pump photon. Similarly, the sum of the momentum of the signal and idler photon must be equal to the momentum of the pump photon. These two conservations are jointly known as phase-matching conditions [110].

$$\begin{aligned} \omega_p &= \omega_s + \omega_i, \\ \overrightarrow{k}_p &= \overrightarrow{k}_s + \overrightarrow{k}_i. \end{aligned} \tag{2.72}$$

where ω_p, ω_s and ω_i are the frequency and $\overrightarrow{k}_p$, $\overrightarrow{k}_s$ and $\overrightarrow{k}_i$ are the wave vector of pump, signal and idler respectively. Both the photons that emerge from the crystal go along different directions following momentum conservation.

Depending upon the crystal structure and orientation of optic axis, there are three types of SPDC: **Type-**0 **Phase Matching:** In Type-0 SPDC process, signal, idler and pump all have same polarisation. The joint state of SPDC photons for horizontally polarised pump is written as,

$$|\psi\rangle_{\text{SPDC}} = |H\rangle_s |H\rangle_i , \tag{2.73}$$

For a vertically polarised pump, the state becomes,

$$|\psi\rangle_{\text{SPDC}} = |V\rangle_s |V\rangle_i . \tag{2.74}$$

Type-I Phase Matching: In Type-I SPDC process, signal and idler have same polarisation but orthogonal to the pump polarisation. The joint state of SPDC photons for

horizontally polarised pump is written as,

$$|\psi\rangle_{\text{SPDC}} = |V\rangle_s |V\rangle_i , \tag{2.75}$$

For vertically polarised pump, the state becomes:

$$|\psi\rangle_{\text{SPDC}} = |H\rangle_s |H\rangle_i , \tag{2.76}$$

The states given in Eq. (2.75) and (2.76) are not entangled. If two Type-I crystals joined together have an optical axis perpendicular to each other then one can generate a polarisation-entangled state using diagonal/anti-diagonal pump polarisation. The joint state of SPDC photons with two crystals stacked together is written as,

$$|\psi\rangle_{\text{SPDC}} = c_1 |H\rangle_s |H\rangle_i \pm c_2 |V\rangle_s |V\rangle_i . \tag{2.77}$$

For maximally entangled state $c_1 = c_2 = 1/\sqrt{2}$. This method was first demonstrated by Kwiat et.al.

Type-II Phase Matching: In Type-II SPDC process, signal and idler have orthogonal polarisation. Both the photons are emitted along two different cones due to the birefringent property of the nonlinear crystal. And the intersection of cones provides the polarisation entangled state. The joint state of SPDC photons of these intersecting points is written as

$$|\psi\rangle_{\text{SPDC}} = \frac{1}{\sqrt{2}} \left(|H\rangle_s |V\rangle_i \pm |V\rangle_s |H\rangle_i \right) . \tag{2.78}$$

Type-II crystal is most commonly used for the generation of the polarisation-entangled state.

2.7.2 Detection of Light

What are photons? Photons, in simple terms, are the fundamental units that trigger a photon counter to click. To understand photons, it is crucial to consider the process of detection. In a laboratory setting, photons are not directly detected; instead, they are typically converted into electrical signals, which are then detected and analysed [111]. This allows us to retrieve the information encoded in the light and carried by the photons. Light travels as a high-frequency electromagnetic wave, and can be detected using two methods: field detection and intensity detection. Field detection enables the measurement of both the amplitude and phase information of the light, while intensity detection only provides information about the light's intensity, without any phase details. Broadly speaking there are two different ways of recording the light. One is the detection of individual photons, while the other involves measuring the currents generated by a stream of photons. The choice between these methods depends on factors such as the time response of the photo-detector and the magnitude of the photon flux. Each technology has its own applications and is employed accordingly.

Single Photon Detection

The measurement of the Fock basis (photon number states) is facilitated by a specific type of detector known as a photon-resolution detector. This detector is designed to distinguish and discriminate between different Fock states, denoted as $|n\rangle$. However, accurately determining the photon number presents significant challenges, and there is currently no detector capable of efficiently achieving this task [112–114]. Instead, a more practical objective is the use of a photon-sensitive detector (Fig. 2.5) that can differentiate between the absence of photons ($|0\rangle$) and the presence of one or more

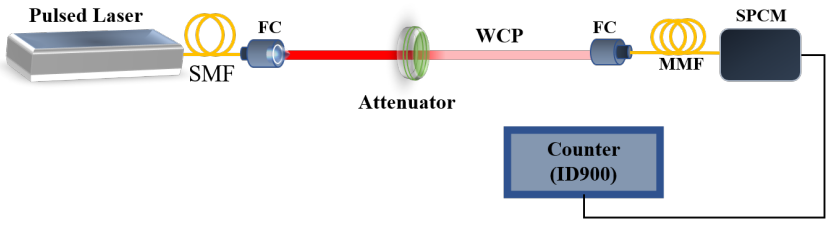

Figure 2.5: Detection of weak coherent pulses by single-photon detector; SMF: Single-mode Fiber; FC: Fiber Coupler; WCP: Weak Coherent Pulses; MMF: Multi-mode Fiber; SPCM: Single-Photon Detector.

photons. Avalanche photodetectors (APDs) are currently employed to achieve photon sensitivity, although even this poses technical difficulties. APDs work on the principle of reverse bias voltage breakdown. They are heavily doped PiN photodetectors that produce more electron-hole pairs for conduction with just a single incident photon. APDs are meticulously calibrated to achieve single-photon detection capability.

Realistic APDs encounter two primary sources of errors. First, not all photons that reach the detector initiate an avalanche. The efficiency (η_{APD}) of the detector represents the ratio of detected photons to the incoming photons count. This efficiency is modeled as a beam splitter with a transmittance (η_{APD}) placed before an ideal detector. The second source of error arises from what is known as dark counts. These correspond to spontaneous clicks that occur without any incident photon triggering them. Fortunately, the influence of dark counts can be reduced to an insignificant level by triggering the detector only when an incoming pulse is anticipated.

Quadrature Detection: Homodyne Detection

Balanced Homodyne Detection (BHD) [36, 115] is a well-known and efficient technique to measure the field quadratures of the electromagnetic oscillator.

Mathematical Treatment of BHD: In a standard BHD, the signal 'a' under study

interferes at a 50% beam-splitter with a strong coherent reference beam 'b', known as the LO, as illustrated in Fig. 2.6. The resulting outputs are collected by two photodetectors, and the difference in the photocurrents is directly related to the field quadrature $\langle \hat{x}_\phi \rangle$. Here, ϕ is determined by the phase difference between the LO and the signal, and it can be easily adjusted by varying the optical path length of the LO. The annihilation

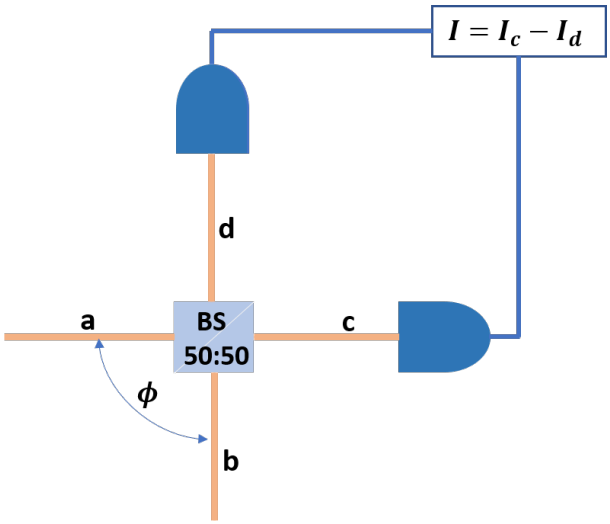

Figure 2.6: Balance homodyne detection scheme.

operators at the two output port of the beam splitter are written in terms of inputs,

$$\hat{c} = \frac{1}{\sqrt{2}}(\hat{a} + \hat{b}), \qquad \hat{d} = \frac{1}{\sqrt{2}}(\hat{b} - \hat{a}), \tag{2.79}$$

After the BS, the two modes are detected by two identical photodetectors. The two photocurrents are measured and subtracted from each other. The photocurrents I_c and I_d are proportional to the photon number observables $\hat{n}_c = \hat{c}^\dagger \hat{c}$ and $\hat{n}_d = \hat{d}^\dagger \hat{d}$.
The difference photocurrent $\hat{I}$ is written as,

$$\hat{I} = \hat{n}_c - \hat{n}_d = \hat{c}^\dagger \hat{c} - \hat{d}^\dagger \hat{d}, \tag{2.80}$$

Using equation Eq. (2.79), it simplifies to,

$$\hat{I} = \hat{b}^\dagger \hat{a} + \hat{a}^\dagger \hat{b},$$

Introducing the phase in the LO arm,

$$\hat{b} \to \hat{b}e^{i\phi}, \qquad \hat{b}^\dagger \to \hat{b}^\dagger e^{-i\phi} \tag{2.81}$$

The photocurrent operator now becomes,

$$\hat{I}_\phi = \hat{a}^\dagger \hat{b}e^{i\phi} + \hat{b}^\dagger \hat{a}e^{-i\phi} \tag{2.82}$$

This is the observable that we are actually measuring here. Now, we have to see the relation of the photocurrent to the quadratures. Consider, the signal mode is given by state ρ_s, and LO mode is given by $z = \frac{1}{\sqrt{2}}(\hat{q} + i\hat{p})$. The expectation value of photocurrent would be given by,

$$\begin{aligned} \langle \hat{I}_\phi \rangle &= Tr\left[\hat{\rho}_s \otimes |z\rangle\langle z| \hat{I}_\phi\right] \\ &= \sqrt{2}|z| Tr\left[\hat{\rho}_s \hat{x}_\phi\right] \\ &= \sqrt{2}|z| \langle \hat{x}_\phi \rangle \end{aligned} \tag{2.83}$$

From the Eq. (2.83), we can see that $\langle \hat{I}_\phi \rangle$ is nothing but scaled $\langle \hat{x}_\phi \rangle$, with the rescaling factor $\sqrt{2}|z|$.

This $\langle \hat{x}_\phi \rangle$ is having form,

$$\langle \hat{x}_\phi \rangle = \hat{q}\cos\phi + \hat{p}\sin\phi \tag{2.84}$$

Calculating the second moment $\langle \hat{x}_\phi^2 \rangle$ (fluctuation of quadrature i.e variance), it would

comes out,

$$\langle \hat{I}_{\phi}^{2} \rangle = \langle \hat{x}_{\phi}^{2} \rangle + \langle \frac{\hat{a}^{\dagger}\hat{a}}{2|z|^{2}} \rangle \tag{2.85}$$

This implies that homodyne photocurrent coincides with quadrature moment only, when the signal mode satisfies,

$$\langle \hat{a}^{\dagger}\hat{a} \rangle \ll |z|^{2} \tag{2.86}$$

Changing the phase of the local oscillator with respect to the signal we would get the quadrature value $\hat{q}$ or $\hat{p}$ for different ϕ values.

Section II - Tools for QKD

In QKD, once the process of key establishment is done the further post-processing of the key is performed to get the secure key. In DVQKD, the key is directly obtained in binary form and one can do the error correction and privacy amplification to obtain the final key. Whereas, in CVQKD the key is obtained in terms of Gaussian random numbers, called the key elements. There are various steps to reach the final secure key which include, parameter estimation, reconciliation, error correction, and privacy amplification. In this Section, we will discuss the steps involved in the process of secure key extraction.

2.8 Shannon Information

The field of Information Theory was originally established by the works of Harry Nyquist and Ralph Hartley, in the 1920s, and Claude Shannon in 1948 [16, 116, 117]. Information theory offers a mathematical framework for quantifying information through Shannon entropy, which measures the information of a random variable X. For a random variable, the entropy is defined as

$$H(X) = -\sum_{x} p(x)\log_2 p(x) \tag{2.87}$$

where, $p(x)$ is the probability of the X having the outcome x. The event X could be a coin toss, die roll, etc. Given $H(X) = 1$ implies that the variable X is maximally random. The relation for Shannon entropy holds for multiple variables. For the two random variables X and Y, the **joint entropy** is given by,

$$H(X,Y) = -\sum_{x,y} p(x,y)\log_2 p(x,y) \tag{2.88}$$

In the case where X and Y are independent, the joint entropy is equal to the sum of their individual entropies.

Conditional entropy is another significant parameter, defined as the uncertainty of variable X when the outcome of variable Y is known.

$$H(X/Y) = -\sum_{x,y} p(x,y)\log_2 \frac{p(x,y)}{p(y)} \tag{2.89}$$

Therefore, one can proceed to define the **mutual information**, which quantifies how much information can be obtained from variable X by observing variable Y, considering both variables X and Y. In practical terms, this is commonly explained as the shared information between variables X and Y.

$$H(X;Y) = I(X;Y) = -\sum_{x,y} p(x,y)\log_2 \frac{p(x,y)}{p(x)p(y)} \tag{2.90}$$

Mutual information, conditional entropy, and joint entropy hold the following relations:

$$\begin{aligned} H(X/Y) &= H(X,Y) - H(Y) \\ I(X;Y) &= H(X) - H(X/Y) = H(X) + H(Y) - H(X,Y) \\ H(X,Y) &\leq H(X) + H(Y) \end{aligned} \tag{2.91}$$

2.8.1 Shannon Entropies for Gaussian States

The Shannon entropy for a variable X which is described by a Gaussian distribution with variance σ^2 and mean zero is defined as,

$$H(X) = \frac{1}{2}\log_2\sigma^2 + C \tag{2.92}$$

where C represents an arbitrary constant. To extend this concept to a two-mode state, we define the covariance matrix (details are given in Sec.2.10.2). The covariance matrix represents the joint entropy for variables X and Y with covariance $C_{X,Y}$, which is defined as

$$\Sigma = \begin{pmatrix} {\sigma^2}_X & C_{X,Y} \\ {C^T}_{X,Y} & {\sigma^2}_Y \end{pmatrix} \tag{2.93}$$

The joint entropy is given by

$$H(X,Y) = \frac{1}{2}\log_2\det[\Sigma] + C" \tag{2.94}$$

where C" represents an arbitrary constant. Likewise, the conditional entropy is defined as,

$$H(Y/X) = \frac{1}{2}\log_2\sigma^2_{Y/X} + C \tag{2.95}$$

where, C represents an arbitrary constant, and $\sigma^2_{Y/X}$ is the conditional variance

$$\sigma^2_{Y/X} = \sigma^2_Y - \frac{C_{X,Y}}{\sigma^2_X} \tag{2.96}$$

Finally, the mutual entropy is written as,

$$\begin{aligned} H(X:Y) &= H(Y) - H(Y/X) = \frac{1}{2}\log_2 \frac{\sigma_Y^2}{\sigma_{Y/X}^2} \\ &= H(X) - H(X/Y) = \frac{1}{2}\log_2 \frac{\sigma_X^2}{\sigma_{X/Y}^2} \\ &= H(X) + H(Y) - H(X,Y) = \frac{1}{2}\log_2 \frac{\sigma_Y^2 \sigma_X^2}{\det\Sigma}. \end{aligned} \tag{2.97}$$

2.9 Quantum Information

Similar to the classical case, the information carried by a quantum state is measured by using von Neumann entropy [18, 118]. The entropy of a state described by a density operator, ρ is given by

$$S(\rho) = -\mathrm{tr}(\rho \log_2 \rho). \tag{2.98}$$

The following relations hold for conditional, joint, and mutual von Neumann entropy

$$\begin{aligned} S(A,B) &= -\mathrm{tr}(\rho^{AB} \log_2 \rho^{AB}) \\ S(A/B) &= S(A,B) - S(B) \\ S(A:B) &= S(A) + S(B) - S(A,B) \end{aligned} \tag{2.99}$$

In the context of von Neumann entropy, conditional entropy can be negative, and it is often regarded as an indication of entanglement.

2.9.1 Holevo Bound

The Holevo bound holds significant importance in quantum information as it sets an upper limit on the accessible information. This bound is particularly crucial for QKD. When Alice prepares a series of states ρ_x, and Bob performs a measurement to obtain outcome Y, the accessible information available to Bob is bounded by the following relation,

$$H(a:b) \leq S(a:B) = \chi(a:B) = S(\rho) - \sum_x p_x S(\rho_x) \tag{2.100}$$

where $\rho = \sum_x p_x \rho_x$ and $\chi(a:B)$ represents the Holevo quantity. In this context, classical states are denoted by lowercase letters to distinguish them from quantum states, which are represented by uppercase letters.

2.9.2 von Neumann Entropy for Gaussian States

A Gaussian state can be represented as a tensor product of thermal states [32]. The covariance matrix Σ, which characterises the Gaussian state, can be written as follows,

$$S\Sigma S^T = \otimes_{k=1}^{N} \lambda_k \mathbb{1} \tag{2.101}$$

where each $\lambda_k \mathbb{1}$ is the covariance matrix of a thermal state and λ_k is a symplectic eigenvalue of Σ. For a N mode thermal state ρ the entropy is given by

$$S(\rho) = \sum_{k=1}^{N} S(G(\lambda_K - 1)/2) \tag{2.102}$$

where

$$G(x) = (x+1)\log_2(x+1) - x\log_2 x \tag{2.103}$$

Symplectic Eigenvalues

The symplectic eigenvalues of the matrix Σ are obtained by diagonalizing it with a symplectic transform S as shown in Eq. (2.101). Determining the symplectic eigenvalues is a straightforward process for both one and two-mode states.

Single-Mode State

The symplectic eigenvalue for a single-mode state can be obtained simply by taking the square root of the determinant of the matrix Σ.

$$\lambda^2 = \det[\Sigma] \tag{2.104}$$

Two-Mode State

For two modes state, finding the symplectic eigenvalues is a more challenging task compared to single-mode states. We define the covariance matrix to find the symplectic eigenvalues. Consider the covariance matrix,

$$\Sigma = \begin{pmatrix} \Sigma_1 & C_{12} \\ C^T{}_{12} & \Sigma_2 \end{pmatrix} \tag{2.105}$$

We define the two symplectic invariants to find the symplectic eigenvalues.

$$\Delta = \lambda_1^2 + \lambda_2^2 = \det\Sigma_1 + \det\Sigma_2 \det C_{12} \tag{2.106}$$

$$\lambda_1^2 \lambda_2^2 = \det\Sigma \tag{2.107}$$

The symplectic eigenvalues are the solutions of the polynomials,

$$z^2 - \Delta z + \det\Sigma = 0 \tag{2.108}$$

With the solution,

$$\lambda_{1,2}^2 = \frac{1}{2}\left[\Delta \pm \sqrt{\Delta^2 - 4\det\Sigma}\right] \tag{2.109}$$

2.9.3 Secret Key Rate

The secret key rate for direct and reverse reconciliation in QKD is given by,

$$r_{DR} = I(A:B) - I(A:E) \tag{2.110}$$

$$r_{RR} = I(A:B) - I(B:E) \tag{2.111}$$

where, $I(A:B)$ is the mutual information shared between Alice and Bob and $I(A:E)$ is the Holevo bound giving the information leakage to Eve. The subscript RR denotes the reverse reconciliation and DR represents direct reconciliation. In RR Alice corrects his erroneous data after sifting by comparing it with Bob. Whereas, in DR Bob corrects his data after verifying it with Alice. For a secure QKD protocol, the quantity must be non-zero. For $r_{RR}, r_{DR} \geq 0$ implies that the mutual information between Alice and Bob, $I(A:B)$ must be greater than Alice and Eve $(I(A:E))$ and Bob and Eve $(I(B:E))$.

2.10 Secure Key Rate for CVQKD Protocols

The asymptotic secure key rate [30] for a CVQKD protocol is given by the relation,

$$K = \beta I(A:B) - I(B:E) \tag{2.112}$$

Here, β is the reconciliation efficiency, and $I(A:B)$ is mutual information shared between Alice and Bob. The factor $I(B:E)$ is the Holevo bound that would tell the information leakage due to the third party called Eve. To calculate the value of $I(A:B)$ & $I(B:E)$, we estimate the parameters for channel transmittance and the excess noise [45].

2.10.1 Transmittance and Noise

A CVQKD protocol is characterised by two important parameters, channel transmittance, and noise. The key rate of the protocol strongly depends on these two factors. The noise in the system is mainly contributed by two reasons: channel noise and detection noise. The detection noise is contributed due to the imperfections in the homodyne measurement and is controlled by the receiver (Bob). The channel noise is added in the channel during the transmission and could be due to a third-party intervention called Eve. The presence of Eve would introduce extra noise called excess noise. The total noise would be sum of the both channel noise and detector noise.

Channel noise is mainly contributed due to channel loss and excess noise, and could be defined as,

$$\Xi_{\text{ch}} = \frac{1 - T_{\text{ch}}}{T_{\text{ch}}} + \xi_A \tag{2.113}$$

where, the first term is the channel loss, and ξ_A is the excess noise introduced in the

channel which could be due to modulation noise or phase noise.

Detection noise is mainly contributed by lossdue to detector efficiency, or due to electronic noise ν_{el}.

$$\Xi_{\text{det}} = \frac{1-\eta_{\text{det}}}{\eta_{\text{det}}} + \frac{\nu_{\text{el}}}{\eta_{\text{det}}} \tag{2.114}$$

Total noise is,

$$\Xi = \Xi_{\text{ch}} + \frac{1}{T_{\text{ch}}}\Xi_{\text{det}} \tag{2.115}$$

T_{ch}, η_{det} and ν_{el} are known parameters whereas, ξ is an unknown parameter that needs to be estimated.

In order to estimate the values for channel transmittance and excess noise, we will consider the case for Gaussian modulation discussed in Chapter 1. The reduced form of Gaussian modulation could be applied to other modulation techniques as well.

As mentioned in Chapter 1, Sec. 1.4, the modulation variance of Alice's encoded state is V_{mod} (in the case of Gaussian modulation). In addition, the noise variance of the coherent state is $V_{\text{o}} = 1$ which comes due to the quantum fluctuations of the source known as shot noise. Once Alice's signal is transmitted through a lossy and noisy channel, Bob will measure the total quadrature variance.

$$\boxed{V_B = TV_{\text{mod}} + 1 + \xi} \tag{2.116}$$

where T is the channel transmittance given by

$$T = T_{\text{ch}}\eta_{\text{det}}\eta_{\text{coup}} \tag{2.117}$$

and ξ is the total excess noise that is contributed due to channel as well as detection losses. ξ could also be introduced by third-party intervention in between the channel.

2.10.2 Covariance Matrix

The bosonic multi-mode states are represented in terms of covariance matrices Σ. The diagonal terms of the covariance matrix give the variance of the quadrature and off-diagonal terms give mutual covariance function. Knowledge of Σ is essential to compute the Holevo bound. An N-mode Gaussian state is characterised by a displacement vector $\hat{x}$ and a covariance matrix of dim $2N$x$2N$.

$$\hat{\mathbf{x}} = (\hat{q}_1, \hat{p}_1, \hat{q}_2, \hat{p}_2, \ldots \hat{q}_N, \hat{p}_N)^T . \tag{2.118}$$

This satisfies the commutation relations.

$$\left[\hat{x}^j, \hat{x}^k\right] = 2i\Omega^{jk} \;\; ; \;\; \Omega = \bigoplus_{l=1}^{N} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{2.119}$$

The elements of the covariance matrix are given by

$$\begin{aligned} \Sigma^{ij} &= \frac{1}{2}\left\langle \left\{ \hat{x}^j - \langle \hat{x}^j \rangle, \hat{x}^k - \langle \hat{x}^k \rangle \right\} \right\rangle && (2.120) \\ &= \frac{1}{2}\left(\langle \hat{x}^j \hat{x}^k \rangle + \langle \hat{x}^k \hat{x}^j \rangle \right) - \langle \hat{x}^j \rangle \langle \hat{x}^k \rangle && (2.121) \\ &= E(\hat{x}^j, \hat{x}^k) && (2.122) \end{aligned}$$

The diagonal elements are given as,

$$\begin{aligned} \Sigma^{jj} &= \left\langle (\hat{x}^j)^2 \right\rangle - \left(\left\langle \hat{x}^j \right\rangle \right)^2 && (2.123) \\ &= V(\hat{x}^j) && (2.124) \end{aligned}$$

$$\Sigma_{AB} = \begin{array}{c} \\ \hat{q}_1 \\ \hat{p}_1 \\ . \\ . \\ . \\ . \\ \hat{p}_N \end{array} \begin{array}{c} \begin{array}{ccccc} \hat{q}_1 & \hat{p}_1 & ..... & \hat{p}_N \end{array} \\ \begin{pmatrix} V(\hat{q}_1) & E(\hat{q}_1,\hat{p}_1) & ..... & E(\hat{q}_1,\hat{p}_N) \\ E(\hat{p}_1,\hat{q}_1) & V(\hat{p}_1) & ..... & E(\hat{p}_1,\hat{p}_N) \\ . & . & ..... & . \\ . & . & ..... & . \\ . & . & ..... & . \\ . & . & ..... & . \\ E(\hat{p}_N,\hat{q}_1) & E(\hat{p}_N,\hat{p}_1) & ..... & V(\hat{p}_N) \end{pmatrix} \end{array} \tag{2.125}$$

Here, the diagonal elements give the variance of quadratures and the off-diagonal elements give the covariance of two quadratures.

For the prepare and measure Gaussian modulated coherent state protocol (GMCS), we can actually take a mathematically equivalent entanglement-based scheme. Alice prepares a two-mode squeezed vacuum state (TMSVS) and performs measurements on both quadratures of her mode using heterodyne detection [45]. She then sends the other mode to Bob. The covariance matrix for TMSVS is defined as,

$$\Sigma_{AB} = \begin{array}{c} \\ \hat{q_A} \\ \hat{p_A} \\ \hat{q_B} \\ \hat{p_B} \end{array} \begin{array}{c} \begin{array}{cccc} \hat{q_A} & \hat{p_A} & \hat{q_B} & \hat{p_B} \end{array} \\ \begin{pmatrix} V & 0 & \sqrt{V^2-1} & 0 \\ 0 & V & 0 & -\sqrt{V^2-1} \\ \sqrt{V^2-1} & 0 & V & 0 \\ 0 & -\sqrt{V^2-1} & 0 & V \end{pmatrix} \end{array} \tag{2.126}$$

$$= \begin{pmatrix} V\mathbb{1}_2 & \sqrt{V^2-1}\sigma_z \\ \sqrt{V^2-1}\sigma_z & V\mathbb{1}_2 \end{pmatrix} \tag{2.127}$$

where, σ_z represents the Pauli matrix and V denotes the variance of the quadrature operators. The variance of the quadratures q and p is defined by the relation,

$$V(\hat{q}) = \langle \hat{q}^2 \rangle - \langle \hat{q} \rangle^2 \qquad (2.128)$$
$$V(\hat{p}) = \langle \hat{p}^2 \rangle - \langle \hat{p} \rangle^2$$

For the GMCS case, the variance of both quadratures is equal and is the sum of actual Alice's modulation variance and shot noise variance,

$$V = V_{\text{mod}} + V_{\text{o}} = V_{\text{mod}} + 1 \qquad (2.129)$$

Hence the covariance matrix in Eq. 2.126 takes the form

$$\Sigma_{AB} = \begin{pmatrix} (V_{\text{mod}} + 1)\,\mathbb{1}_2 & \sqrt{\left(V_{\text{mod}}^2 + 2V_{\text{mod}}\right)}\sigma_z \\ \sqrt{\left(V_{\text{mod}}^2 + 2V_{\text{mod}}\right)}\sigma_z & (V_{\text{mod}} + 1)\,\mathbb{1}_2 \end{pmatrix}. \qquad (2.130)$$

When transmitting the state to Bob, the signal is influenced by the transmittance of the channel T as well as the excess noise ξ coming from imperfect modulation, detection noise, etc. By modeling this channel loss as the output of a beam splitter of transmittance T one can get a covariance matrix after transmission as follows,

$$\Sigma_{\text{AB}} = \begin{pmatrix} V_A\,\mathbb{1}_2 & \text{Cov}(A,B)\,\mathbb{1}_2 \\ \text{Cov}(A,B)\,\mathbb{1}_2 & V_B\,\mathbb{1}_2 \end{pmatrix} \qquad (2.131)$$
$$= \begin{pmatrix} (V_{\text{mod}} + 1)\,\mathbb{1}_2 & \sqrt{T\left(V_{\text{mod}}^2 + 2V_{\text{mod}}\right)}\sigma_z \\ \sqrt{T\left(V_{\text{mod}}^2 + 2V_{\text{mod}}\right)}\sigma_z & (TV_{\text{mod}} + 1 + \xi)\,\mathbb{1}_2 \end{pmatrix}.$$

Hence, for Gaussian modulation CVQKD, the covariance matrix can be defined by

Eq. 2.131 followed by the Gaussian distribution $Q \sim P \sim N(0, V_{\text{mod}})$ for the quadratures mentioned in Sec. 1.4. The matrix can be further reduced to represent the discrete modulation CVQKD.

2.10.3 Signal to Noise Ratio and Mutual Information

The SNR is simply described by,

$$SNR = \frac{P_S}{P_N} \tag{2.132}$$

where P_S is the total signal power and P_N is the total noise power arriving at the channel output.

The variance in Bob's quadrature (homodyne detection) was obtained previously as

$$V_B = V(\hat{q}_B) = V(\hat{p}_B) = TV_{\text{mod}} + 1 + \xi, \tag{2.133}$$

Here, TV_{mod} corresponds to the signal (with damped modulation) and $1+\xi$ is the added noise.

The SNR for the case of homodyne detection in Gaussian modulation is defined as

$$\text{SNR} = \frac{TV_{\text{mod}}}{1+\xi} \tag{2.134}$$

where, T denotes the transmittance, V_{mod} denotes the modulation variance of Alice's quadratres, ξ is the total excess noise.

The **mutual information** between Alice and Bob is given by the relation,

$$\begin{aligned} I_{AB} &= \frac{1}{2}\log_2(1+\mathrm{SNR}) \\ &= \frac{1}{2}\log_2(1+\frac{TV_{\mathrm{mod}}}{1+\xi}) \end{aligned} \tag{2.135}$$

2.10.4 Estimation of Holevo Bound

Holevo bound is the maximum information Eve can have on the shared key before privacy amplification. For reverse reconciliation, this is given by,

$$I_{EB} = S_E - S_{E|B}. \tag{2.136}$$

Here, S_E represents the von Neumann entropy of the state accessible to Eve and $S_{E|B}$ is the same after Bob has done his measurements (homodyne or heterodyne). The von Neumann entropy of a Gaussian state is given by the symplectic eigenvalues of its covariance matrix discussed in Sec. 2.9.2. For a covariance matrix Σ, the symplectic eigenvalues are defined as the modulus of the ordinary eigenvalues of the matrix.

$$\bar{\Sigma} = i\Omega\Sigma \tag{2.137}$$

Ω is defined in Eq. (2.119). Since only the modulus of the eigenvalues is considered, a $2N$x$2N$ covariance matrix will give only N symplectic eigenvalues (see Sec. 2.9.1). For a Gaussian state defined by a covariance matrix Σ, the von Neumann entropy is given by

$$S = \sum_i g(\nu_i) \tag{2.138}$$

with

$$g(\nu_i) = \frac{\nu+1}{2}\log_2\frac{\nu+1}{2} - \frac{\nu-1}{2}\log_2\frac{\nu-1}{2} \tag{2.139}$$

where, ν_i are the symplectic eigenvalues of Σ.

2.10.5 Equivalence of Coherent State and TMSVS Protocols

The security proofs against various attacks rely on an entanglement-based description of the protocol, which is formally equivalent to the prepare and measure scheme presented in the Chapter. So, Alice can go from a prepare and measure scenario to an entanglement-based scenario which is easier for doing security analysis. Therefore, Alice and Bob scale the quadrature values they obtained from experimental measurements, transforming Σ^{PM} to Σ^{EB}. The covariance matrix for prepare and measure protocol for transmission T and excess noise ξ is given by,

$$\Sigma^{\text{PM}} = \begin{pmatrix} V_{\text{mod}}\mathbb{1}_2 & \sqrt{\frac{T}{\mu}}V_{\text{mod}}\,\mathbb{1}_2 \\ \sqrt{\frac{T}{\mu}}V_{\text{mod}}\,\mathbb{1}_2 & \frac{T}{\mu}V_{\text{mod}} + 1 + \frac{\varepsilon}{\mu}\mathbb{1}_2 \end{pmatrix} = \begin{pmatrix} a^{\text{PM}}\mathbb{1}_2 & c^{\text{PM}}\mathbb{1}_2 \\ c^{\text{PM}}\mathbb{1}_2 & b^{\text{PM}_1} \end{pmatrix}. \tag{2.140}$$

Here $\mu = 1$ for homodyne detection and $\mu = 2$ for heterodyne detection. The entanglement-based TMSVS covariance matrix is given by,

$$\begin{aligned} \Sigma^{\text{EB}} &= \begin{pmatrix} V\mathbb{1}_2 & \sqrt{T}\sqrt{V^2-1}\sigma_z \\ \sqrt{T}\sqrt{V^2-1}\sigma_z & (T[V-1]+1+\xi)\mathbb{1}_2 \end{pmatrix} \\ &= \begin{pmatrix} (V_{\text{mod}}+1)\,\mathbb{1}_2 & \sqrt{T}\sqrt{V_{\text{mod}}^2+2V_{\text{mod}}}\sigma_z \\ \sqrt{T}\sqrt{V_{\text{mod}}^2+2V_{\text{mod}}}\sigma_z & (TV_{\text{mod}}+1+\xi)\,\mathbb{1}_2 \end{pmatrix} \end{aligned} \tag{2.141}$$

$$= \begin{pmatrix} a^{\mathrm{EB}}\mathbb{1}_2 & c^{\mathrm{EB}}\sigma_z \\ c^{\mathrm{EB}}\sigma_z & b^{\mathrm{EB}}\mathbb{1}_2 \end{pmatrix}$$

Alice proceed to find the values of $a^{\mathrm{EB}}, b^{\mathrm{EB}}$ and c^{EB}. Using the below transformation Alice can go from a prepare and measure scenario to an entanglement-based scenario which is easier for doing security analysis.

1. Since $a^{\mathrm{EB}} = V = V_{\mathrm{mod}} + 1$, this can be easily calculated by Alice.
2. Comparing Eq. (2.141) and Eq. (2.140) one can see $b^{\mathrm{EB}} = \mu b^{\mathrm{PM}} - \mu + 1$. Alice can calculate b^{PM} from the disclosed data by Bob and hence find b^{EB}.
3. To find c^{EB} Alice & Bob rescales their quadrature values as,

$$\begin{aligned} \hat{q}_A^{\mathrm{EB}} &= \sqrt{\frac{V+1}{V-1}}\hat{q}_A^{\mathrm{PM}} = \sqrt{\frac{V_{\mathrm{mod}}+2}{V_{\mathrm{mod}}}}\hat{q}_A^{\mathrm{PM}} \\ \hat{p}_A^{\mathrm{EB}} &= -\sqrt{\frac{V+1}{V-1}}\hat{p}_A^{\mathrm{PM}} = -\sqrt{\frac{V_{\mathrm{mod}}+2}{V_{\mathrm{mod}}}}\hat{p}_A^{\mathrm{PM}}, \\ \hat{q}_B^{\mathrm{EB}} &= \sqrt{\mu}\hat{q}_B^{\mathrm{PM}}, \\ \hat{p}_B^{\mathrm{EB}} &= \sqrt{\mu}\hat{p}_B^{\mathrm{PM}}, \end{aligned} \tag{2.142}$$

$$c^{\mathrm{EB}} = \langle \hat{q}_A^{\mathrm{EB}}\hat{q}_B^{\mathrm{EB}} \rangle = \sqrt{\frac{V_{\mathrm{mod}}+2}{V_{\mathrm{mod}}}}\sqrt{\mu}\langle \hat{q}_A^{\mathrm{PM}}\hat{q}_B^{\mathrm{PM}} \rangle \tag{2.143}$$

Alice will use the data disclosed by Bob to compute $\langle q_A^{\mathrm{PM}} q_B^{\mathrm{PM}} \rangle$ and $\langle p_A^{\mathrm{PM}} p_B^{\mathrm{PM}} \rangle$ and multiply the factor $\sqrt{(V_{\mathrm{mod}}+2)/V_{\mathrm{mod}}}\sqrt{\mu}$ to get c^{EB}.

From this Alice can compute the transmittance and excess noise as follows,

$$\begin{aligned} T &= \frac{\left(c^{\mathrm{EB}}\right)^2}{V_{\mathrm{mod}}^2 + 2V_{\mathrm{mod}}} = \mu\left(\frac{c^{\mathrm{PM}}}{V_{\mathrm{mod}}}\right)^2 \\ \xi &= V_B - TV_{\mathrm{mod}} - 1 = b^{\mathrm{EB}} - TV_{\mathrm{mod}} - 1 \end{aligned} \tag{2.144}$$

Using this information, Alice can proceed to find the Holevo bound discussed in Section 2.10.4 and finally calculate the secure key rate.

Chapter 3

BB84 Protocol using Heralded Single-Photon Source

The BB84 quantum key distribution (QKD) protocol set the course for achieving secure communication. Since then, much work has been done in the direction of QKD implementation to improve the experimental limitations and the security aspects. In this Chapter, we have implemented a passive QRNG-based BB84 QKD protocol using a heralded single-photon source employing the SPDC process. The proposed protocol is secure against PNS and side-channel attacks, offering an advantage over a typical BB84 and decoy state protocol. Further, the implementation does not require an external QRNG source and can be implemented with fewer resources than the BBM92 protocol. The heralded photon from an SPDC process is used to prepare the four polarisation states and is then sent to Bob through a quantum channel. The quality of the single-photon source is calculated by measuring the second-order correlation $g^2(0)$ function. The security of the implemented protocol is hence given, and the key rate is extracted.

3.1 Introduction

Quantum key distribution (QKD) is one of the most ubiquitous applications of quantum information, which exploits the fundamental principles of quantum mechanics to exchange the cryptographic key between two communicating parties. It provides information-theoretic security in the sense that the security of the protocol entirely relies on the laws of quantum mechanics instead of the complexity of the mathematical algorithms; hence, making no assumptions about the adversary's technological powers.

The first proposed QKD protocol was BB84 [119], where the key information is encoded into the polarisation state of a single-photon. Since the implementation of BB84, several protocols have been demonstrated [120–123]. These protocols are theoretically unconditionally secure [124–126]. However, various experimental impairments raise the security threats to these protocols[127–129]. A typical BB84 requires a single-photon source that deterministically produces a single-photon per pulse. The generation of true single-photons is experimentally challenging; instead, we use weak coherent pulses that follow Poissonian statistics. This leads to a non-zero probability of having more than one photon. Such implementations are susceptible to photon number splitting (PNS) [128] attack by an eavesdropper. To reduce the vulnerability against such attacks; several innovative protocols have been demonstrated, which include decoy state protocol [97], entanglement-based (EB) protocols [120, 121], and measurement device independent (MDI) QKD protocols [130]. However, the implementation of these protocols is much more complicated in practice. In implementations of the decoy state BB84 protocols, multiple lasers are often used to generate the signal and the decoy states, opening the implementation to various side-channel attacks. Moreover, such an implementation also leads to an increase in the setup size

and complexity. On the other hand, the EB protocols are proven to be more secure but suffer from a low key generation rate since a fraction of the key is used for entanglement verification. Another major challenge with EB protocols is the distribution of the entanglement over long distances with high fidelity. The EB protocols require more resources than the typical prepare and measure BB84 protocol.

To get a trade-off between resources and security, we have implemented the BB84 protocol using a heralded single-photon source [131]. One of the ways to generate a single-photon source is the nonlinear process of spontaneous parametric down conversion (SPDC) [132] where a photon pair is generated from the nonlinear crystal followed by certain phase-matching conditions. By doing the conditional measurement on one of the photons, we can infer the presence of the other. Such a process is called heralding. To perform the QKD, Alice keeps one of the photons generated by the SPDC process for heralding, and the other photon is encoded in four different delays and polarisation states. The encoded photons are transmitted to Bob through a quantum channel. Bob measures the photons using single-photon detectors. To check the quality of the single-photon source, we have measured the second-order correlation function $g^2(0)$ [104, 133]. Thus we assure the security of the implemented protocol and extract the key rate.

The advantage of our implementation of BB84 using the heralded single-photon over a typical BB84 lies in the fact that the protocol provides security against PNS attack since we are using a single-photon source instead of weak coherent pulses. Moreover, the protocol offers advantages over the decoy state protocol since we do not require additional sources, and the four polarisation states are prepared by using only a single source, which prevents any side-channel attacks [134]. In addition, the proposed method uses less resources compared to BBM92 protocol [44] and does not

require an external quantum random number generator (QRNG) to prepare various polarisation states randomly.

This Chapter is organized into the following sections. In Section 5.2, we have given a background for the understanding of the protocol and given the security parameters for the protocol. Section 5.4 describes the experimental implementation of BB84 QKD protocol by using a heralded single-photon source. We highlight the results obtained from the experiment. We conclude our work with some remarks in Section 5.5.

3.2 Background

In this section, we describe the implementation of BB84 protocol using heralded single-photon source. For the implementation of the protocol, we use the SPDC process to generate single-photon pairs. The generation of single-photon pairs using SPDC process is performed at Alice's end, like in a typical BB84. In this process, an incident pump photon gets annihilated and creates a pair of photons such that the total energy and momentum of the system remain conserved. The generated photons of the pair are called signal and idler. By detecting one of the photons using a single-photon detector, the presence of the other photon can be inferred. Such a process is called heralding. Alice uses signal photon for heralding, and idler photon is used to prepare the four polarisation states $|H\rangle$, $|V\rangle$, $|D\rangle$, and $|A\rangle$. The encoded states are transmitted to Bob through a free space channel. Bob performs the detection using single-photon detectors. The whole process is divided into the following steps.

3.2.1 Random Selection of the States

Usually, in a typical BB84 and decoy state protocol, we require a random number that is generated using a QRNG [135, 136]. In heralded BB84 protocol, the job of

randomly selecting the states, is embedded in the setup itself.

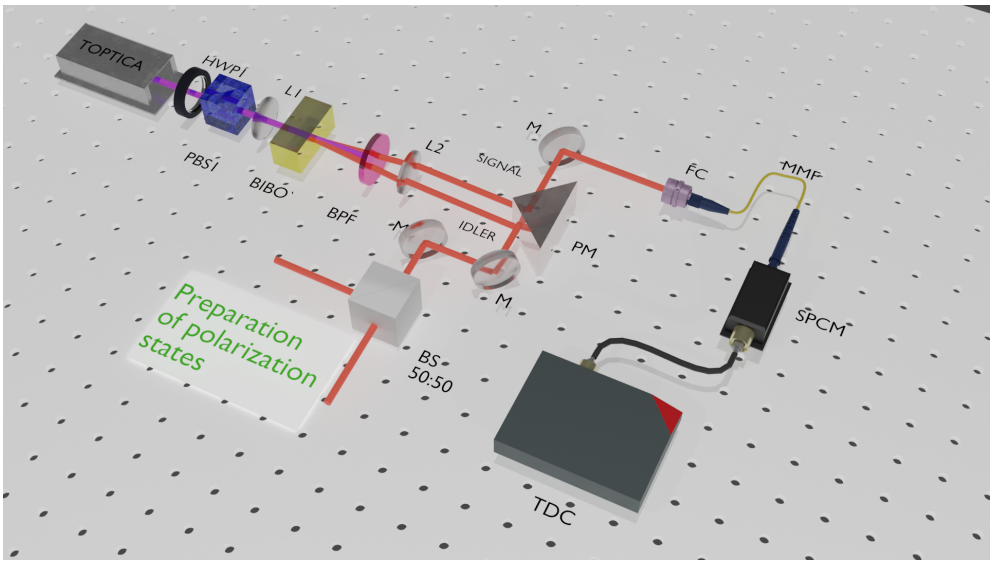

Figure 3.1: Schematic for SPDC process; HWP: Half Wave Plate; PBS: Polarising Beam Splitter; L: Lens; BIBO: Bismuth Borate Nonlinear Crystal; BPF: Band-pass Filter; PM: Prism Mirror; FC: Fiber Coupler; MMF: Multi-mode Fiber; SPCM: Single-Photon Detector; TDC: Time-to-Digital Converter; BS: Beam Splitter.

The experimental setup for generating a single-photon using the SPDC process is shown in Fig. 3.1. Alice has a continuous wave diode laser (TOPTICA) operating at 405 nm with an output power of 6 mW. A combination of half-wave plate (HWP1) and polarising beam splitter (PBS1) is used to tune the power of the laser. A nonlinear crystal, BIBO of type-I, is used to generate the single-photon pairs using the SPDC process. A lens (L1) of focal length 50 cm is used to focus the pump beam onto the crystal to increase the process's efficiency. A pair of non-collinear vertically polarised signal and idler is emitted from the crystal, which are separated by using a prism mirror (PM). A band-pass filter (BPF) of 810 ± 5 nm is used to block the pump beam. Signal photon is used for heralding. It is coupled to the fiber coupler (FC) through multi-mode fiber (MMF) and is measured by using a single-photon detector (SPCM). The timestamps are recorded using a time-to-digital converter (TDC). The idler arm is used

to prepare the four polarisation states, which are then transmitted to Bob via free space.

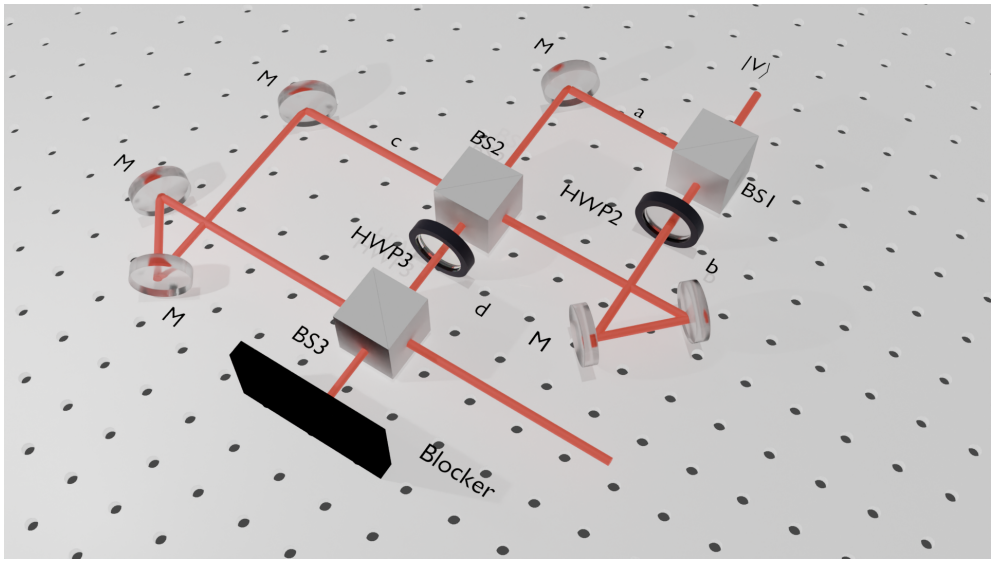

Figure 3.2: State preparation for BB84 protocol using heralded single-photon source; HWP: Half Wave Plate; BS: Beam Splitter; M: Mirrors.

Once we generate the signal and idler photons, we prepare the four polarisation states $|H\rangle$, $|V\rangle$, $|D\rangle$, and $|A\rangle$. The state preparation setup consists of two cascaded Mach-Zehnder interferometers with Half Wave Plates (HWPs) in them, shown in Fig. 3.2. As such, a single-photon passing through the setup can take four paths. The specific path the photon chooses is made random by the use of beam splitters. The HWPs change the polarisation depending on the path chosen. We ensured that the beam splitters are as close to 50:50 as possible to generate the four polarisation states with equal probability. The BSs placed in the idler arm do the job of randomly selecting the photon sent to Bob.

The input polarisation to BS1 is $|V\rangle$. The photon can choose either of the four paths: ac, bc, ad, or bd. The HWP2 and HWP3 are placed at 45^{o} and 22.5^{o} to convert the polarisation into $|H\rangle$ and $|D\rangle$, respectively. The photon following the path 'ac' or

'bc' is $|V\rangle$ or $|H\rangle$ polarised. The photon following the paths 'ad' or 'bd' is $|A\rangle$ or $|D\rangle$ polarised. The states after BS3 are transmitted to Bob through a quantum channel.

3.2.2 Transmission Through Channel

The quantum state is transmitted to Bob through a quantum channel. For sending qubits in polarisation degree of freedom, one can use free space or optical fiber as a channel. Free space offers an advantage as the polarisation drifts in free space are much less compared to fiber. Exploring free space is essential for terrestrial applications and satellite communication. Alice transmits her states to Bob through free space.

3.2.3 Detection of State

The photons are measured by projecting their polarisation state onto the four states by employing a combination of HWPs and PBSs followed by SPCMs. Bob's detection setup includes a 50:50 beam splitter (BS4), which acts as a basis selector that randomly selects the basis for the projection measurement, as shown in Fig. 3.3. The measurement of the state in $\{H,V\}$ and $\{D,A\}$ basis is done by keeping a PBS3 and a combination of HWP4 and PBS2 respectively. The photons are detected by single-photon avalanche detectors (Excelitas, SPCM-AQRH-14-FC). The detector efficiency of the detectors is 65%. We use multi-mode fibers to couple the photons to the detectors. The number of detected photons and their arrival times are recorded by using the time-to-digital converter (TDC) and time tagger.

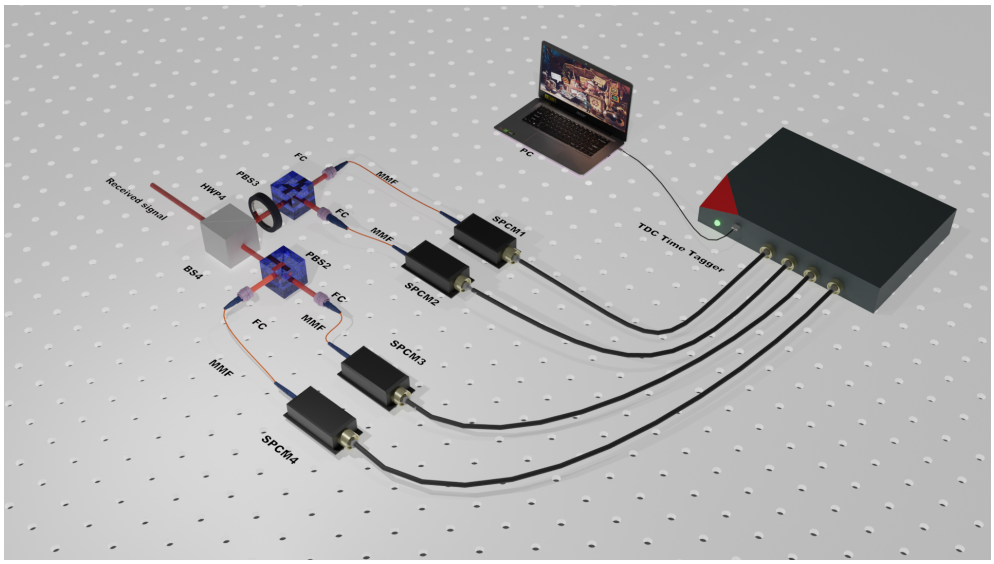

Figure 3.3: Detection of the quantum states at receiver's end; HWP: Half Wave Plate; PBS: Polarising Beam Splitter; FC: Fiber Coupler; SPCM: single-Photon Detector; TDC: Time-to-Digital Converter; BS: Beam Splitter.

3.2.4 Post-processing

Once the key establishment process is done, Alice and Bob further process their data to extract the secure key. They perform sifting to get the correlated bit string. Additionally, they do the reconciliation to estimate and correct the error present in the correlated data. The final step includes privacy amplification to make the key more secure by minimising the information to Eve.

The sifting process requires that the photon arrival time at the receiver's end and the time when they are launched from the transmitter must be known. Alice and Bob are inherently synchronised due to SPDC process and thus the timestamp information can be correctly extracted by both Alice and Bob. Since Alice has encoded her state in polarisation states following different optical paths, she knows the precise delays for various polarisation states, which is shown in Table 3.1. Moreover, the absolute delay of the heralded signal photon from the crystal to the detector is known by Alice, which

is 3.07 ns. To perform sifting, Alice and Bob follow the steps mentioned here.

Path	Absolute Time Delay (ns)	Output States
ac	11.84	$\|V\rangle$
ad	8.8	$\|A\rangle$
bc	13.57	$\|H\rangle$
bd	10.52	$\|D\rangle$

Table 3.1: The table contains time delays for different output polarisation states at Alice's end, and this delay information is limited to Alice only.

- Bob sends his timestamps and corresponding basis information to Alice. Alice compares the heralded signal with Bob's timestamps.
- The relation between the recorded timestamps of Alice (t_A) and Bob (t_B) follow the relation

$$t_B = t_A + \Delta + \delta_{ch} \tag{3.1}$$

  where Δ is the delay in the path lengths in the state preparation setup, and δ_{ch} is the delay due to the quantum channel.
- If the difference in the recorded timestamps matches the time delay for any of the four polarisation states, then the timestamp corresponds to the state sent by Alice.
- Alice removes all the detections for which the timestamp difference is not one of the four-time delays mentioned in Table 3.1. Also, the detections corresponding to the wrong basis measurements are discarded.
- Alice and Bob are left with correlated key elements and perform further post-processing to get the secure key.

The quantum bit error rate (QBER) is then evaluated using a small portion of the sifted key. The estimated QBER is used to evaluate the mutual information shared

between Alice and Bob and also to further assess the amount of information leaked to a potential Eve. The final steps include error correction using LDPC codes [137, 138] and then privacy amplification using Toeplitz hashing [90].

3.2.5 Error Correction

In classical communication, error correction codes are employed to mitigate errors induced by channel noise [138, 139]. This is accomplished by introducing additional bits, known as parity bits (r), into the message. The error correction codes involve the use of a generator matrix (G) at the transmitter, while a parity check matrix (H) is utilized at the receiver to calculate syndromes (s) for decoding. In QKD, the decoding process is performed at a single node, either Alice or Bob. Unlike classical communication, only the syndrome (s) is exchanged between Alice and Bob. Based on the syndrome (s) information, both parties modify their respective keys. Through this process, the keys at both Alice and Bob eventually become identical. During the parameter estimation (PE) phase, if the QBER falls below the specified threshold determined by the protocol, the remaining keys undergo error correction. This leads to the establishment of identical keys between Alice and Bob. The error correction procedure can be executed by considering either Alice's or Bob's bits as correct.

For error-correcting, the remaining bits in the sifted key are divided into small blocks of certain bits (say l). r parity bits are required to construct a parity check matrix $[F]_{r\times l}$.

$$\begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_r \end{bmatrix}_{r\times 1} = \begin{bmatrix} F_{11} & F_{12} & \cdots & F_{1l} \\ F_{21} & F_{22} & \cdots & F_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ F_{r1} & F_{r2} & \cdots & F_{rl} \end{bmatrix}_{r\times l} \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_l \end{bmatrix}_{l\times 1} \tag{3.2}$$

Equation (3.2) denotes the basic operation for finding syndrome. After multiplication with sift key this results in syndrome $[s]_r$ that is sent over the public channel to Bob. Bob matches these blocks of syndrome with his ones for detecting the errors. The syndrome which does not match is then corrected by the maximum likelihood technique [140]. There are several kinds of error-correcting algorithms eg. parity checks, Hamming code, and Low-Density Parity Check (LDPC) [137, 141]. The common error-correcting technique used in QKD is LDPC which is efficient and easy to implement in the system.

3.2.6 Privacy Amplification

Privacy amplification (PA) is a crucial process in QKD that aims to eliminate any leaked information and distill a final secret key from a long-secret random sequence, utilizing a universal hash function [142]. When combined with error correction, such as LDPC or any other error correction codes, it allows for minimizing Eve's information about the key, reducing it to a negligibly small amount in the asymptotic limit. To ensure the effectiveness of PA, the selection of a hash function over the public channel must only occur after the quantum exchange between Alice and Bob. This precaution prevents Eve from strategizing her attack based on their choice. Among various hash functions suitable for privacy amplification, Pulitzer hashing [143] stands out as a 2-universal hash function, enhancing the quality of randomness. For optimal performance, a completely random initial seed is required, which can be obtained from the output of a QRNG. The error-corrected bit string can be effectively hashed using this approach. By integrating privacy amplification with error correction and employing the 2-universal hash function, the security of the final secret key is significantly enhanced in the context of QKD. The hashing of the error-corrected bit string can be

given by [144]

$$\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{bmatrix}_{m\times 1} = \begin{bmatrix} h_1 & 0 & \cdots & 0 & 0 \\ h_2 & h_1 & \cdots & 0 & 0 \\ h_3 & h_2 & \cdots & 0 & 0 \\ \vdots & h_3 & \cdots & h_1 & 0 \\ h_{m-1} & \vdots & \cdots & h_2 & h_1 \\ h_m & h_{m-1} & \cdots & \vdots & h_2 \\ 0 & h_m & \cdots & h_{m-2} & \vdots \\ 0 & 0 & \cdots & h_{m-1} & h_{m-1} \\ 0 & 0 & \vdots & \cdots & h_m \end{bmatrix}_{m\times l} \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_l \end{bmatrix}_{l\times 1} \tag{3.3}$$

Here, $[g]_{l\times 1}$ is the error corrected bit length, $[h]_{m\times l}$ is the hash matrix and $[y]_{m\times 1}$ is the final secret key which has no correlation with Eve. This process is similar for Alice and Bob which both can do independently. Estimation of final bit length after PA is given by

$$m = l - t - s, \tag{3.4}$$

Here l is the error corrected bits, and t is the amount of knowledge exchanged between Alice and Bob to correct the error due to all possible reasons. Exchanging syndromes in error correction might leak some information to Eve that's why it is subtracted. Security parameter s can be chosen according to the key one needs to compress in PA [143]. This parameter also depends on the number of bits sacrificed due to information exchange in EC. To check the quality of PA one can use randomness test suites, NIST, DieHarder, ENT, etc. To finally test that the keys are identical, Alice encrypts a short message with the generated key for Bob to check whether he can decrypt or not.

3.2.7 Security of the Protocol: $g^{(2)}(0)$ Correlation

In quantum optics, the measurement of the second-order correlation $g^{(2)}(\tau)$ plays an important role, particularly in the observation of a purely quantum phenomenon called 'anti-bunching' [25]. This measurement is commonly carried out using the Hanbury Brown Twiss (HBT) experiment [104]. In the case of an ideal single-photon source, where photons are emitted sequentially, each photon faces the option of being transmitted through the BS or being reflected. When the two paths are equal, the probability of getting the clicks in two detectors simultaneously is zero, i.e. $g^{(2)}(0) = 0$. This confirms the true single-photon nature of the source and ensures the security of the QKD experiments. For heralded single-photon sources produced by SPDC, the correlation of the photons in the HBT experiment is performed between the idler (i) and the conditioned detection of the signal (s), as depicted in Figure 3.4. In the per-

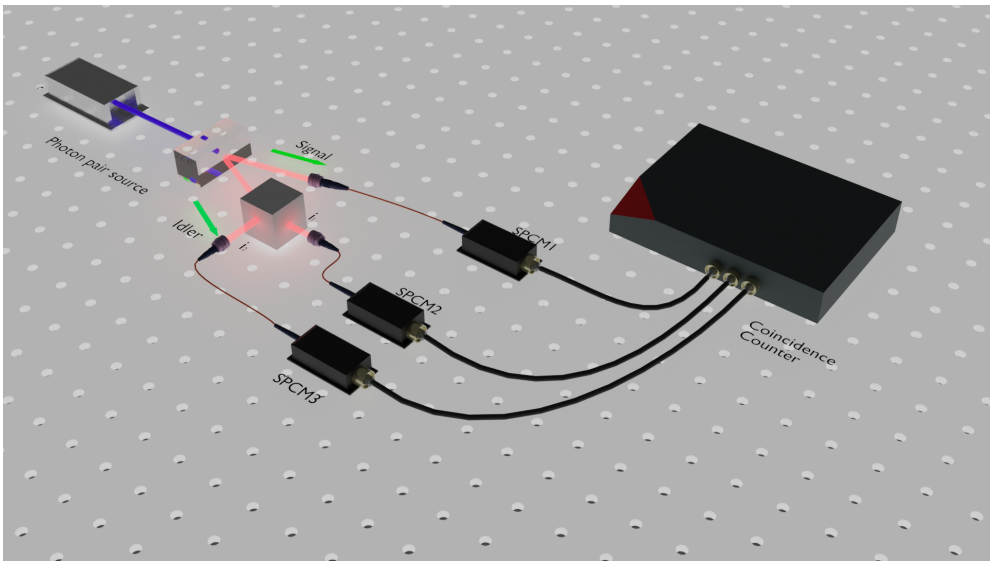

Figure 3.4: An illustration of the HBT experiment to find the second-order correlation $g^{(2)}(0)$.

fect case of a single-photon source, where there is no delay between the detections of photons in arms s, i_1, and i_2, the three-fold detection probability among these arms

becomes zero. This probability, represented as P_{s,i_1,i_2}, when normalized with respect to the corresponding two-fold coincidences, provides the second-order correlation (for zero delay).

$$g^{(2)}(0) = \frac{P_{s,i_1,i_2}}{P_{s,i_1}P_{s,i_2}} \tag{3.5}$$

where P_{s,i_1} and P_{s,i_2} are the probabilities of two-fold coincidence between $s-i_1$, and $s-i_2$ pairs. The expression for the conditioned probability of coincidence detection is given by $P_{i,j} = \frac{R_{i,j}}{R_i}$, where $R_{i,j}$ represents the coincidence rates in the respective arms, and R_i represents the count rate of the heralding arm. By substituting various probabilities into Eq. 3.5, the expression for $g^{(2)}(0)$ in terms of experimentally measured rates can be represented as follows:

$$g^{(2)}(0) = \frac{R_{s,i_1,i_2}R_s}{R_{s,i_1}R_{s,i_2}} \tag{3.6}$$

To calculate $g^{(2)}(0)$, one can directly measure the three-fold coincidences between the heralding signal mode and the two idler modes. The value of $g^{(2)}(0) = 0.006 \pm 0.0002$ for multi-mode fiber.

3.3 Results and Discussion

We performed the experiment for BB84 QKD protocol using a heralded single-photon source in our lab over free space. The experimental setup for the protocol is shown in Fig. 3.5. The overview of the transmitter and receiver setup in the laboratory is shown in Fig. 3.6. Alice used a continuous wave diode laser (TOPTICA) operating at a wavelength of 405 nm. To prepare the state, one of the photons generated by the SPDC process is heralded by Alice, and the other photon is encoded in four different polarisation states. The encoded photon is transmitted to Bob through a quantum channel. Bob detects the photon using a single-photon detector. Alice and Bob collect

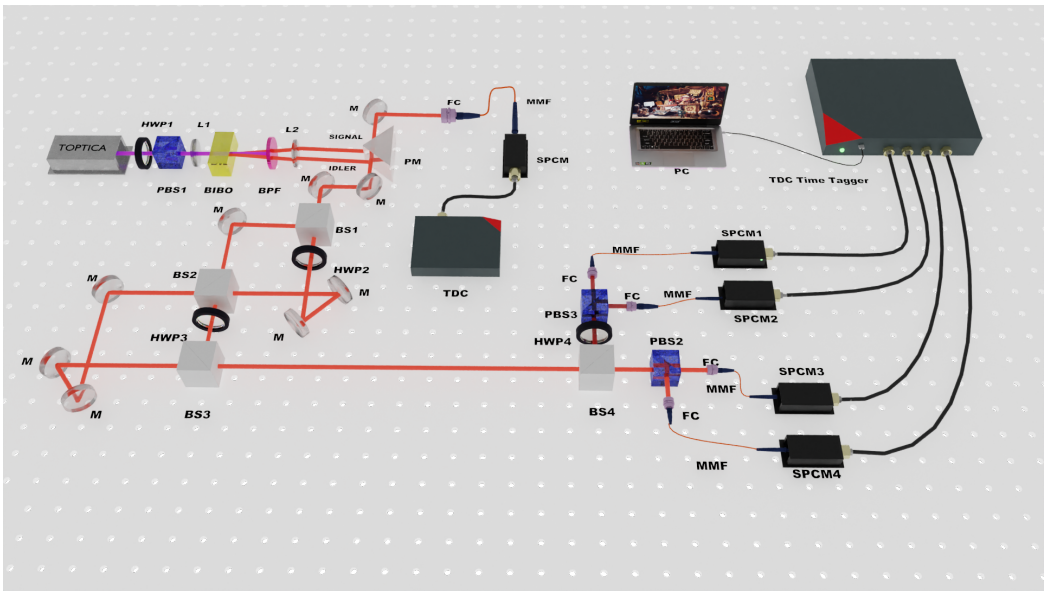

Figure 3.5: Experimental setup for BB84 protocol using heralded single-photon; HWP: Half Wave Plate; PBS: Polarising Beam Splitter; L: Lens; BIBO: Bismuth Borate Nonlinear Crystal; BPF: Band-pass Filter; PM: Prism Mirror; FC: Fiber Coupler; MMF: Multi-mode Fiber; SPCM: Single-Photon Detector; TDC: Time-to-Digital Converter; BS: Beam Splitter; M: Mirrors.

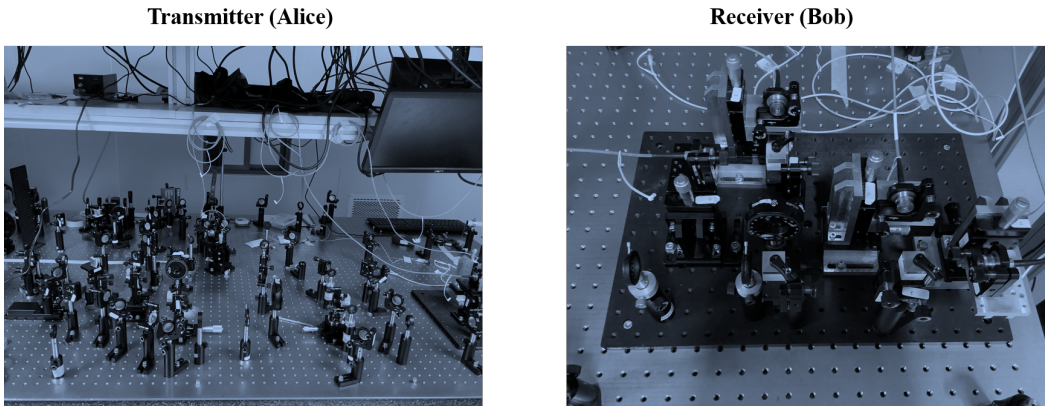

Figure 3.6: Laboratory view of transmitter and receiver setup for BB84 using a heralded single-photon. The receiver on the breadboard is made ready for the field experiment.

the timestamps of the recorded photons. They further performed the sifting to get the correlated data, followed by the steps mentioned in Section 5.2.

While performing the experiment, we made the assumption that the beam splitters

used in the experiment were nearly 50:50. Further, we assumed that the detectors were operating at the same efficiencies. We calculated the $g^{(2)}(0)$ and ensured that our source is true single-photon nature. The secure key rate K, is obtained using the relation [145],

$$K = P_1 * (1 - 2H(\delta)) \tag{3.7}$$

where H is the binary Shannon entropy, δ is the bit error, and P_1 is the probability of the photon pair detection.

We measured the various experimental parameters required to perform the QKD. The channel transmittance for free space in lab is 98%. The detection efficiency of the detectors is 65%. The coupling efficiency of the multi-mode fiber is 85%. The obtained sifted key rate is 14 **kbps**, with a QBER of **7%**. The secure key rate obtained after error correction and privacy amplification is 5 **kbps**.

We plotted the correlated counts obtained from the independent detections performed by Alice and Bob. The correlation is established between the heralded photon measured by Alice and the polarisation encoded photons received by Bob at different time delays. The time delay for the heralded photon is fixed, which is 3.07 ns. The photons at Bob's end arrive at different delays. The correlated counts for various measured polarisations are plotted in Fig. 3.7. From the figure, we can see that the correlated counts are less for V-polarisation. This could be due to the experimental imperfections or poor coupling of the polarisation to fiber.

Further, we performed the experiment to calculate the second-order correlation function, $g^{(2)}(0)$, at Alice's end. The calculated values of $g^{(2)}(0)$ would confirm the true single nature of the photon source. We use multi-mode fibers to couple the photons into the detector. The experimentally measured $g^{(2)}(0)$ correlation obtained for Alice

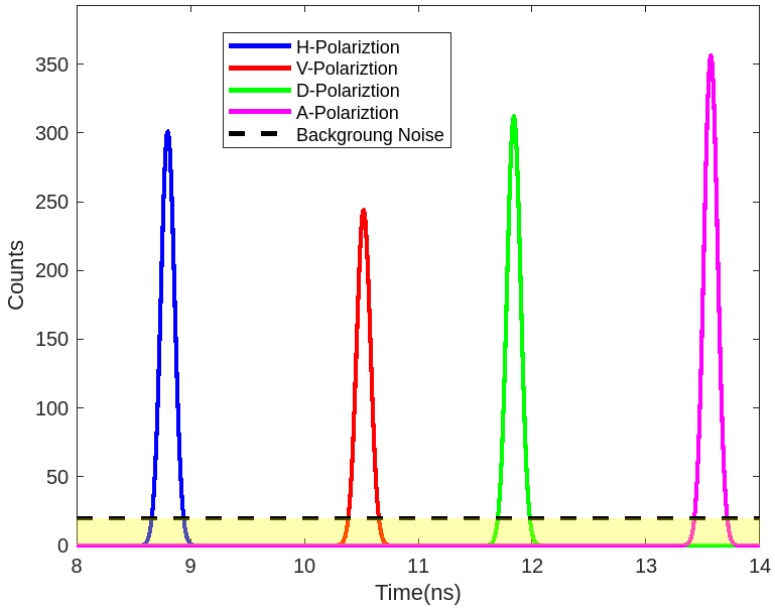

Figure 3.7: Output of the four independent correlated detections performed for Alice and Bob basis. The peaks indicate the correlated counts for the respective polarisations. The yellow zone indicates the background counts that represents the unwanted detections due to stray light or uncorrelated signal and idler photons.

has a value 0.006 ± 0.0002, which deviate slightly from the ideal value zero, hence certify the single-photon nature of the source.

We have performed a simulation of the expected key rate vs distance for the proposed protocol and we have compared it with a decoy state protocol. The results are plotted in Fig. 3.8. In this simulation we have considered a weak coherent pulse based decoy state protocol with a mean photon number $\mu = 0.1$. In the proposed protocol we have considered the photon statistics of the emitted pair to be sub-Poissonian with a mean photon number $\mu = 0.1$. The quantum channel has been considered to be an optical fiber. The transmittance of the channel versus distance is given by $t = 10^{\frac{-\alpha l}{10}}$, where l is the length of the channel and $\alpha = 0.2\text{dB/km}$. For a free space channel a similar simulation can be performed by considering the free space losses which include losses due to divergence, atmospheric scattering, and atmospheric extinction. It is seen that the proposed protocol outperforms the decoy state protocol for longer distances as

is expected from single photon based QKD protocols.

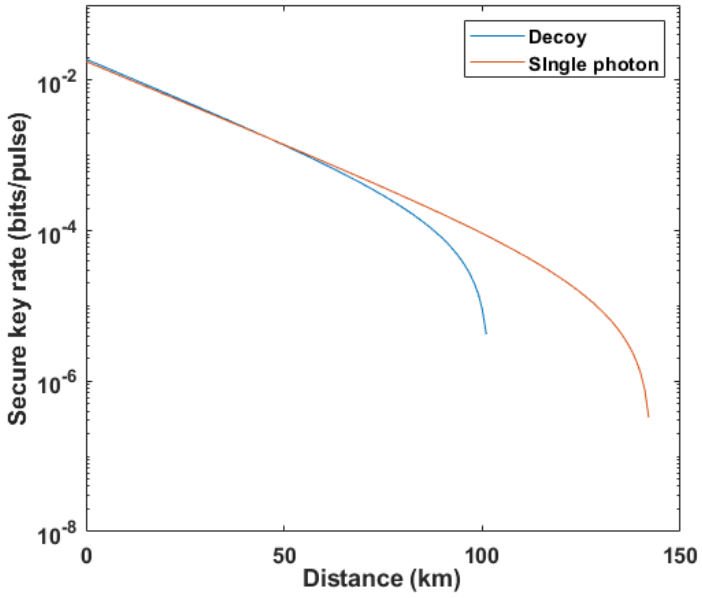

Figure 3.8: Comparison plot of the secure key rate vs distance for a weak coherent pulse based decoy state protocol and the proposed protocol.

3.4 Conclusion

In conclusion, we have implemented a BB84 protocol using a heralded single-photon source. The protocol is secure against PNS attacks, implying no requirement for decoy signals to check for Eve. Further, the implementation provides additional security against side-channel attacks and offers an advantage over typical BB84 and decoy state protocol. The protocol requires fewer resources than BBM92, and eliminates the requirement of external QRNG. Additionally, the quality of the true single-photon source is certified by calculating the second-order correlation function. Further, we are working to improve the QBER of the protocol.

Chapter 4

Measuring the Shot Noise for Continuous Variable Applications

Measuring the quantum fluctuations of a laser source is the first task in performing CVQKD protocols. The quantum fluctuations of the source are measured using balanced homodyne detection. In this chapter, we have measured the shot noise of a pulsed laser using imperfect homodyne detection. The imperfections accounted for in the detection process are a delay between the homodyne output arms and also due to the selection of the pulse integration window larger as well as smaller than the photocurrent pulse width during the analysis. We have analysed the imperfect detection results for two different experimental layouts, and a comparative study has been performed. From our analysis, it is evident that these imperfections play a significant role in balanced homodyne detection and must be optimized properly. Our results indicate that balanced homodyne detection can be performed using limited resources, which paves the way for easy experimental realization of optical homodyne tomography and CVQKD in a laboratory setting.

4.1 Introduction

The first step in the experimental realization of any quantum key distribution (QKD) protocol [30, 146] is measuring the quantum fluctuations of a source. For a coherent laser source, the quantum fluctuations are measured in terms of shot noise [24]. Shot noise is the fundamental noise present in the state and is unavoidable. The calibration of the shot noise [147] is essential for coherent state based continuous variable (CV) QKD protocols [60, 99–101, 148, 149] to characterize the minimum noise that is present in the state. In CVQKD protocols, the shot noise is the minimum uncertainty present in the state, and all the noises are calculated with respect to the shot noise [45]. The detector and channel imperfections manifest as excess noise [150–152] over and above the shot noise. In CVQKD protocols, the presence of an eavesdropper is detected based on the excess noise, which is the difference between the observed noise and the shot noise [69, 153].

Balanced homodyne detection (BHD) is a well-established technique used to measure the field quadratures of the electromagnetic field [104, 111] and shot noise. BHD has become a standard tool in experimental quantum optics and is used in quantum tomography [36, 63, 115], and quantum information applications [62, 154, 155]. Shot noise of a source is measured using balanced detection where the signal is split equally using a 50:50 beam splitter (BS) and made to fall on two identical photodetectors. The resulting photocurrents are subtracted and amplified. The subtraction process eliminates all sources of classical noise, and we measure the quantum or shot noise [29].

While measuring shot noise using BHD, it is essential to ensure that the delay between the two homodyne arms is zero and the intensities are equal, where we assume that detectors have the same efficiencies. Imperfection in any of these conditions can

lead to errors in the shot noise measurement [156]. The inefficiencies in the BHD process that could affect the measurement are imperfect balancing due to optical losses, non-unitary detector efficiencies, and electronic noise [157–159]. In addition to these, the imperfections in the detection process could be due to a delay between the homodyne output arms and also due to an improper selection of the pulse integration window during the analysis. These imperfections are to be taken care of, especially in time domain BHD [160, 161], where a pulsed laser source is used. In time domain BHD, the output photocurrents consist of a train of pulses. The quadrature value is retrieved by integrating or averaging the photocurrent over the pulse region [162]. The time lag between the pulses arriving at the two detectors causes different responses between them leading to an improper cancellation of the subtracted output. Moreover, a wrong selection of the integration window could lead to an error in the measured quadrature value.

In this chapter, we have measured the shot noise of a pulsed laser source using imperfect detection. The study of shot noise measurements performed in this Chapter are carried out in order to understand the impact of imperfections in the detection setup on balanced homodyne detection. These studies are crucial for systems ultrafast laser systems employing femtosecond or picosecond pulses with high repetition rates which in turn are essential for high rate QKD applications. We have considered two different layouts and have studied the effect of delay and pulse integration window on the measurement of shot noise. In Layout-1 (Fig. 4.1), we have used a commercially available balanced amplified detector. The output signals from the two photodetectors are subtracted and amplified using a transimpedance amplifier (AMP). In Layout-2 (Fig. 4.2), we simply use two individual photodetectors and subtract the signal using a digital storage oscilloscope (DSO) without amplification. The experiment performed using Layout-2 is to study the measurement of shot noise using two

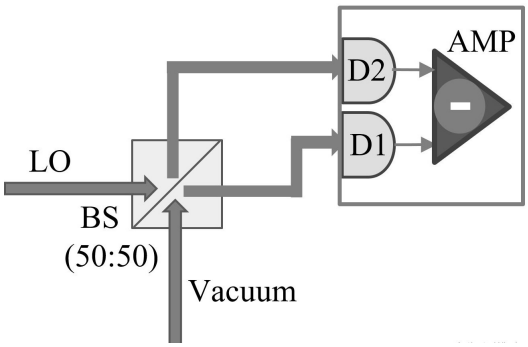

Figure 4.1: The schematic diagram for balanced detection with amplification, Layout-1; LO: Local Oscillator Field; BS: Beam Splitter; D1 & D2: Photodetectors; AMP: Transimpedance Amplifier.

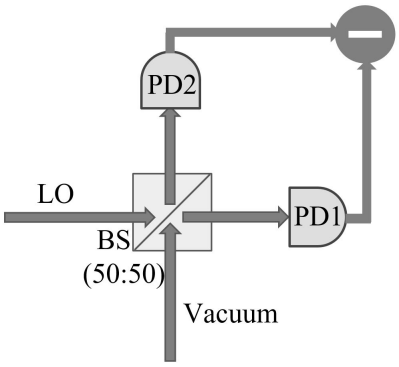

Figure 4.2: The schematic diagram for balanced detection without amplification, Layout-2; LO: Local Oscillator Field; BS: Beam Splitter; PD1 & PD2: Photodetectors.

individual photodetectors. Such a setup has an advantage in reducing the cost of the experimental resources as well as increasing the bandwidth of detection for high rate QKD applications. Since the photodetectors work at GHz, whereas the commercial balanced detectors are limited to hundreds of MHz. We have measured the shot noise using Layout-1 and Layout-2 for three different delay conditions and for various pulse integration windows. We have performed a comparative study for both layouts.

The motivation behind the present work is to find out a method for shot noise measurement and CVQKD implementation that requires less resources and is cost-effective.

The chapter is organized as follows. In Sec. 4.2, a theoretical background for homodyne detection using a pulsed laser source is outlined. The effect of delay and pulse integration window on shot noise measurement is discussed, and simulation results are presented. In Sec. 4.3, we have described the experimental setup for Layout-1 and Layout-2 to study the effects of the imperfections mentioned above. The experimental results for both layouts are shown and discussed in Sec. 4.4. We end with the concluding remarks in Sec. 4.5.

4.2 Theory and Simulation

BHD (Fig. 4.3) is a popular method to measure the quadratures of the electromagnetic field modes where the signal whose quadratures are to be measured interferes with a strong coherent field called the local oscillator (LO) at a 50:50 beam splitter. The resulting beams are made to fall upon photodetectors, and the generated photocurrents are subtracted. By varying the phase difference between the LO field and the signal field, the suitable quadrature is selected for measurement. For a single-mode of the electromagnetic field, the quadrature operators are defined as

$$\hat{q} = \frac{1}{\sqrt{2}}(\hat{a} + \hat{a}^{\dagger}), \tag{4.1}$$

$$\hat{p} = \frac{1}{i\sqrt{2}}(\hat{a} - \hat{a}^{\dagger}). \tag{4.2}$$

The homodyne output operator, $\hat{i}$ is proportional to the difference of the intensities in the output arms, i.e.,

$$\hat{i} \propto \hat{I}_1 - \hat{I}_2. \tag{4.3}$$

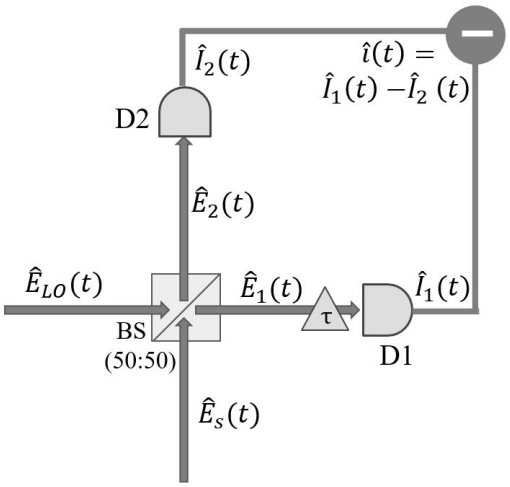

Figure 4.3: The schematic diagram of imperfect balanced homodyne detection; BS: Beam splitter; τ: Delay between the two homodyne outputs; $\hat{E}_{\rm LO}(t)$ & $\hat{E}_{\rm s}(t)$: LO and signal fields; $\hat{E}_1(t)$ & $\hat{E}_2(t)$: BS output modes; $\hat{I}_1(t)$ & $\hat{I}_2(t)$: Photocurrents of photodetectors D1 & D2 respectively; $\hat{\imath}(t)$: Subtracted photocurrent.

The expectation value of the homodyne operator for a general signal is evaluated to be

$$\langle \hat{i}_\phi \rangle = \sqrt{2}|\alpha_{\rm LO}|\langle \hat{q}_{\rm s}\cos\phi + \hat{p}_{\rm s}\sin\phi \rangle, \tag{4.4}$$

where $\hat{q}_{\rm s}$ and $\hat{p}_{\rm s}$ are the quadratures of the signal field, and ϕ is the phase difference between the signal and the LO. By setting the phase difference between the signal and the LO to 0 or $\pi/2$, the quadratures $\hat{q}_{\rm s}$ or $\hat{p}_{\rm s}$ can be measured respectively.

In the experiment performed in the present chapter, we have used a pulsed laser source as the LO field. Classically the electric field equation for a pulsed laser source is given by,

$$E(t) = \sum_{l=-M}^{M} E_0 e^{-i(\omega_l t + \phi_l)} + \text{h.c.}, \tag{4.5}$$

where the index l represents a single-mode of the field and h.c. stands for Hermitian conjugate. The frequencies of consecutive modes are equally spaced i.e., $\omega_{l+1} - \omega_l = \Delta\omega$. The phase difference between consecutive modes is made constant which results

in a train of pulses. Here, we outline a simple quantum picture of the effect of delay on the photocurrents generated and its effect on the measurement of shot noise.

The electromagnetic field [25] of the LO is given by

$$\begin{aligned}\hat{E}_{\mathrm{LO}}(t) &= \sum_{l=-M}^{M} \hat{a}_l e^{-iw_l t} + \mathrm{h.c.} \\ &= \hat{E}^{+}_{\mathrm{LO}}(t) + \hat{E}^{-}_{\mathrm{LO}}(t). \end{aligned} \tag{4.6}$$

$\hat{E}^{+}(t)$ and $\hat{E}^{-}(t)$ are referred to as the positive and negative frequency parts of the electromagnetic fields respectively. The state of the LO field is written as a multi-mode coherent state such as

$$|\bar{\alpha}\rangle = \bigotimes_{l=-M}^{M} |\alpha_l\rangle\,, \tag{4.7}$$

where the phase difference between the coherent states of successive modes is a constant, i.e., $\alpha_l = |\alpha_0| e^{il\phi_0}$. The intensity of the LO field is given by,

$$I_{\mathrm{LO}}(t) = \frac{|\alpha_0|^2}{2}\left(\frac{\sin^2\left((M+0.5)\Delta\omega t\right)}{\sin^2\left(0.5\Delta\omega t\right)}\right). \tag{4.8}$$

Similarly, the signal field derived from the same source is given by

$$\hat{E}_{\mathrm{s}}(t) = \sum_{l=-M}^{M} \hat{b}_l e^{-iw_l t} + \mathrm{h.c.}. \tag{4.9}$$

For measuring the shot noise of the pulsed laser source, the signal arm is blocked. Hence, the state of the signal field is given by

$$|\bar{0}\rangle = \bigotimes_{l=-M}^{M} |0_l\rangle\,, \tag{4.10}$$

which is the multi-mode vacuum state. The combined state of the input fields is given

by

$$|\psi\rangle_{\text{in}} = |\bar{\alpha}\rangle_a \otimes |\bar{0}\rangle_b \,, \tag{4.11}$$

The action of the 50:50 beam splitter on the input fields is given by the matrix equation[25]

$$\begin{pmatrix} \hat{c} \\ \hat{d} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \hat{a} \\ \hat{b} \end{pmatrix}, \tag{4.12}$$

where $\hat{a}$ and $\hat{b}$ are the annihilation operators of the input modes and $\hat{c}$ and $\hat{d}$ are the annihilation operators of the output modes. Using the transformation relation in Eq. (4.12), the positive frequency part of the output fields from the beam splitter is given by

$$\hat{E}_1^+(t) = \sum_l \frac{1}{\sqrt{2}} (\hat{a}_l + \hat{b}_l) e^{-iw_l t}, \tag{4.13}$$

$$\hat{E}_2^+(t) = \sum_l \frac{1}{\sqrt{2}} (\hat{b}_l - \hat{a}_l) e^{-iw_l t}. \tag{4.14}$$

In a conventional balanced homodyne experiment, the intensities and the path lengths after the BS are balanced in order to eliminate the classical noise. However, precisely balancing the path lengths is often a difficult task as there could be a delay between the photocurrents due to the different responses of the photodetectors or even due to their internal construction. The delay between the generation of the photocurrents is modeled as a path delay between the two output arms. The extra phase picked up by the corresponding field in that arm is given by

$$\hat{E}_1^+(t) = \sum_l \frac{1}{\sqrt{2}} (\hat{a}_l + \hat{b}_l) e^{-iw_l t} e^{-iw_l \tau}, \tag{4.15}$$

where τ is the delay between the two photocurrents. The photodetectors in the output

arms measure the intensity which is given by the operator

$$\hat{I}(t) = \hat{E}^{-}(t)\hat{E}^{+}(t), \tag{4.16}$$

where $\hat{E}^{-}(t) = (\hat{E}^{+}(t))^{\dagger}$. The subtracted photocurrent is evaluated using

$$\begin{aligned} \hat{i}(t) &\propto \hat{I}_1(t) - \hat{I}_2(t) \\ &= \hat{E}_1^{-}(t)\hat{E}_1^{+}(t) - \hat{E}_2^{-}(t)\hat{E}_2^{+}(t). \end{aligned} \tag{4.17}$$

In order to evaluate the statistics of the photocurrent, we evaluate the expectation value and the variance of the difference current operator with respect to the input state given in Eq. (4.11). Evaluating the expectation value of the difference current operator given in Eq. (4.17) with respect to the state in Eq. (4.11), we have

$$\begin{aligned} \langle \hat{i}(t) \rangle_{\psi_{\text{in}}} &= \langle \hat{E}_1^{-}(t)\hat{E}_1^{+}(t) - \hat{E}_2^{-}(t)\hat{E}_2^{+}(t) \rangle_{\psi_{\text{in}}} \\ &= \frac{|\alpha_0|^2}{2}\Big(\frac{\sin^2\left((M+0.5)\Delta\omega(t+\tau)\right)}{\sin^2\left(0.5\Delta\omega(t+\tau)\right)} \\ &\quad - \frac{\sin^2\left((M+0.5)\Delta\omega t\right)}{\sin^2\left(0.5\Delta\omega t\right)}\Big). \end{aligned} \tag{4.18}$$

It is evident from Eq. (4.18), that as τ approaches 0, the expectation value vanishes. This is in accordance with the general expression for the homodyne output and can be verified from Eq. (4.4). Similarly, the variance of the difference photocurrent is evaluated to be

$$\begin{aligned} \langle \Delta\hat{i}^2(t) \rangle_{\psi_{\text{in}}} &= \langle \hat{i}^2(t) \rangle_{\psi_{\text{in}}} - \langle \hat{i}(t) \rangle_{\psi_{\text{in}}}^2 \\ &= \frac{|\alpha_0|^2(2M+1)}{2}\Big(\frac{\sin^2\left((M+0.5)\Delta\omega(t+\tau)\right)}{\sin^2\left(0.5\Delta\omega(t+\tau)\right)} \end{aligned}$$

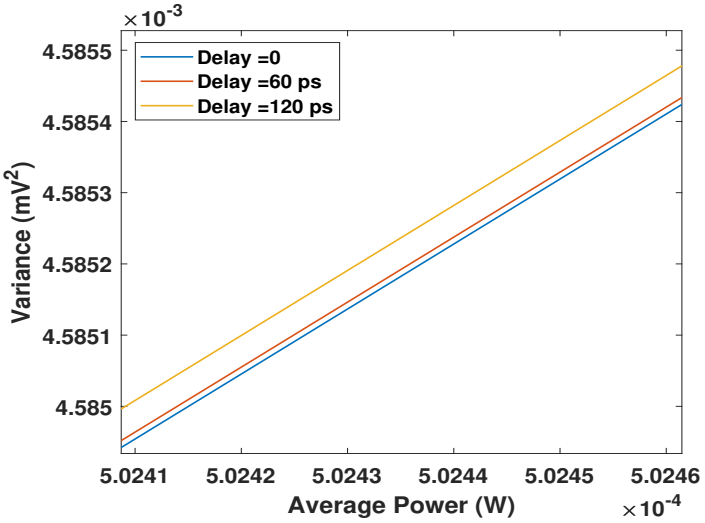

Figure 4.4: Simulated results for shot noise for various delays. The curve shows voltage variance for different average power values for 0 delay and delays of 60 ps and 120 ps.

$$+\frac{\sin^2\left((M+0.5)\Delta\omega t\right)}{\sin^2\left(0.5\Delta\omega t\right)}\Big). \tag{4.19}$$

It is readily seen from Eq. (4.19), that as τ approaches 0, the variance of the difference current is proportional to the intensity of the LO field Eq. (4.8). We have performed a simulation on the measurement of the shot noise of a pulsed laser source when there is a delay between the two homodyne arms. We have also simulated the effect of different pulse integration windows on the measurement of shot noise. In the simulation, we have generated a pulsed laser field with a repetition rate of 80 MHz. The impulse response of the photodetectors has been taken into account to generate output electronic pulses with a width of 1.6 ns. These parameters are chosen in order to replicate the conditions observed in our experiment. For ultrafast pulses, when detected using photodetectors, the output photocurrent pulses have a pulse width of the order of ns. This is due to the impulse response of the photodetector. In our exper-

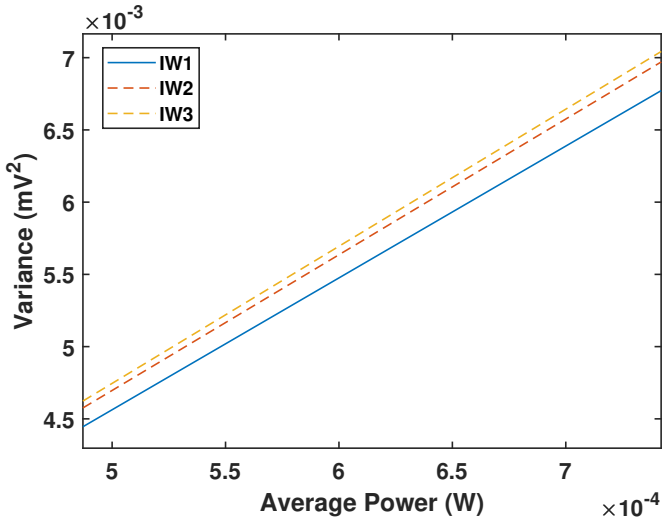

Figure 4.5: Simulated results for shot noise for various pulse integration windows (IW). The voltage variances are plotted against the average power for different integration windows (IW1, IW2 & IW3). The integration windows selected are 1.6 ns, 1.8 ns, & 2 ns, respectively.

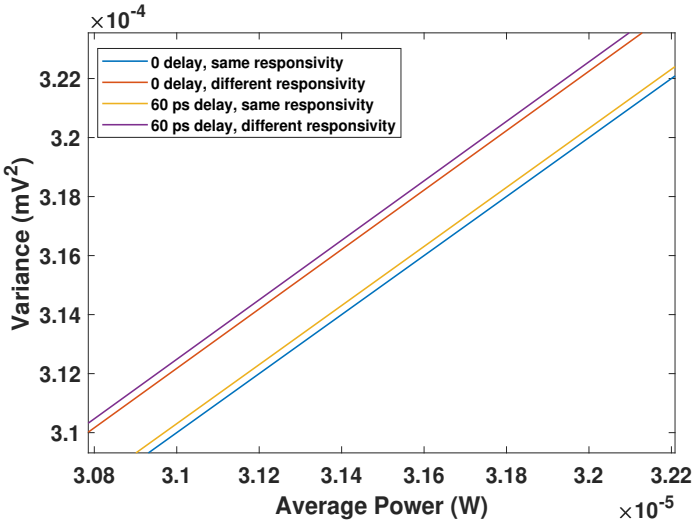

Figure 4.6: Simulated results for shot noise for various delays with different responsivities of the detector. A 1% difference in the responsivities of the detectors has been considered here. The shot noise variance is plotted against the input LO power for different delays as well for the case of different detector responsivities.

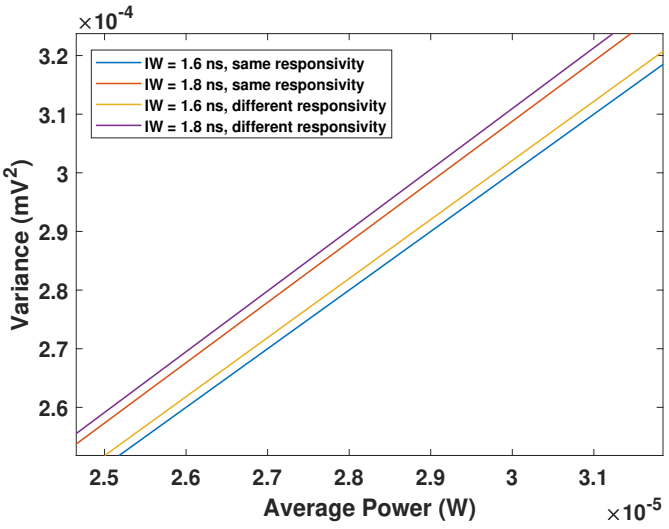

Figure 4.7: Simulated results for shot noise for various integration windows with different responsivities of the detector. A 1% difference in the responsivities of the detector has been considered here. The shot noise variance is plotted against the input LO power for different delays and for the case of different detector responsivities.

imental setup, it was observed that the output photocurrent pulses had a pulse width of 5 ns and 1 ns for Layout-1 and Layout-2, respectively. Our simulation has taken these effects into account. Further, the delay between the homodyne arms has no significant impact on the shot noise measurement if the pulse width is much larger than the delay. The simulated results for various delay conditions are shown in Fig. 4.4, and the results for the various integration windows are shown in Fig. 4.5. It is seen from Fig. 4.4 that on increasing the delay between the output arms, the measured shot noise also increases. Further, this increase has a non-linear dependence on the delay as evident from Eq. (4.19). Similarly, from Fig. 4.5, it is evident that, on increasing the pulse integration window, the measured shot noise value increases. Fig. 4.6 depicts the effect of different responsivities of the photodetectors on shot noise measurement for various delays between the detector arms. Similarly, Fig. 4.7 depicts the effect of different responsivities of the photodetectors on shot noise measurement for different integration windows used. A difference of 1% in the responsivities between the detec-

tors is considered here. It is evident that when there is a difference in the responsivities between the detectors, the measured shot noise increases. The experimental results are discussed and compared with the theoretical simulations in Sec. 4.4.

4.3 Experimental Setup

The implementation of a BHD for time domain analysis is followed by the below experimental details.

4.3.1 Pulsed Laser Source

In the experimental setup, we have used an 810 nm ultrafast mode-locked Ti-Sapphire laser, with an output power of approximately 500 mW. The pulse width of the laser is around 30 fs with a repetition rate of 80 MHz. The spectral width of the laser is 20 nm as shown in Fig. 4.8. A variable optical attenuator (VAT) is used to reduce the laser

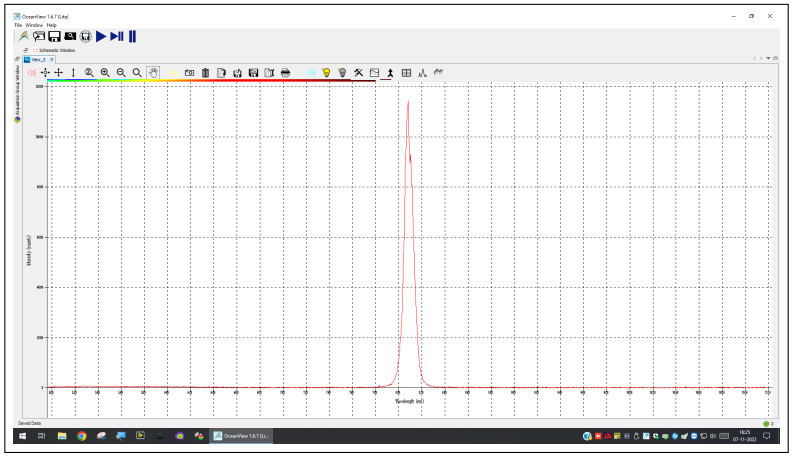

Figure 4.8: Laser spectrum for femtosecond pulsed laser.

output power to 2 mW which is desired for our experiment. The beam is split using a 50:50 beam splitter (BS). Two attenuators (ATT) are placed in the output arms of the BS in order to balance the photocurrents. The attenuators are a combination of a half-

wave plate (HWP) and a polarising beam splitter (PBS). The experimental schematic for both layouts is similar except for the detection part.

4.3.2 BHD with Amplification

The experimental setup for Layout-1 is as shown in Fig. 4.9. In Layout-1, we have used a commercially available balanced detector (Thorlab's PDB435A, DC-350 MHz) to measure the subtracted photocurrent output which is the homodyne signal. The

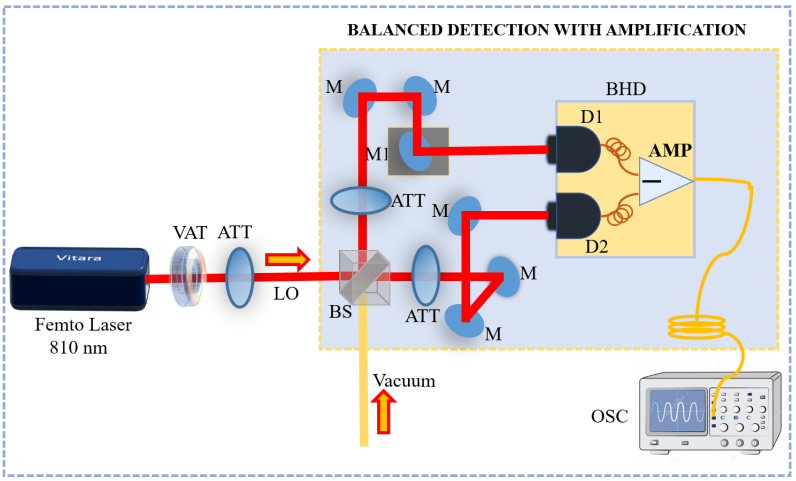

Figure 4.9: The schematic diagram for Layout-1. A mode-locked 810nm pulsed laser having a repetition rate 80 MHz is used as a source, and a variable attenuator (VAT) is used to control its power. A 50:50 beam splitter (BS), with additional attenuators in each arm, is used to balance the photocurrents. Mirror M1 is used to control the delay between the two output arms. The output difference signal from BHD consisting of photodetectors (D1 and D2) and transimpedance amplifier (AMP) is seen and recorded on an oscilloscope (OSC).

balanced detector consists of two photodetectors (D1 and D2) and the photocurrents are subtracted and amplified internally using a trans-impedance amplifier (AMP). A digital storage oscilloscope (Agilent/Infiniium DSO 900254A, 2.5 GHz, 20 GSa/s) is used to record the output signal of BHD. The mirror M1 is mounted on a translation stage in order to control the delay between the two arms. The experimental setup is

shown in Fig. 4.9.

To confirm the linear functioning of the photodetectors, the average voltage signal is determined as a function of the input optical power for each photodetector. The noise variance of a balanced detector is expected to change linearly with the LO power with a constant offset representing the electronic noise. We measured the shot noise as a function of LO power for three different delays and the results are discussed in Sec. IV.

4.3.3 BHD without Amplification

The experimental setup for Layout-2 is as shown in Fig. 4.10. In Layout-2, we have used two individual photodetectors (PDs), [DET025AFC, bandwidth 2 GHz, efficiency 76 %], to measure the photocurrents. The difference signal is obtained by subtracting the photocurrents using a digital storage oscilloscope (DSO 900254A, 20GS/s, 2.5GHz). The experimental setup for the same is shown in Fig.4.10. Mirror M1 is placed on a translation stage and is used to control the delay between the two output arms of BS. Similar to Layout-1, we have performed the linearity test of the photodetectors and have measured the shot noise as a function of LO power. The results are presented in Sec. IV, and both layouts are compared.

4.3.4 Data Acquisition

The data acquisition for both Layout-1 and Layout-2 is similar. The steps involved in the process are detailed below.

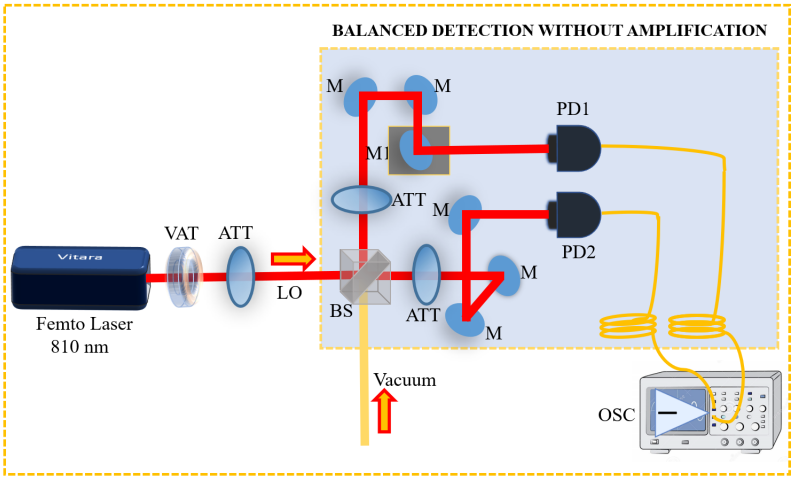

Figure 4.10: The schematic diagram for Layout-2. A mode-locked 810 nm pulsed laser having a repetition rate 80 MHz is used as a source, and a variable attenuator (VAT) is used to control its power. A 50:50 beam splitter (BS) with additional attenuators in each arm is used to balance the power. Mirror M1 controls the delay between the two arms of BS. Instead of using a BHD, we use two photodetectors and subtract the output photocurrents using the oscilloscope (OSC) and save the pulses.

Photodetector Linearity Test

The first step in the process of balanced detection includes the characterization of the individual photodetectors. To perform the linearity test of individual photodetector we proceed with the following steps,

- Sequentially, we open the photodetectors one at a time and record the output voltage as a function of the incident optical power on each detector. The optical power is controlled by using ATT placed before the BS.

- An acquisition window of 50 ns is set in the oscilloscope that contains 4 pulses/-trace with a separation of 12.5 ns. In this setting, both the detector outputs are recorded. 2000 such time traces (containing 8000 pulses) are recorded for each power value.

- The measurement is repeated for input optical power varying from 100 μW to 400 μW.

- The average voltage signal from both the photodetectors is plotted versus the input optical power incident on them. The resultant graphs for Layout-1 and Layout-2 are shown in Fig. 4.14 and Fig. 4.15 respectively.

Shot Noise Linearity Test

In the process of characterizing balanced detection, another essential test involves measuring the noise variance with respect to the LO power. This measurement is conducted with the input set to the vacuum state, meaning the signal beam is blocked. In a balanced detection, the noise variance is expected to change linearly with the LO power, with a constant offset representing electronic noise. This linear relationship ensures that the measured noise corresponds to the shot noise. The steps for measuring shot noise are detailed below.

1. An acquisition window of 50 ns is set in the oscilloscope that contains 4 pulses in a single trace with a separation of 12.5 ns. In this setting, the subtracted signal is recorded. 2000 such time traces (containing 8000 pulses) are recorded for each power value shown in Fig. 4.11.

2. The average trace is calculated and subtracted from each original trace shown in Fig. 4.12.

3. The traces obtained by this procedure are shown in Fig. 4.13.

4. To measure the shot noise, the processed pulses are integrated over a window of 5 ns for Layout-1 and 1 ns for Layout-2. This dissimilarity in the integration

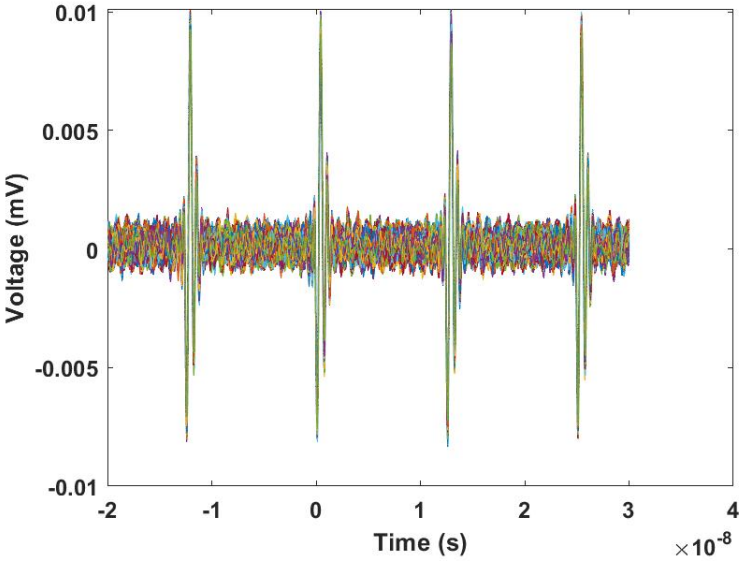

Figure 4.11: Data processing procedure, for Layout-2 at a fixed LO power. 2000 original time traces containing 8000 pulses.

windows is due to the different response times of the photodetectors. The variance of all such integrated values is determined for one particular power. This procedure is repeated for the various LO powers considered.

5. The measurement is repeated for LO power varying from 250 μW to 950 μW within a step size of 50 μW for both Layout-1 and Layout-2. The power of the LO is changed using ATT placed before the BS in each case.

6. The data is collected for three different delays; 0 ps, 70 ps, and 140 ps for both Layout-1 and Layout-2. The graphs for shot noise for the respective layouts at different delay conditions are shown in Fig. 4.16 and Fig. 4.17.

7. To study the effect of the pulse integration window on shot noise, the delay is fixed between the homodyne arms and the integration window is varied for both layouts. For Layout-1, the zero delay condition is set, and the integration windows 4.2 ns, 4.6 ns, 5.3 ns, 6.8 ns, and 8.2 ns are considered. For Layout-2,

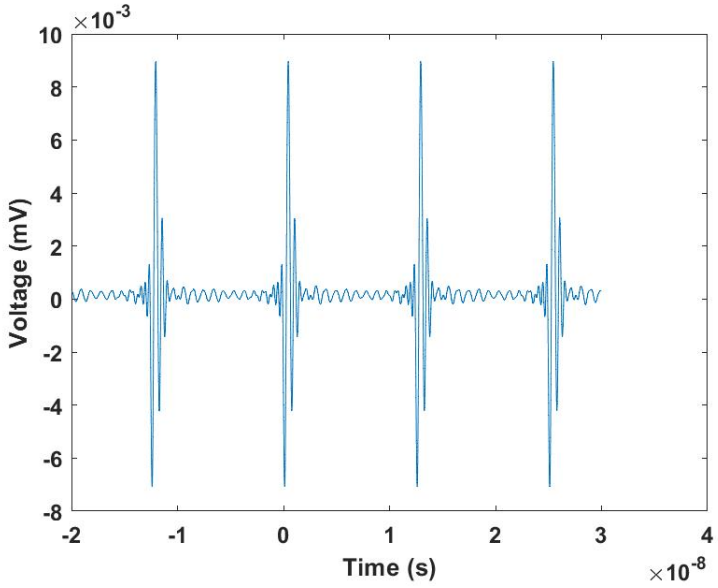

Figure 4.12: 2000 processed traces (8000 pulses) obtained by subtracting the average trace from the original traces.

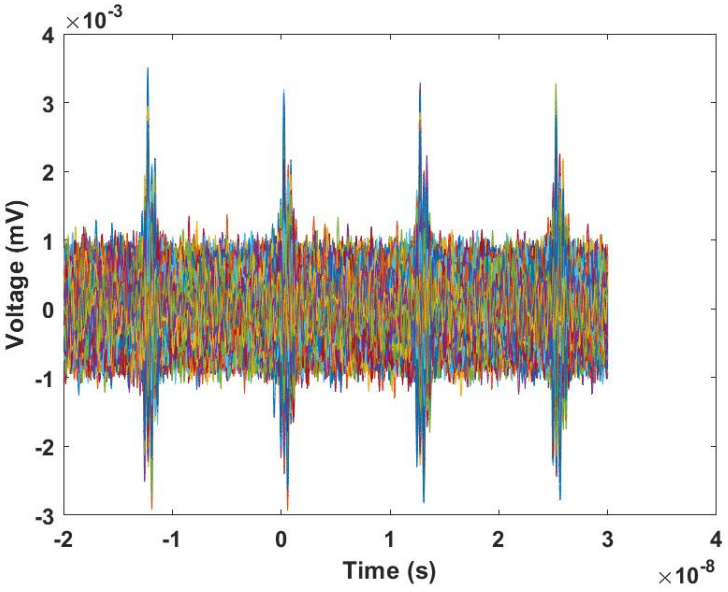

Figure 4.13: Average trace obtained by averaging 2000 original time traces.

the zero delay condition is set and the integration windows 0.8 ns, 1 ns, 1.2 ns, 1.5 ns, and 1.75 ns are considered. The graphs for the same are shown in Fig. 4.18 and Fig. 4.19.

8. The electronic noise is measured by blocking the LO beam and recording the resulting noise signal in the oscilloscope. The integration process is carried out over the corresponding intervals and the electronic noise is estimated.

4.4 Results and Discussion

We have carried out an experiment to measure the shot noise using the two layouts described in the previous Section. We are interested in studying the effect of delay between the two homodyne arms and the effect of varying the pulse integration window on the measured shot noise. We have also performed a comparative study of both layouts. The data acquisition procedure has been described in Sec. 4.3.4.

Fig. 4.14 and Fig. 4.15 plot the results of the linearity test of the individual photodetectors for Layout-1 and Layout-2, respectively. It is evident from Fig. 4.15 that both the photodetectors exhibit a linear response to the input optical power and that their responses are identical. From Fig. 4.14, it is evident that the photodetectors in the balanced detector exhibit a linear response to the input optical power. However, it is readily seen that the responses differ slightly in the high power regime. This is due to the fact that there is a difference in the responsivities of the photodetectors of about 7%. The simulated impact of different responsivity on the measured shot noise is shown in Sec. 4.2. There could be an additional noise added to the shot noise due to the different responsivity of the detectors. This difference can be compensated by adjusting the power in one of the homodyne output arms in the experimental setup such that both detectors show similar behavior. This compensation is achieved experimentally

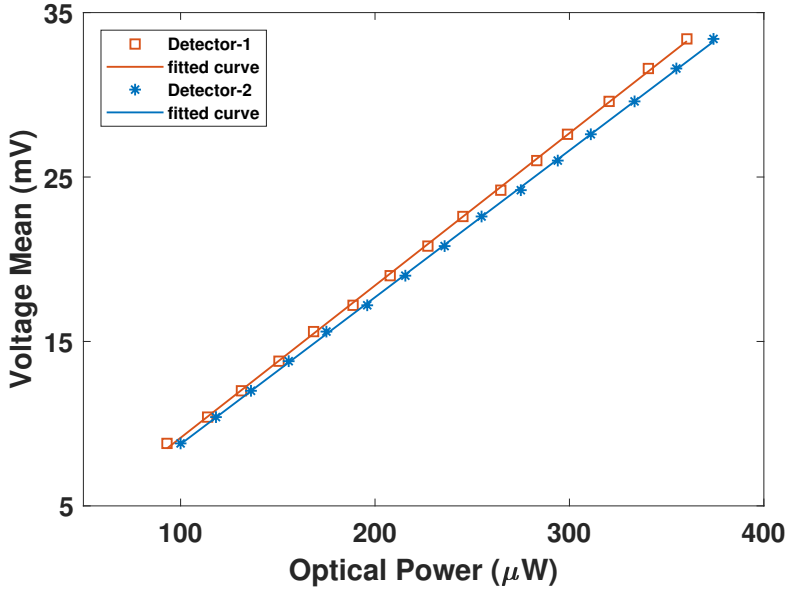

Figure 4.14: Linearity graphs for the photodetectors for Layout-1. The graph plots the mean output voltage as a function of the input optical power incident on the photodetectors.

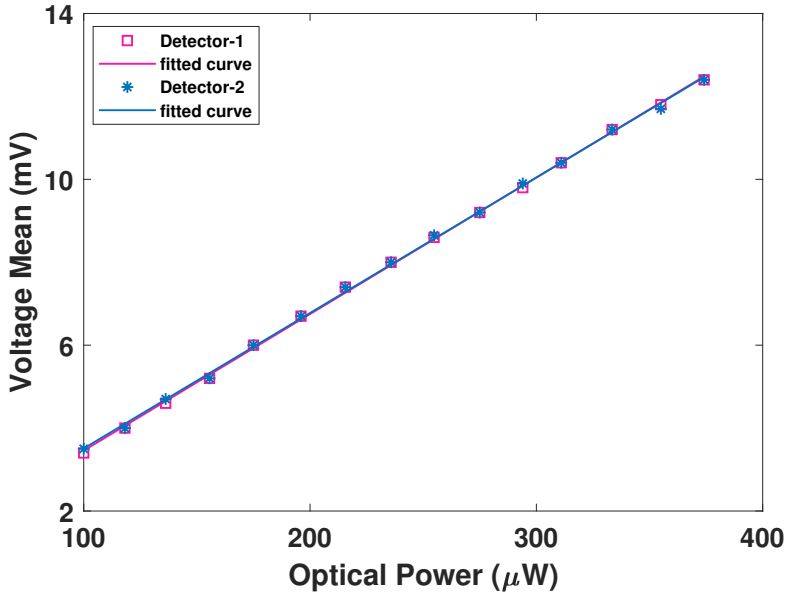

Figure 4.15: Linearity graph for the photodetectors for Layout-2. The graph plots the mean output voltage as a function of the input optical power incident on the photodetectors.

by adjusting the attenuators (ATT) positioned in the homodyne output arms.

Fig 4.16 and Fig. 4.17 plot the variation of the shot noise measured as a function of the LO power for different delay conditions for Layout-1 and Layout-2, respectively. It is observed that the shot noise measured using the balanced detector follows the linearity trend for all the delays considered. It is further seen that, on increasing the delay between the homodyne arms, the slope of the shot noise graph increases. We define the signal-to-noise ratio (SNR) as the ratio between the measured quadrature variance at a particular LO power to the electronic noise measured. An SNR of 1.27 is obtained for zero delay condition at 950 μW LO power. The shot noise clearance can be defined as $10\log_{10}(\text{SNR})$. For our experimental scenario, the clearance is found to be 1.04 dB for the maximum LO power of 950 μW. The SNR increases with increasing LO power since the shot noise variance increases linearly as a function of LO power while electronic noise remains constant. In Fig. 4.16, the measured variances include contributions from electronic noise and quantum noise. By taking the difference between the measured variances at zero delay and the electronic noise, the quantum noise remains, which is plotted in the inset in the same figure. The same process, when applied to the measured variances at various delays yields similar graphs and are plotted in the inset. The subtracted variances at various delays have contributions from classical noise over quantum noise. The same process could be applied to the variances measured using Layout-2 to extract the quantum noise and the contribution of classical noise over the quantum noise for various delays. On comparing Fig. 4.16 and Fig. 4.4, it is readily seen that the experiment reproduces the theoretical simulation results. It is observed from Fig. 4.17 that the shot noise measured using Layout-2 is seen to be underestimated compared to the electronic noise. This could be due to the reason that the signal is almost merged with the electronic noise because of the absence of the amplifier, and we are not able to resolve it. However, it is seen that the slope of the shot noise graph

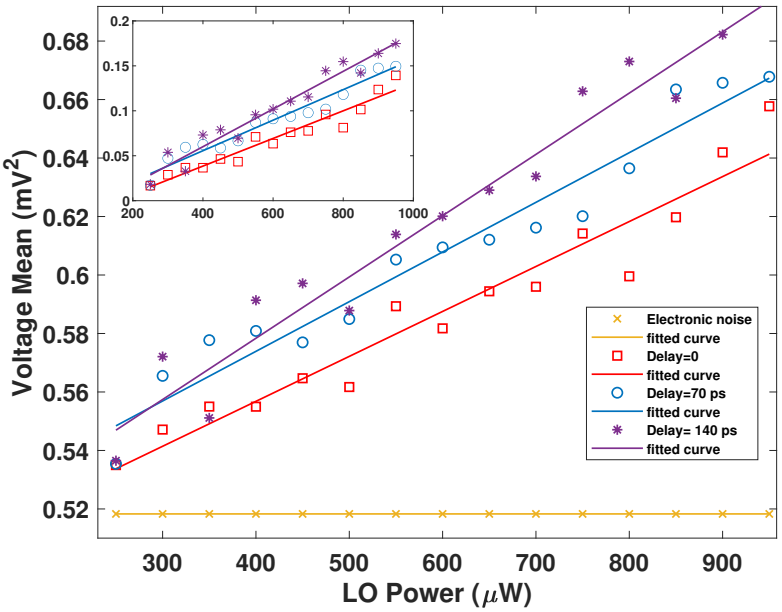

Figure 4.16: Shot noise graph for different LO power values for Layout-1. The voltage variances are plotted against three delay conditions i.e. 0 ps, 70 ps, and 140 ps. The constant line denotes the electronic noise. The data points represent experimental results, and the lines are the fitted curves. The inset denotes the difference between the measured variances and electronic noise at various delays. Thus, the graph for zero delay in the inset corresponds to the quantum noise, while the rest of the graphs in the inset contains an additive classical noise over the quantum noise.

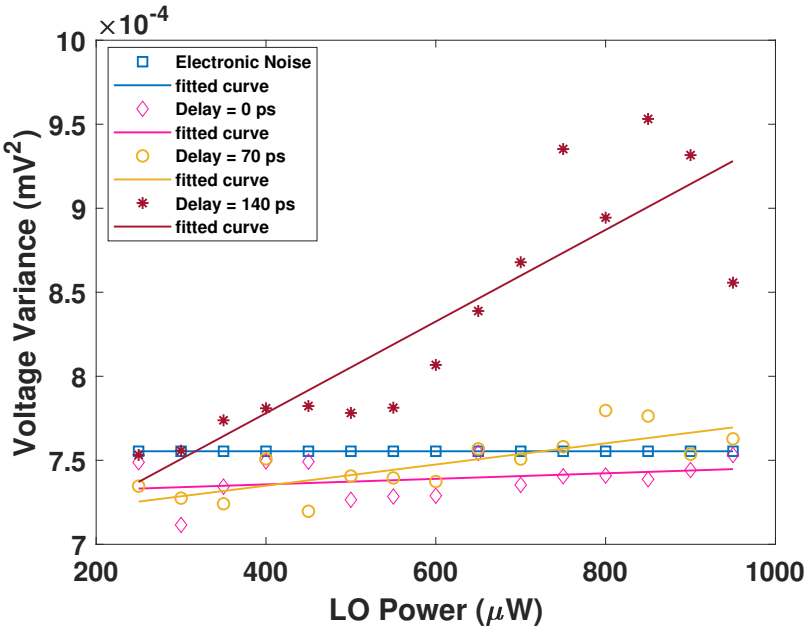

Figure 4.17: Shot noise linearity graph for different LO power values for Layout-2. The graph consists of electronic noise and variance for three delay conditions i.e. 0 ps, 70 ps, and 140 ps.

increases with increasing delay between the homodyne arms. It is seen that for the case of 140 ps delay, the data deviates from the linearity at some power values. We repeated the measurements, but the behavior is consistent for this particular case. However, we choose to work in the linear region only.

Fig. 4.18 and Fig. 4.19 show the shot noise measured versus the LO power for varying pulse integration window for zero delay condition for Layout-1 and Layout-2 respectively. It is observed that both graphs follow the linearity trend expected and with the same slope. However, the intercept is seen to increase which indicates a constant additive noise which is over and above the shot noise. This might be due to the reason that with an increase in pulse integration window we are including an additive noise to the estimation process leading to an increase in the shot noise values. This consequently leads to an overestimation of the electronic noise level. Comparing Fig. 4.5 with Fig. 4.18 and Fig. 4.19, it is seen that the experimental measurements of

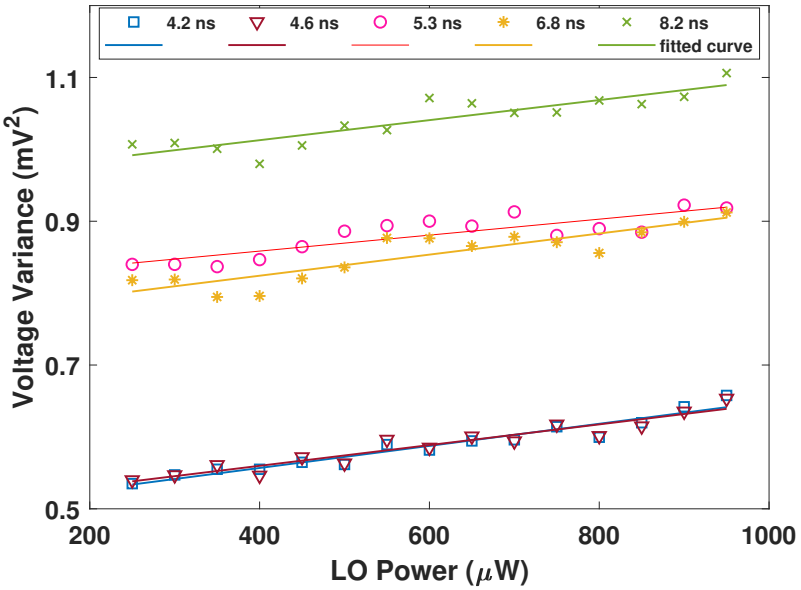

Figure 4.18: A graph for variance vs LO power for different integration windows, i.e., 4.2 ns, 4.6 ns, 5.3 ns, 6.8 ns, and 8.2 ns for Layout-1.

shot noise using various pulse integration windows match the results of the simulation based on the theory outlined in Sec. 4.2.

From the graphs, it is evident that the delay and pulse integration window have a considerable effect on the measurement of shot noise and must be accounted for carefully. Comparing the two schemes, we can conclude that there is a difference in the estimation of the shot noise at the zero delay condition, which is due to a difference in the amplification. Both layouts behave in a similar fashion on increasing the delay. Since the shot noise characterization is the primary task, one can use Layout-2 at the cost of increased variance due to some additional delay. Since the delay introduced is constant for each power value of the local oscillator, it should not affect the shot noise linearity trend. By accounting for the constant additive noise increase, we can use Layout-2 for estimating the shot noise of any pulsed laser source. This is particularly advantageous for experiments in continuous variable quantum optics as the

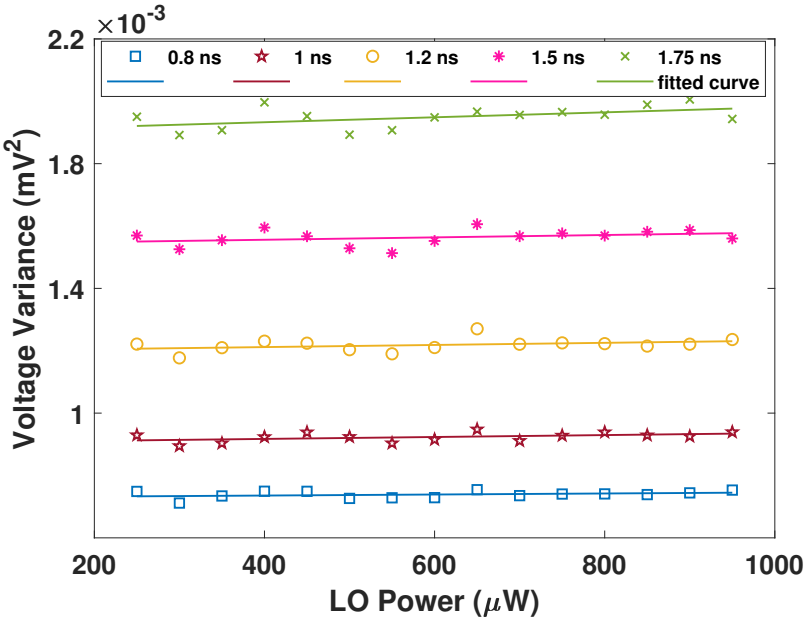

Figure 4.19: A graph for variance vs LO power for different integration windows i.e. 0.8 ns, 1 ns, 1.2 ns, 1.5 ns, and 1.75 ns for Layout-2.

layout requires fewer resources and there is no need to worry about the specifics of the amplifier such as gain and common mode rejection ratio (CMRR). One application of balanced detection has been the implementation of Quantum Random Number Generators (QRNG) based on shot noise [35, 136, 163]. Such QRNGs employ the use of a continuous wave laser as one can generate random numbers at a very high rate. The current studied experimental setup can be extended to generating random numbers at a very high rate using the shot noise of a pulsed laser source. However, the rate of random number generation will be limited by the repetition rate of the laser source. Further, the quality of the random numbers thus generated will be affected by the various imperfections which are addressed in this chapter. The excess noise added to the shot noise due to improper calibration of delay and pulse integration window could affect the quality of QRNG. This study might be helpful in characterizing such a QRNG and statistically validating the random numbers thus generated.

4.5 Conclusion

We have proposed a cost-effective scheme for measuring the shot noise of a pulsed laser source. We have studied the effect of delay between the homodyne arms and pulse integration window on the measurement of shot noise of a pulsed laser source. The parameters of delay and pulse integration window have a considerable effect on the measurement of shot noise and need to be accounted for carefully. By accounting for the additive noise caused by the introduction of a delay, Layout-2 proves to be an economical method for performing homodyne detection. Such a method is surely beneficial for demonstrations of CVQKD or optical tomography where homodyne detection is used.

Chapter 5

Free Space Discrete Modulation CVQKD

Quantum Key Distribution (QKD) offers unconditional security in principle. Many QKD protocols have been proposed and demonstrated to ensure secure communication between two authenticated users. Continuous variable (CV) QKD offers many advantages over discrete variable (DV) QKD since it is cost-effective, compatible with current classical communication technologies, efficient even in daylight, and gives a higher secure key rate. Keeping this in view, we demonstrate a discrete modulation CVQKD protocol in the free space which is robust against polarisation drift. We also present the simulation results with a noise model to account for the channel noise and the effects of various parameter changes on the secure key rate. These simulation results help us to verify the experimental values obtained for the implemented CVQKD.

5.1 Introduction

With the advancement in technology, the demand for secure communication has increased. In classical communication, the security relies on the complexity of the underlying mathematical algorithm and can be easily compromised once there is enough computational advancement [164]. QKD [119, 165] provides a secure way to distribute a key between two communicating parties, Alice and Bob. QKD uses quantum states to encode the key information, and its security completely relies on the laws of quantum mechanics, making no assumptions about the adversary's technological power [166]. The key exchange takes place through the quantum channel and is post-processed using an authenticated classical channel.

Implementing QKD over large distances enables secure quantum communication over a global scale and involves DVQKD protocols, which require encoding the key information in a single quantum state [88, 167–171]. The practical implementation of these QKD protocols involves various challenges, one of which is the generation of deterministic single-photons. However, achieving this in experimental setups can be difficult. Therefore, in order to experimentally demonstrate the DVQKD protocols, weak coherent pulses are widely used as an approximate single-photon source. But the risk of photon number splitting attacks would still persist in the weak coherent source, which could lead to security loopholes [172]. On the other hand, entanglement-based DVQKD protocols [44] are unconditionally secure [132], but the key rate obtained is very low.

Among the class of QKD protocols, CVQKD protocols have the potential to be proven as one of the best candidates [46, 99, 173]. CVQKD protocols use the quadratures of the electromagnetic field to encode key information [30, 174]. These protocols

are compatible with well-established classical communication technologies, thus enabling us to use existing communication infrastructure with enhanced security [175, 176] provided through quantum mechanics. Further, CVQKD protocols could be implemented using standard telecommunication components with a higher key rate [66, 177] as compared to DVQKD protocols. The state preparation step requires the use of amplitude and phase modulators, and the measurement step uses balanced homodyne detectors that are already available commercially and operate at a very high rate [62, 154, 155]. In addition, homodyne detectors are cost-effective and have high quantum efficiency at telecommunication wavelengths. These protocols are efficient at room temperature and daylight since the local oscillator acts as a spectral, temporal, and spatial filter and is robust against stray light.

According to the modulation scheme, we can divide CVQKD protocols into Gaussian modulation (GM) CVQKD and discrete modulation (DM) CVQKD. In the former case, one performs Gaussian modulation for both amplitude and phase quadratures, like Gaussian modulated coherent state (GMCS) or GG02 protocols [60, 61, 101]. The latter is based on the discrete modulation of the quadratures, like quadrature amplitude modulation (QAM) [49], and quadrature-phase sifts keying (QPSK) [48, 74, 178, 179] Gaussian modulated protocols offer practicality, advanced security proofs, [175] and have been successfully demonstrated to distances of hundreds of km [148] in fiber, making them efficient for metropolitan area networks. However, implementing such protocols over long distances is challenging as it is difficult to maintain good reconciliation efficiency at low signal-to-noise ratio (SNR) [67, 68]. The DM-CVQKD protocols simplify the modulation scheme and key extraction task, which is a bit complicated in GM-CVQKD protocols, where one extracts the key from continuous random values. DM-CVQKD protocols are remarkable for long-distance applicability even at low SNR [64, 180].

In this Chapter, we report the implementation of a free space DM-CVQKD protocol in the lab. The Chapter is structured as follows. In Sec. 5.2, the theoretical background for the protocol is discussed, and a noise model is presented to account for the channel noise. The imperfections present in the experiment are simulated and discussed. In Sec. 5.3, the experimental setup for the four-state DM-CVQKD is presented. Sec. 5.4 shows the experimental results, and we end up with concluding remarks in Sec. 5.5.

5.2 Theory and Simulation

In this Section, we discuss the theoretical aspects of the protocol implemented and present the details of the simulation performed. Further, we describe imperfections in the experimental implementation and provide models to simulate them. We end the Section with remarks on the security of the protocol and present the simulated results.

5.2.1 Protocol Execution

The protocol implemented in this manuscript consists of the following steps.

1. Alice randomly selects from the four coherent states $|\alpha e^{i\phi_A}\rangle$, where ϕ_A is chosen from $0, \pi/2, \pi$, and $3\pi/2$ by modulating the phase of her signal. This signal is transmitted to the receiver Bob. The phases 0 and π correspond to encoding the bit in the $\hat{q}$ basis, and $\pi/2$ and $3\pi/2$ correspond to the $\hat{p}$ basis, respectively. Here, $|\alpha|^2$ is the mean photon number of the signal.

2. Bob performs homodyne detection [36] on the received signal and randomly decides to measure the $\hat{q}$ quadrature or the $\hat{p}$ quadrature by modulating the phase of the local oscillator (LO), choosing ϕ_B as 0 or $\pi/2$ respectively.

3. After the exchange of signals, Alice discloses the basis in which the bit was encoded, and Bob discloses the basis in which the signal was measured. They retain the pulses for which the encoding and the measuring basis match. This process is called sifting.

4. The quadrature probability distributions for the measurements made by Bob for various $\phi = \phi_A - \phi_B$ are Gaussian centered at $\pm\alpha$ for $\phi = 0$ and π respectively and at 0 for $\phi = \pi/2$ and $3\pi/2$. The probability distributions for $\phi = \pi/2$ and $3\pi/2$ are indistinguishable and hence do not contribute to the key.

5. The measured values for $\phi = 0$ and π contribute to the key. Since in homodyne detection, the measured output values are continuous, Bob assigns a threshold x_0 to the sifted signals for post-selection and assigns his bit value as

$$\text{bit value} = \begin{cases} 1 & x_\phi > x_0 \\ 0 & x_\phi < -x_0 \\ \text{inconclusive} & -x_0 < x_\phi < x_0. \end{cases} \tag{5.1}$$

6. Alice assigns her bit value as 1 for $\phi_A = 0$ and $\pi/2$ and 0 for $\phi_A = \pi$ and $3\pi/2$.

7. Alice and Bob disclose a fraction of their raw key in order to perform parameter estimation and mutual information to get the final secret key.

In order to understand the limitations of the carried out laboratory demonstration, a simulation of the DM-CVQKD protocol was performed.

5.2.2 Noise Model

One of the major roadblocks in the implementation of quantum information protocols is the presence of noise and attenuation, which is unavoidable due to interactions of the quantum system with the environment. The state that Alice prepares is sent to Bob via a quantum channel which in reality can either be a fiber optic or a free space. The propagation of this state through the quantum channel alters the state at the output, which in turn affects Bob's measurement and introduces errors in the generated key. The effect of the transmission losses and the channel noise on the transmitted state can be evaluated by considering a model as shown in Fig. 5.1.

A fictitious beam splitter of transmittance $T < 1$ is inserted into the quantum channel separating Alice and Bob. The beam splitter couples the quantum state to the environment, which introduces noise in the state (see App. A). The transmittance T models the attenuation of the signal in the quantum channel. The density matrix for the ensemble of states shared by Alice can be written as

$$\hat{\rho}_{\text{sig}} = \frac{1}{4}\left(|\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle-\alpha| + |i\alpha\rangle\langle i\alpha| + |-i\alpha\rangle\langle-i\alpha|\right). \tag{5.2}$$

The effect of the channel can be evaluated by using the covariance matrix formalism [46]. The covariance matrix for the state in Eq. (5.2) is evaluated as

$$V = \begin{pmatrix} \frac{|\alpha|^2}{2} + \frac{1}{4} & 0 \\ 0 & \frac{|\alpha|^2}{2} + \frac{1}{4} \end{pmatrix}. \tag{5.3}$$

Here, $V_{\text{mod}} = \frac{|\alpha|^2}{2}$ is Alice's modulation variance. The covariance matrix after propa-

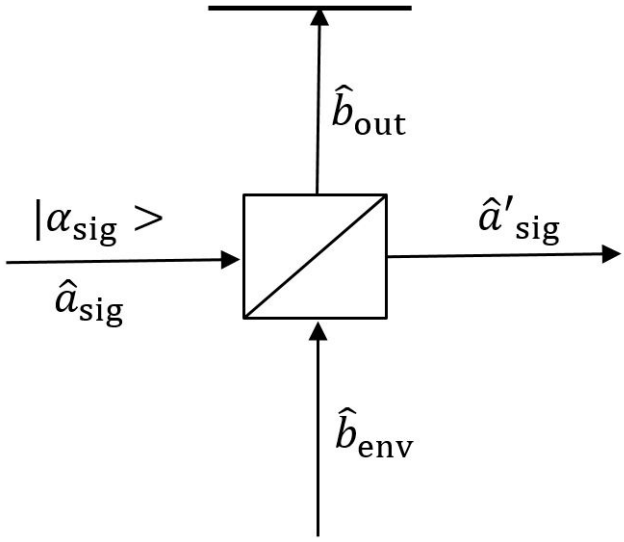

Figure 5.1: Theoretical model of the channel transmittance and noise included in the simulation. The beam splitter has a transmittance $T \leq 1$ and couples the quantum state $|\alpha\rangle_{\text{sig}}$ with the environment and hence introduces excess noise in input state. Here $\hat{a}_{\text{sig}}$ & $\hat{b}_{\text{env}}$ represent the input field operators of signal and the environment respectively and $\hat{a}'_{\text{sig}}$ & $\hat{b}_{\text{out}}$ denote the output field operators after interaction at the BS.

gation through the channel can be evaluated as

$$V_{\text{Bob}} = \begin{pmatrix} T\frac{|\alpha|^2}{2} + \frac{1}{4} + \xi_{\text{ch}} & 0 \\ 0 & T\frac{|\alpha|^2}{2} + \frac{1}{4} + \xi_{\text{ch}} \end{pmatrix}, \tag{5.4}$$

where ξ_{ch} is the noise added to the signal due to transmission in the channel.

Similarly, an imperfect homodyne detection at the receiver end can also be modeled using a beam splitter with transmittance η, which denotes the detection efficiency and noise ξ_{ele}, which models the electronic noise in shot noise units. The final covariance matrix for Alice and Bob's data will read as

$$V_{\text{AB}} = \begin{pmatrix} \frac{\alpha|^2}{2}\text{I}_2 & \frac{\sqrt{T\eta}|\alpha|^2}{2}\text{I}_2 \\ \frac{\sqrt{T\eta}|\alpha|^2}{2}\text{I}_2 & (T\eta\frac{|\alpha|^2}{2} + \frac{1}{4} + \xi_{\text{ch}} + \xi_{\text{ele}})\text{I}_2 \end{pmatrix}, \tag{5.5}$$

where I_2 represents the 2x2 identity matrix.

5.2.3 Mutual Information and Security

The secret key rate for a QKD protocol is defined by the relation,

$$k_{DR} = \beta I(A:B) - I(A:E) \text{ or} \tag{5.6}$$

$$k_{RR} = \beta I(A:B) - I(B:E), \tag{5.7}$$

in the case of direct and reverse reconciliation, respectively [134]. Here $I(A:B)$ is the mutual information shared between Alice and Bob, and $I(A:E)$ or $I(B:E)$ is the information leakage to Eve in case of direct reconciliation or reverse reconciliation. β is the reconciliation efficiency.

For DM-CVQKD under consideration, we have evaluated the mutual information between Alice and Bob by the relation,

$$\begin{aligned} I_{\mathrm{AB}} = {} & \frac{(q_1+q_2)}{2} + \frac{q_1}{2}\log_2\left(\frac{q_1}{(q_1+q_2)}\right) + \\ & \frac{q_2}{2}\log_2\left(\frac{q_2}{(q_1+q_2)}\right), \end{aligned} \tag{5.8}$$

where,

$$q_1 = \mathrm{erfc}\left(\frac{(x_0-\sqrt{T}\alpha)}{\sqrt{2(\frac{1}{4}+\xi_{\mathrm{ch}}+\xi_{\mathrm{ele}})}}\right) \text{ and} \tag{5.9}$$

$$q_2 = \mathrm{erfc}\left(\frac{(x_0+\sqrt{T}\alpha)}{\sqrt{2(\frac{1}{4}+\xi_{\mathrm{ch}}+\xi_{\mathrm{ele}})}}\right). \tag{5.10}$$

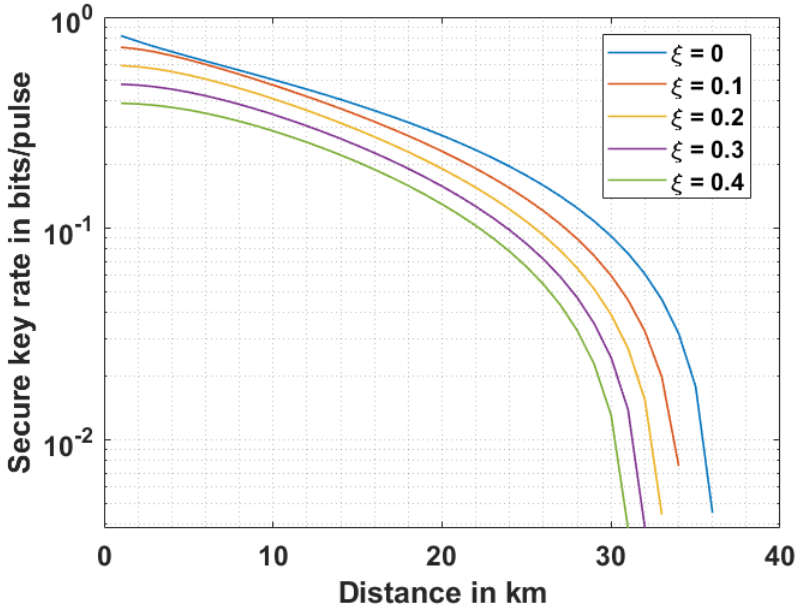

Figure 5.2: Plot of mutual information as a function of transmittance with different excess noises. Here, $\xi = \xi_{ch} + \xi_{ele}$ represents the total excess noise at Bob's end. ξ_{ch} denotes the noise added to the signal due to transmission in the channel & ξ_{ele} denotes the electronic noise present in the detection.

In Fig. 5.2, we plot the secret key rate achieved by the protocol for the case of a simple beam splitter attack by Eve. In this attack, Eve replaces the channel with a beam splitter of similar transmittance and a perfectly transmitting channel. Eve splits the signal on the beam splitter and keeps a part of the signal for measurement. The transformation on the state can be seen as

$$|\alpha\rangle_B |0\rangle_E \rightarrow |\sqrt{T}\alpha\rangle_B |\sqrt{1-T}\alpha\rangle_E , \tag{5.11}$$

where T is the transmittance of the channel, and the subscripts denote the person receiving the state. Eve then waits for the basis announcement and measures her state in the correct basis. Depending on the measurement result Eve makes a guess on the state sent by Alice. If her measured quadrature value is positive she makes a guess of Alice's bit as 1 otherwise as 0. The mutual information between Eve and Bob, $I(B:E)$,

can be evaluated and the secret key rate can be given as in Eq. (5.7). We have evaluated the mutual information between Bob and Eve for this particular beam splitter attack numerically, and the final secret key rate is as shown in Fig. 5.2. The secret key rate has been evaluated assuming the protocol is implemented with transmittance known as a function of distance. It is seen from Fig. 5.2 that for experimentally relevant values of excess noise, the protocol achieves a positive key rate even up to a distance of 35 km.

5.2.4 Simulation Results

In this Section, we have presented the simulation results obtained from our study. The results would help in a better understanding of the experimental setup and optimization of the experimental parameters. For simulation, the channel transmittance T, and the excess noise were considered as 0.9 (under lab conditions) and 0.02, respectively. Also, the signal was taken to be a weak coherent state with an average of 1 photon per pulse. Fig. 5.3 depicts the probability distribution of the values measured by Bob after both have disclosed their phases. It can be seen that the probability distributions for $\phi = 90^\circ$ and $\phi = 270^\circ$ are indistinguishable from each other, and hence Alice and Bob discard those measurements. The mean of the probability distribution corresponding to $\phi = 0^\circ$ and $\phi = 180^\circ$ differs from ± 1 due to attenuation in the channel and is given by $\pm\sqrt{T}$. Fig. 5.4 depicts the post-selection efficiency and the quantum bit error rate (QBER) versus the threshold value selected for various mean photon numbers of the signal. It can be readily seen from Fig. 5.4 that increasing the threshold value decreases the bit error rate and also decreases the post-selection efficiency. The trade-off gained by reducing the bit error rate is the reduction in post-selection efficiency which ultimately has an effect on the key rate. The simulation can help in optimizing the trade-off between bit error rate and post-selection efficiency by the optimal selection

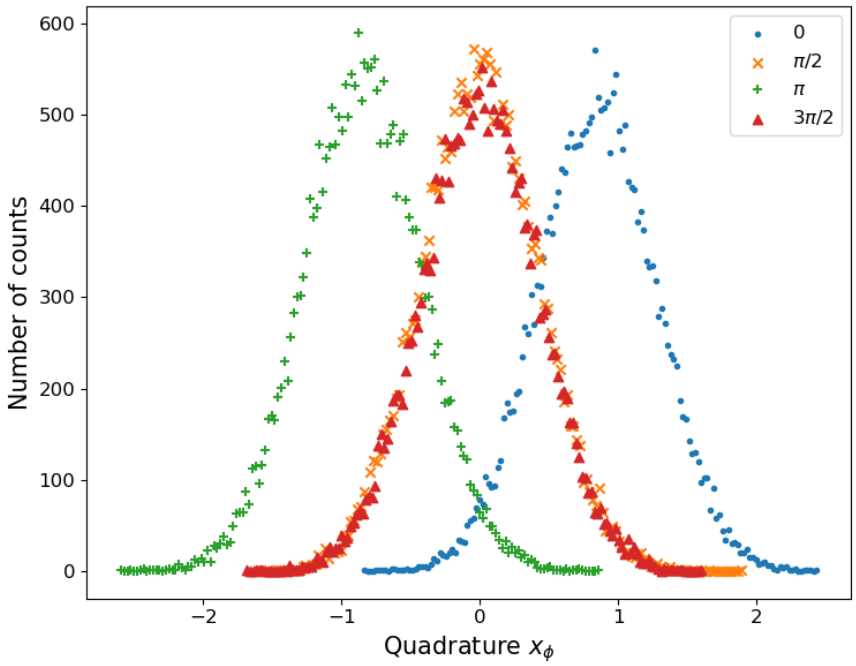

Figure 5.3: The simulated probability distribution of the measured homodyne output $\hat{x}_\phi$ corresponding to $\phi = 0, \pi/2, \pi, 3\pi/2$. Here, the mean photon number of the signal is 1. The channel transmittance T was taken to be 0.9 (under lab conditions) and the excess noise was taken to be 0.02. The probability distributions corresponding to $\phi = \pi/2$ and $\phi = 3\pi/2$ are indistinguishable; hence, the corresponding measurements are discarded.

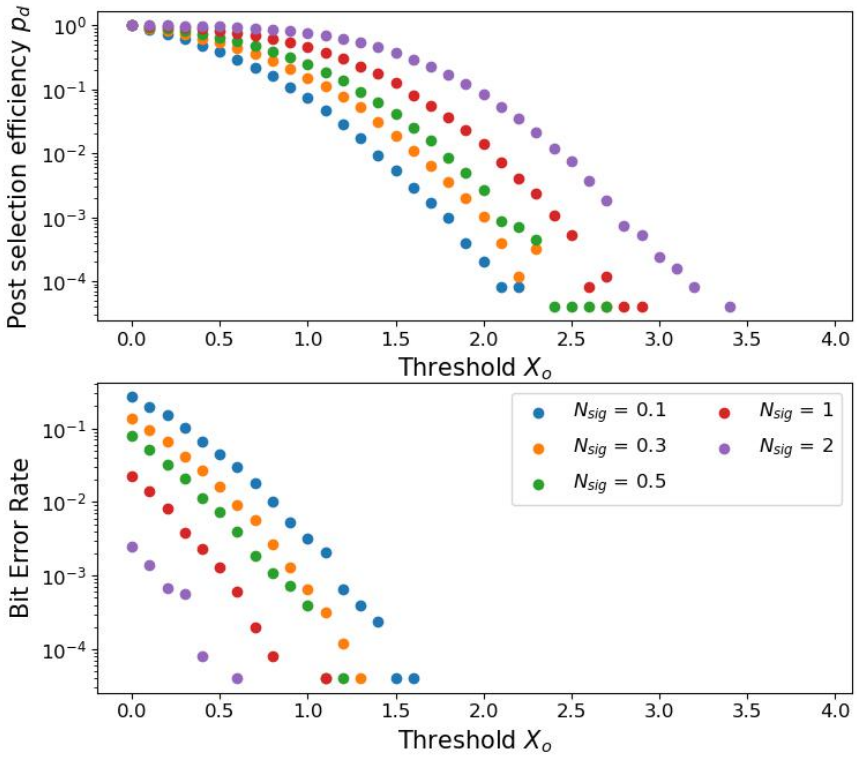

Figure 5.4: Plot of post-selection efficiency (top) and bit error rate (bottom) as a function of the threshold for various average photon number in the signal. The channel transmittance T was taken to be 0.9 (under lab conditions) and the excess noise was taken to be 0.02. It can be readily seen from the above graphs that on increasing the threshold x_0, the bit error rate decreases; however, it also results in a decreasing post-selection efficiency which results in a lower key rate.

of the threshold value for the experiment being performed.

5.3 Experimental Setup

The experimental setup for the demonstration of DM-CVQKD protocol in free space is shown in Fig. 6.1. We have used a 780 nm pulsed laser (NPL79B) operating at a 1 MHz repetition rate and 30 ns pulse width. We set up a Mach Zehnder interferometer (MZI) for the implementation of the DM-CVQKD protocol. The beam from the laser splits at a PBS into two arms of the interferometer. One arm is the signal, and the other is the local oscillator (LO). Alice controls the signal arm, whereas the LO arm is a part of Bob's detection system. We have used electro-optic phase modulators (EO-PM-NR-C1) to modulate the phase of Alice and Bob's signals.

We used a high-speed AWG (Tektronix AWG5000) to drive a high-voltage amplifier (Thorlabs HVA200) which in turn drives the PM. Both signal and LO arms include four mirror alignments (M_2, M_3 and M_8, M_9 are placed on translation stages) to adjust the delay between them. Before using the PM, the interferometer is calibrated so as to have zero phase difference between the arms. To do this, the mirror M_5 is placed on a PZT-stage (Attocube, ECSx3080) controlled by an AMC100 controller for a fine scan of the interferometer phase. Homodyne detection is performed at the final BS. The detection system includes a balanced homodyne detector, BHD (Thorlab's PDB435A, DC-350 MHz), which measures the subtracted photocurrent falling on the two detectors. A mixed signal oscilloscope, MSO (Tektronix 6-series), is used to record the output signal of BHD.

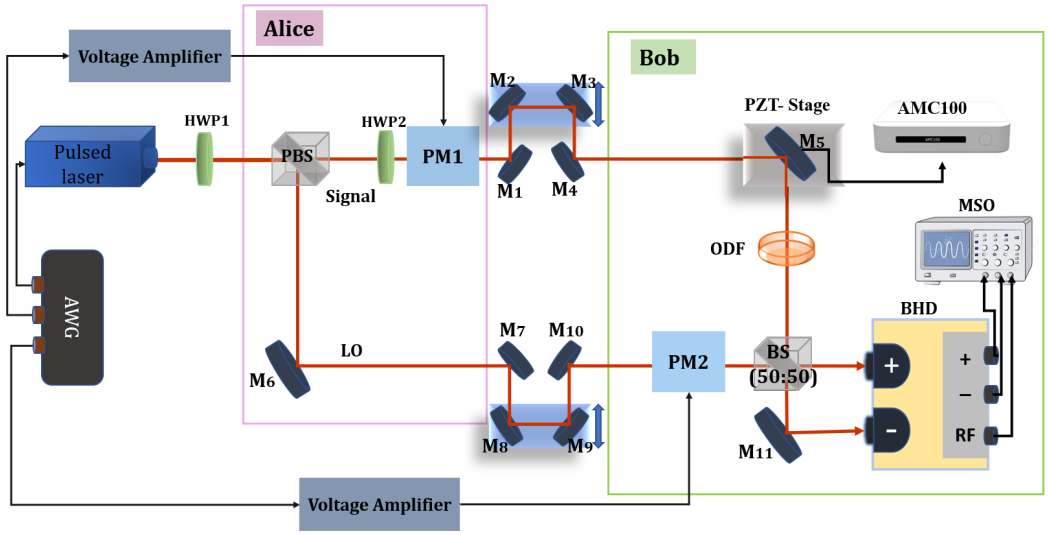

Figure 5.5: Experimental scheme for free space DM-CVQKD: HWP: Half Wave Plate; PBS: Polarising Beam Splitter; PM: Electro-optic Phase Modulator; LO: Local Oscillator; M: Mirrors; PZT: Piezo Controlled Nano-positioner Stage; AMC100: Nano-positioner Controller; ODF: Optical Density Filter; BS: Beam Splitter; BHD: Balanced Homodyne Detector; MSO: Mixed Signal Oscilloscope; AWG: Arbitrary Waveform Generator.

5.3.1 Alice

One arm of the interferometer i.e. the signal arm, is controlled by Alice. The phase modulator PM1 is used to encode the four-phase values for Alice i.e., $0, \pi/2, \pi$ and $3\pi/2$. The half voltage, V_π of PM is 170 V. An optical density filter (ODF) with $OD = 4$ is placed in the signal arm to reduce the signal intensity. Using the combination of HWP1 and ODF, we can control the mean photon number of the signal.

5.3.2 Bob

The other arm of the interferometer, which is the LO arm, is controlled by Bob. The power of the LO is varied using the HWP1 placed before the PBS. PM2 selects the $\hat{q}$-quadrature and $\hat{p}$-quadrature values corresponding to 0, and $\pi/2$. The mirror M_5 is

placed on a piezo nano-positioner stage to fine tune the path delay between the signal and LO arms. Bob performs homodyne detection at the final BS of the interferometer.

5.3.3 Data Acquisition

The phase modulation at both Alice's and Bob's ends is performed at a rate of 1 MHz. The subtracted output signal from the BHD is saved using an MSO. We have saved $8.1\text{x}10^4$ pulses in a single acquisition. Once sufficient data has been recorded, post-processing is performed. We integrate the individual pulses over their respective pulse duration. Each integrated value corresponds to one quadrature value at that particular phase. We then perform sifting, and the raw key is generated. The raw key is further processed, and the secure key is obtained. Error correction and privacy amplification are performed using LDPC codes and Toeplitz hashing, respectively.

5.4 Results and Discussion

In this Section, we present the results of our experimental implementation of the protocol. The security analysis of the DM-CVQKD experiments performed in the Chapter includes an asymptotic analysis of the security. Further, we have used the assumption that the excess noise due to an imperfect detection system is well characterised as in a trusted device scenario. The excess noise due to the channel has been attributed to Eve. Initial security analyses of DM-CVQKD protocols have assumed that the security of the Gaussian modulation can be extended to discrete modulation protocols under certain conditions on the modulation variance. However, recent results have improved upon this method, and better secure key rate bounds are available based on numerical methods [181].

The initial step in implementing the DM-CVQKD protocol is balancing the mea-

surement setup (not shown in Fig 6.1) and measuring the shot noise variance of the laser source [147, 153]. In the previous Chapter, we have performed the shot noise measurements using femtosecond laser. The study of shot noise measurements performed in Chapter-4 were carried out in order to understand the impact of imperfections in the detection setup on balanced homodyne detection. These studies are crucial for systems ultra-fast laser systems employing femtosecond or picosecond pulses with high repetition rates which in turn are essential for high rate QKD applications. We further found that these imperfections have negligible impact on nanosecond pulsed laser sources. While performing the CVQKD experiments we employed a nanosecond pulsed laser due to the constraint on the modulators performing at a max rate of 1 MHz. The effect of the excess noise due to imperfections in the homodyne measurement was found to be negligible and we were further able to ensure that the studied imperfections were mitigated by careful alignment.

To perform the intial calibration, the signal arm is blocked, and the difference signal is measured as a function of the LO power. This measurement is used to find out the shot noise and define the shot noise unit (SNU) for the experiment. Once the initial calibration is done, the power of the LO is fixed at 0.25 mW. The electronic noise-to-shot noise (electronic-to-shot noise ratio) clearance is found to be 15 dB. We then proceed with the implementation of the DM-CVQKD protocol.

The interferometer is calibrated to achieve zero path difference between the arms. The condition for constructive and destructive interference is achieved with a visibility of 98%. The signal is attenuated by using an optical density filter (ODF) of OD = 4 with an input power of 60 μW before ODF. The delay introduced by the ODF is compensated by scanning the translation stage and PZT stage. The phase of the signal is then varied from 0 to 2π by applying an appropriate voltage to the PM and the $\hat{q}$

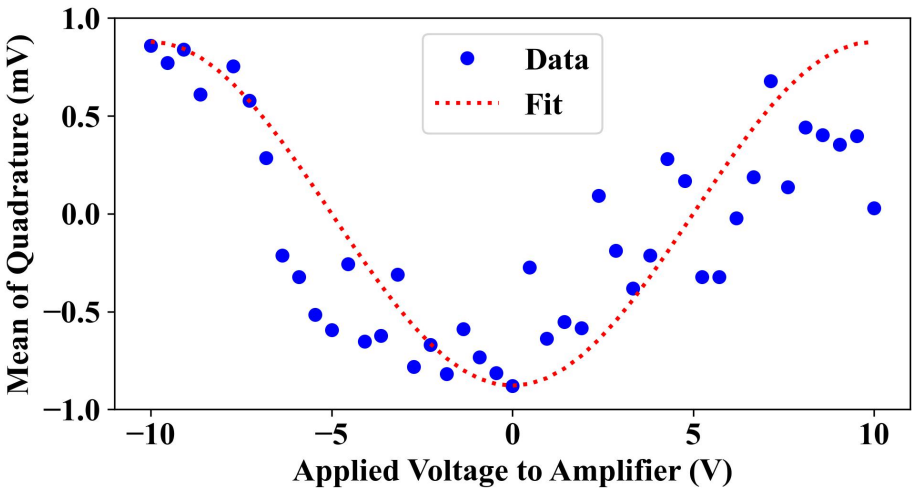

Figure 5.6: The variation of the mean $\hat{q}$ quadrature value of the signal as a function of the applied voltage to the PM. The voltage being applied to the PM is amplified using a voltage amplifier with a gain of -20X.

quadrature is measured using homodyne detection. For each applied voltage, 2000 pulses are saved, and the mean of the integrated values for the pulses are plotted as a function of the applied voltage as shown in Fig 5.6. The fluctuation in the data is due to the inherent phase instability of the Mach-Zehnder interferometer.

A proof of principle experimental demonstration of free space DM-CVQKD has been performed. The voltages fed to both Alice and Bob's PM are generated randomly using an AWG, shown in Fig. 6.1. A single acquisition in the MSO contains $8.1\text{x}10^4$ pulses. In order to retrieve the quadrature values from the signal, pulses are integrated over the respective time window. We do the basis sifting for Alice and Bob's data. The sifted key has a length of $4\text{x}10^4$ bits. The probability distributions of the quadrature values corresponding to relative phases are plotted in Fig 5.7. The threshold value x_0 chosen for the experiment is 0. For our laboratory experiments, the channel transmittance, $T = 0.95$, and detector efficiency $\eta = 0.76$ are observed. We calculated the mutual information between Alice and Bob, and finally, the secure key rate is extracted. The experimental parameters are shown in Table 5.1.

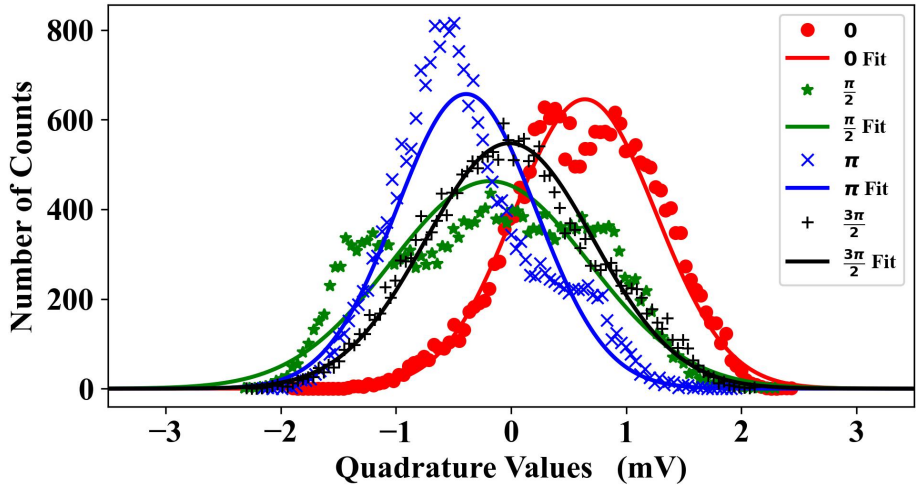

Figure 5.7: Probability distributions of the homodyne detected signal for the four relative phases between signal and LO. The points represent the experimental data, and the curves represent the best fit.

Parameters	Values
Signal processed	8.1x10^4 pulses
Sifted bits	4x10^4 bits
PSE	3.2x10^4 bits
QBER	5%
Secure key rate	0.35 (bit/pulse)

Table 5.1: The experimental results for the executed protocol for a single acquisition window. Here, PSE is the Post-selection Efficiency and QBER is the Quantum Bit Error Rate.

While performing CVQKD experiments, the very important parameter is the phase fluctuation of the Mach-Zehnder interferometer that affects the key rate. To account for these fluctuations, the phase stabilization of the MZI should be performed. To maximize the key rate, we will consider the noises introduced due to various sources present in the experiment in the near future. The advantage of DM-CVQKD is that it can go beyond QPSK modulation with constellations of larger size (e.g., 64 or 256 QAM). Such intermediate-size constellations provide better performance than the 4-state QPSK in practice. This could be one of the interesting perspectives of this work. We are exploring different CV-QKD schemes, including 16, 64, and 256 QAM. A

comparative study will also be performed to see the performance of these protocols and to explore their sustainability over atmospheric channels.

5.5 Conclusion

We have performed a prototype tabletop experiment of the DM-CVQKD protocol and have used the results to extract a secure key. We have also performed a simulation with a realistic noise model encountered in field demonstrations. The trade-off between the secure key rate and the bit error rate is illustrated using the results of the simulation. These studies assist in surveying the feasibility of continuous variable-based QKD protocols for ground as well as satellite-based communication systems. Conclusively, we can say that continuous variable-based QKD protocols can be perceived as the next frontier in the field of secure communication, be it fiber, free space, or satellite-to-ground communication.

Chapter 6

Implementation of Gaussian Modulation CVQKD

In this chapter, we performed the demonstration of Gaussian modulation CVQKD protocol over free space in the laboratory setting. We transmitted the Gaussian modulated coherent state over a quantum channel and performed the shot noise-limited homodyne detection at the receiver's end. We carefully calibrated the setup and calculated the electronic noise, shot noise and detection efficiency of the setup. We calculated the mutual information between Alice and Bob. Further, the processing of the data is under progress to assess the efficacy of this particular implementation to compare it with other implementations. The study of the protocol over free space would help in the field tests over the atmospheric channels and to check the feasibility of the satellite communication.

6.1 Introduction

QKD is one of the major applications of quantum information science. It is a process of generating a secure key between two legitimate users, Alice and Bob, over an insecure channel. The first QKD protocol was proposed in 1984, known as the BB84 protocol, which uses single-photons as an information carrier and belongs to the class of DVQKD. An alternative to the protocol is given after fifteen years of the first protocol of DVQKD, which was QKD with continuous variables (CV) proposed by Grosshans and Grangier (GG) in 2002. The first protocol of CVQKD was proposed using squeezed state of light. Later, protocols with coherent states came into the picture. The coherent state CVQKD protocol has an advantage over the squeezed state, as the generation of squeezed states is technically difficult. In the coherent state CVQKD, the key information is encoded in amplitude and phase of weak coherent states, thus allowing for implementation with current modulation methods and telecom-based equipment. The physical implementation of CVQKD using Gaussian modulated coherent state (GMCS) is based on mature optical communication techniques with high reliability and low cost. The motivation for CVQKD comes due to the better efficiency of homodyne detection at telecommunication wavelength (1550 nm) over single-photon detectors. These wavelengths are used in fiber optics because they have the lowest attenuation of the fiber.

Achieving a high secure key rate and long transmission distance are the major parameters for any secure communication for its practical applicability. Numerous progress has been made in this direction for Gaussian modulation (GM) CVQKD protocols. A secure key rate of 1 Mbps@25 km [182] and 6.214 bps@202 km [148] has been achieved in fiber using a transmitted local oscillator (LO) scheme. But transmitting LO along with the signal in fiber could lead to cross-talk and might be venerable

to quantum hacking attacks [183–185]. To overcome such limitations, the scheme using a local-local oscillator (LLO) has been proposed and demonstrated successfully. A secure key rate of 26.9 Mbps@15 km [186] and 7.04 Mbps@25 km [187] has been obtained using the LLO scheme. A recent study highlights the asymptotic secure key rate experimentally calculated to be 7.55 Mbps@50 km, 1.87 Mbps@75 km, and 0.51 Mbps@100 km, respectively [188] using the LLO scheme over the fiber channel.

While working with fiber as a quantum channel, we are limited by various factors like fiber losses; polarisation drifts inside the fiber, dispersion losses, and imperfect phase noise compensation. The problems are more prominent at higher speeds and over long distances. Compared to fiber-based CVQKD, the least work has been done in the direction of free space CVQKD. The free space CVQKD has the advantage over fiber-based as the transmission losses in free space are less than the fiber. It is easy to detect the presence of Eve in the line of sight. In addition to this, a free space channel is insensitive to polarisation compared to a fiber channel, which results in light polarisation being nearly unchanged during propagation. The feasibility of CVQKD in free space over long distances would help in satellite-based communication [189–191] and quantum networking [192, 193]. Practically, GM-CVQKD protocols have made significant progress in both theoretical security aspects [175, 194–196] and experimental techniques [197, 198].

In this chapter, we have implemented free space GM-CVQKD over 5-meters in our lab. In Sec. 6.2, we discuss the theoretical background for the protocol. In Sec. 6.3 we show the experimental implementation of the setup. In Sec. 6.4 we discuss the experimental results and we end up with concluding remarks in Sec. 6.5.

6.2 Theory

In GM-CVQKD protocol, Alice randomly generates two groups of Gaussian random numbers from two identical and independent normal distributions $N(0,V_A)$ corresponding to quadrature q and p. The quadrature q and p have the same modulation variance V_A in terms of shot noise unit. Gaussian modulation consists of intensity modulation and phase modulation. Intensity obeys a Rayleigh distribution, while phase obeys a uniform distribution. The quadratures q and p follow the relations,

$$\begin{aligned} q &= A_{sig}\cos\phi_{sig}, \\ p &= A_{sig}\sin\phi_{sig} \end{aligned} \tag{6.1}$$

where $A_{sig} = \sqrt{q^2+p^2}$ and $\phi_{sig} = \tan^{-1}(q/p)$ are the information loaded on the intensity modulator and phase modulator. After the preparation of each coherent state, Alice transmits the state to Bob through a quantum channel. Bob performs either homodyne (heterodyne) detection to extract the quadrature q or p (q & p). Later, using a publicly authenticated channel, he informs Alice about which quadrature he measured, so she may discard the irrelevant data. After many similar exchanges, Alice and Bob share a set of correlated Gaussian variables, which we call 'key elements'.

Alice and Bob perform classical data processing to obtain a secure binary key. They publicly compare a random sample of their key elements to evaluate the error rate and transmission efficiency of the quantum channel. From the observed correlations, Alice and Bob evaluate the amount of information they share ($I_{\mathrm{AB}} = I_{\mathrm{BA}}$), and the maximum information Eve may have obtained (by eavesdropping) about their values (I_{AE} or I_{BE}). From this information, they extract a common secure key 'k' of a certain length. This requires classical communication over an authenticated pub-

lic channel and may be divided into two steps, reconciliation (correcting the errors while minimizing the information to Eve) and privacy amplification (making the key secure) [67]. As we deal here with continuous data, we are developing reconciliation algorithms to extract common bit strings from the correlated key elements.

In the process of information reconciliation, where one party sends information about their key to the other party, two different approaches can be employed: forward reconciliation, where Bob corrects his bits based on Alice's data, or reverse reconciliation, where Alice corrects her bits based on Bob's data [59, 68]. In forward reconciliation, if the channel transmittance is less than 50% (3 dB loss limit), no secure key can be extracted. To overcome this limitation, Alice and Bob opt for reverse reconciliation. In this method, Bob sends the correction information to Alice, who then corrects her bit string based on Bob's data. In this scenario, Bob's data is considered primary, and since Alice possesses more information about Bob's measurement results than Eve does, the mutual information I_{AB} remains greater than I_{BE} for any total transmission T. As a result, a non-zero key can be obtained even for high transmission losses.

After the successful reconciliation process, Alice and Bob will possess the same bit string. However, it is important to note that Eve might still have some information about the key. To minimize Eve's probability of successfully guessing a portion of the key to an acceptable level, Alice and Bob perform privacy amplification, a process detailed further in Chapter 3, to enhance the security of the key.

The process of estimating the parameters experimentally is discussed in detail here,

Secure Key Rate: The secure key rate exchanged between Alice and Bob is calculated by using the relation,

$$k = \beta I_{\mathrm{AB}} - I_{\mathrm{BE}} \tag{6.2}$$

where, β is the reconciliation efficiency, and I_{AB} is the mutual information exchanged between Alice and Bob. I_{BE} denotes the Holevo bound, which put an upper bound to the information shared between Bob and Eve.

Parameter Estimation: In QKD protocols, the estimation of channel parameters holds significant importance. The mutual information between Alice and Bob, denoted as I_{AB}, is solely dependent on the signal-to-noise ratio (SNR).

The SNR for the case of homodyne detection in Gaussian modulation is defined as

$$\mathrm{SNR} = \frac{TV_{\mathrm{mod}}}{1+\xi} \tag{6.3}$$

where, T denotes the total transmittance, V_{mod} is Alice modulation variance, and ξ denotes the total excess noise.

The **mutual information** between Alice and Bob is defined by

$$\begin{aligned} I_{AB} &= \frac{1}{2}\log_2(1+\mathrm{SNR}) \\ &= \frac{1}{2}\log_2(1+\frac{TV_{\mathrm{mod}}}{1+\xi}) \end{aligned} \tag{6.4}$$

The **Holevo bound** I_{EB}, puts an upper bound to the information shared between Bob and Eve and is defined as,

$$I_{\mathrm{EB}} = S_E - S_{E/B} \tag{6.5}$$

here, S_E and $S_{E/B}$ represent the von Neumann entropy of the state accessible to Eve for collective measurement and projective measurement performed by Bob. The Holevo bound is derived from the covariance matrix mentioned in Chapter 2, Sec. 2.10.2. The

entropies S_E and $S_{E/B}$ are determined by the symplectic eigenvalues of the covariance matrix describing these states. The actual quantum state from which S_E and $S_{E/B}$ are derived depends on which kind of eavesdropping attack is assumed. More details regarding the covariance matrix and Holevo information have been discussed in Chapter 2.

This is to be considered that the detection performed in the experiment is quantum (shot noise) limited detection. So, prior to the actual parameter estimation, the measurement apparatus needs to be calibrated in order to map Bob's measurement in terms of shot noise unit (SNU) [45].

6.3 Experimental Setup

The experimental setup for the demonstration of GM-CVQKD protocol in free space over a distance of 5 meters is shown in Fig. 6.1.

At **Alice's** side, a 780 nm pulsed laser (NPL79B) operating at a 1 MHz repetition rate and 30 ns pulse width is used as a source. The beam is divided into two parts by a polarising beam splitter (PBS1). The upper arm is the local oscillator (LO) arm and the lower arm is the signal arm. The signal is incident on amplitude (EO-AM-NR-C1) and phase (EO-AM-NR-C1) modulator to generate amplitude and phase modulated signal. The electrical modulation signal is generated by using high-speed arbitrary waveform generator, AWG (Tektronix AWG5000) and is fed to the high voltage amplifiers (Thorlabs HVA200), which in turn drives the amplitude and phase modulators. An optical density filter (ODF) with $OD = 2$ is placed in the signal arm to reduce the signal intensity further. Using the combination of half wave plate (HWP1) and ODF, we can control the intensity (hence mean photon number) of the signal. The signal and LO beams are multiplexed at the PBS3, having orthogonal polarisations. Both the

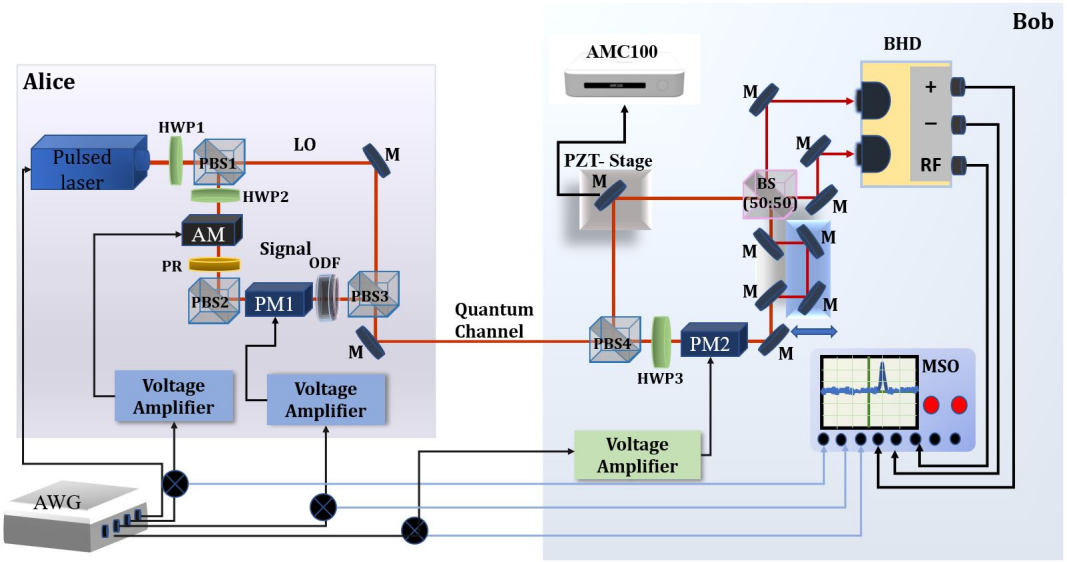

Figure 6.1: Experimental scheme for free space GM-CVQKD over 5 meters: HWP: Half Wave Plate; PBS: Polarising Beam Splitter; PM: Electro-optic Phase Modulator; AM: Electro-optic Amplitude Modulator; PR: Polariser; LO: Local Oscillator; M: Mirrors; PZT: Piezo Controlled Nano-positioner Stage; AMC100: Nano-positioner Controller; ODF: Optical Density Filter; BS: Beam Splitter; BHD: Balanced Homodyne Detector; MSO: Mixed Signal Oscilloscope; AWG: Arbitrary Waveform Generator.

signal and LO are transmitted through the free space over a single transmission line.

State Preparation: Random Voltage Generation by AWG

As discussed in Sec. 6.2, in GM-CVQKD protocol the random voltages are selected from the two identical Gaussian distributions. These distributions are generated by using MATLAB programming and are shown in Fig. 6.2 (a) and Fig. 6.2 (b). We obtain the Rayleigh distribution and uniform distribution from these Gaussian distributions by using the conversion relation given in Eq. 6.1. The random voltages given to AM are selected from the Rayleigh distribution and the random voltages fed to PM are selected from the uniform distribution, which is shown in Fig. 6.2 (c) and Fig. 6.2 (d). Both distributions are fed to the AWG. The AWG's signal is given to the amplifiers which in turn drive the AM and PM of Alice. The AM and PM are high-voltage devices with a

half-wave voltage of 260 V and 170 V. So, we use two cascaded amplifiers to achieve the high voltages.

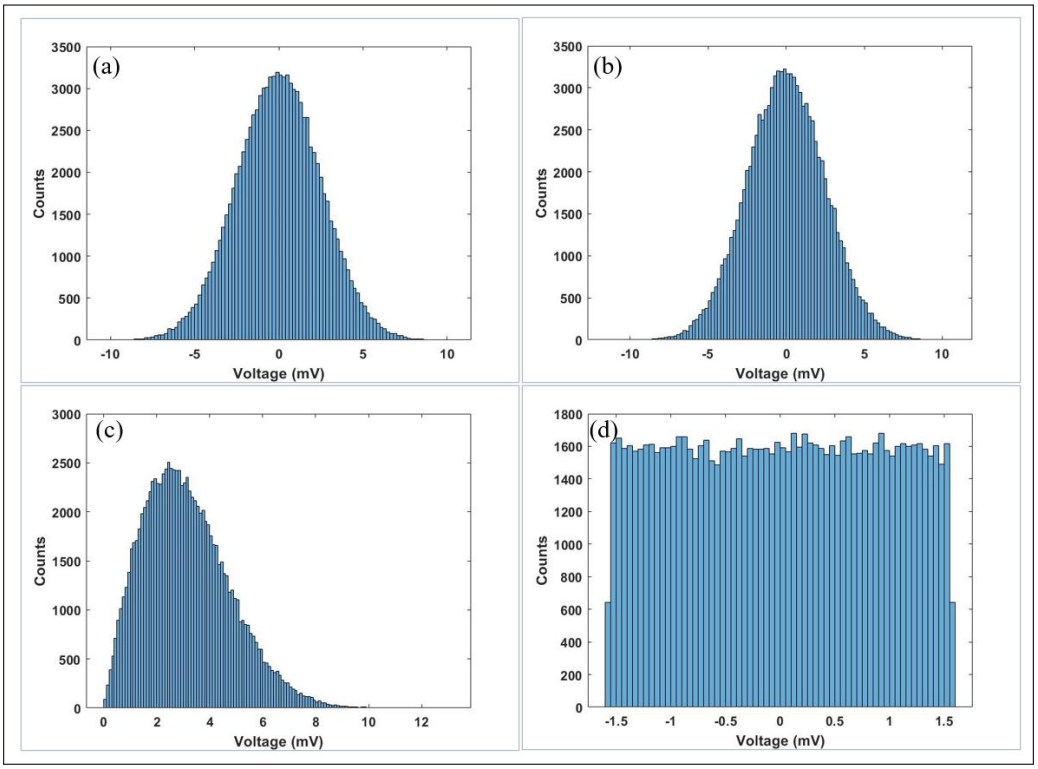

Figure 6.2: Distributions fed to the AM and PM of Alice. Figure (a) and Figure (b) represent the Gaussian distributions corresponding to the quadrature q and p generated using MATLAB programming. Figure (c) and Figure (d) are the Rayleigh and uniform distributions fed to the AWG which drives the AM and PM of Alice.

Quantum Channel

The encoded signal along with the LO is transmitted through the free space over a distance of 5 meters. The beam diameter increases with the propagation distance. The beam is de-magnified at the receiver side by using a lens combination (not shown in the Fig. 6.1) of 50 cm and 10 cm to obtain the original beam diameter which is 800 μm.

At **Bob's** end, a PBS4 is placed to separate the signal and LO. The transmitted arm is the LO arm and the reflected arm is the signal arm. The beam in the LO arm is incident on the PM2 followed by an HWP3. PM2 selects the q-quadrature and p-quadrature values corresponding to the phase values 0, and $\pi/2$. A delay line is kept in the LO arm to compensate for the delay introduced by AM placed in the signal arm of Alice. A mirror M in the signal arm is placed on a piezo controlled translation stage, PZT-stage (Attocube, ECSx3080) controlled by an AMC100 controller for a fine scan of the interferometer phase. The two beams, i.e., signal and LO interfere at the 50:50 BS, and homodyne detection is performed. The detection system includes a balanced homodyne detector, BHD (Thorlab's PDB435A, DC-350 MHz), which measures the subtracted photocurrent falling on the two detectors. A mixed signal oscilloscope, MSO (Tektronix 6-series), is used to record the output signal of BHD.

Data Acquisition

The amplitude and phase modulation at both Alice's and Bob's ends is performed at a rate of 1 MHz. The random voltage signals of 1 μs for the respective cases are generated using AWG. The voltage signals are fed to the AM and PM of Alice and Bob. A copy of the signal from AWG is given to the MSO for the record of the given voltages. The subtracted output photocurrent from BHD is saved in MSO. The recorded signals in the MSO are shown in Fig. 6.3. Channel-1 is the homodyne output of the balanced detector. Channel-2 and Channel-3 are the copy of random voltages fed to AM and PM of Alice. Channel-4 is the copy of the random voltage fed to the PM of Bob. In a single acquisition $2\text{x}10^5$ pulses are saved. Once sufficient data has been recorded, post-processing is performed.

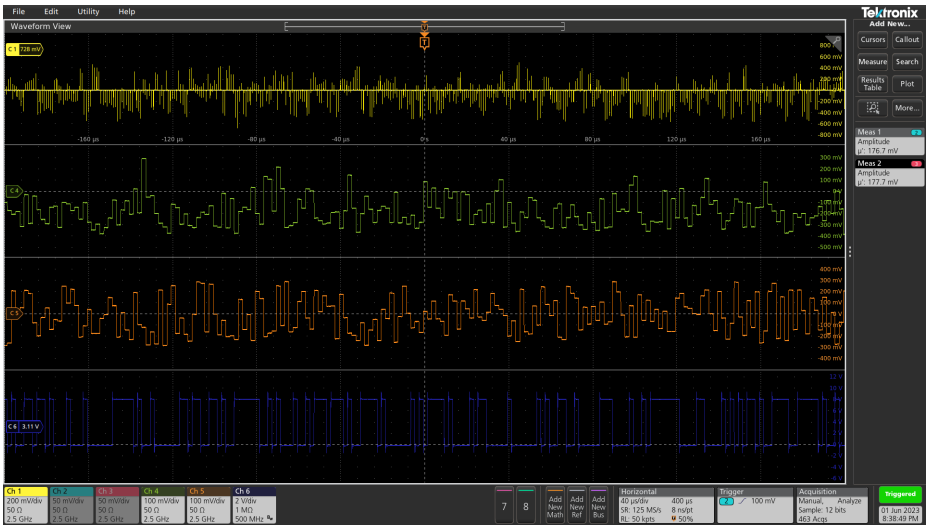

Figure 6.3: The voltage signals recorded in the oscilloscope. Channel-1 is the difference signal of the balanced detector. Channel-2 and Channel-3 are the copy of the random voltage signals fed to the AM and PM of Alice. Channel-4 is the random voltage signal fed to PM of Bob.

Post-processing

Once Alice and Bob exchange sufficient signals (key elements), they further do the post-processing of the data which includes the following steps.

Quadraure Extraction: The distributions fed for the amplitude and phase modulation of Alice are Rayleigh and uniform distributions. We do the intensity and phase modulation of the signal at a certain optical power. We retrieve the quadratures strike out q and p for Alice by using the relation mentioned in Eq. 6.1. Whereas, at Bob's end we get a series of pulses in terms of voltage signals. We integrate each pulse over its respective pulse duration. We use Python programming to perform the integration. These integrated values correspond to the quadrature value q or p depending on the basis selection of Bob. Now, Alice and Bob are at the same level, Alice having a pair of (q and p) and Bob with (q or p).

Sifting: Further, we then strike out sifting to generate the raw key. Alice and Bob use a classical authenticated channel to announce the basis. Bob will disclose on which basis he has done the measurement and Alice will keep the respective basis and discard the mismatched values. Both Alice and Bob are left with the correlated string of Gaussian data. We calculate the mutual information shared between Alice and Bob. Further, the processing of the data is under progress to assess the efficacy of this particular implementation to compare it with other implementations.

6.4 Results and Discussion

As discussed in the previous chapters, The initial step in the protocol execution is the measurement of shot noise and checking the clearance of the signal (shot noise to electronic noise ratio). We measured the electronic noise by blocking the signal and LO. The distribution of the measured electronic noise is shown in Fig. 6.4.

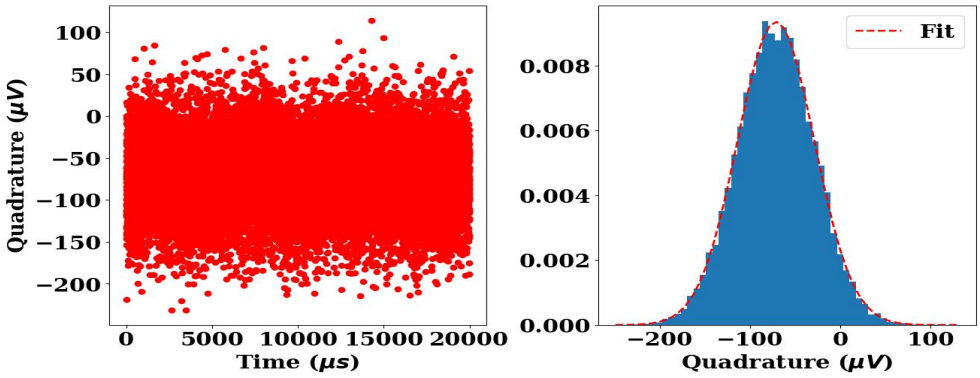

Figure 6.4: Electronic noise distribution. The left side shows the data points and the right side shows the distribution of the electronic noise.

We then measured the shot noise of the LO at a fixed power by blocking the signal arm. We measured the shot noise at LO power 274 μW at the receiver's end. To measure the shot noise, we recorded 10,000 pulses in a single acquisition and integrated

the individual pulse over the pulse width. The distribution for the integrated values at a fixed LO power is shown in Fig. 6.5.

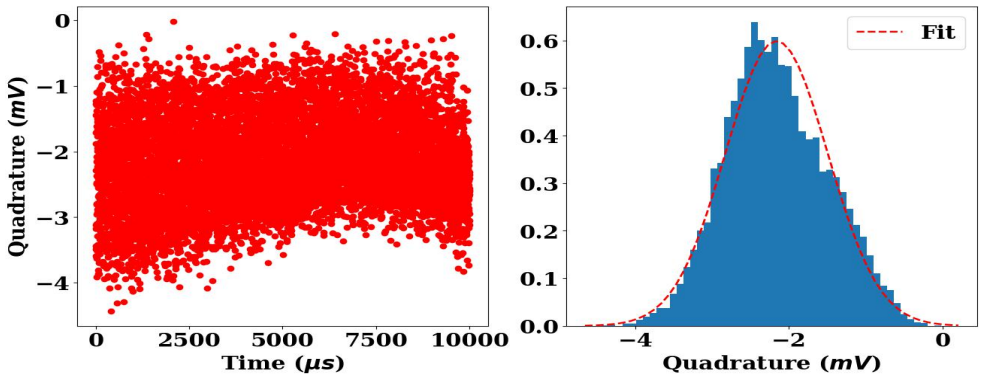

Figure 6.5: The distribution of the integrated quadrature values for shot noise measurement at fixed LO power. The left side shows the data points and the right side shows the distribution of the measured shot noise.

We calculated the voltage variance for the given LO power from the integrated values. We re-scaled the voltage variance to define the shot noise unit (SNU). We calculated the electronic noise in term of SNU and the values are given in Tab. 6.1. The electronic noise-to-shot noise (electronic-to-shot noise ratio) clearance is found to be 15 dB.

Paramters	Values
Shot noise unit (SNU)	1.069
Electronic noise (SNU)	0.04

Table 6.1: The table contains the values of shot noise unit (SNU) and electronic noise calculated from the experiment.

We proceed further with the implementation of GM-CVQKD. In Gaussian modulation, we take the assumption that the protocol works in asymptotic limits. We do not consider the finite size effect on the secure key rate. A further assumption is that collective attacks are optimal as we are working in an asymptotic regime. Further,

we consider that the excess noise due to the electronic noise does not contribute to Eve's information as in a trusted device scenario. Alice prepared the amplitude and phase-modulated coherent state and transmit it to Bob through a quantum channel. Bob performed balanced homodyne detection to retrieve the state back. Both Alice and Bob performed sifting and are left with the correlated Gaussian key elements. The probability distributions for Alice and Bob after performing the sifting process are shown in Fig. 6.6 and Fig. 6.7. From the Figures, we observed that Alice's distributions are more scattered compared to the distributions of Bob. This perhaps could be due to the modulation performed at Alice's end. The random pattern feed to the modulators repeats after a fixed time. We are further verifying the reasons for the scattering of Alice's Data.

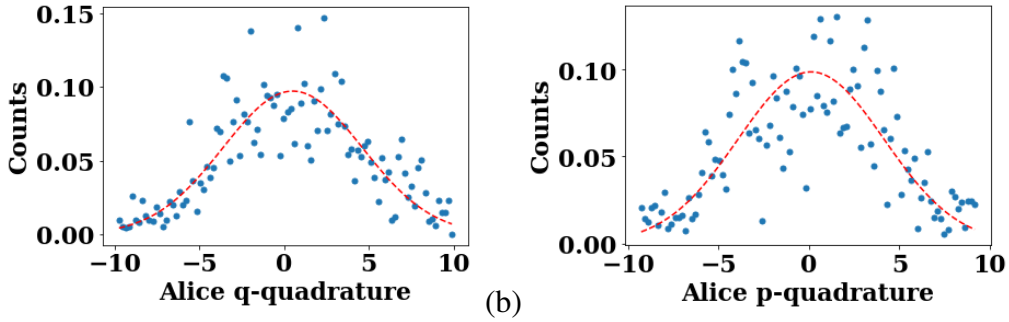

Figure 6.6: Probability distributions for Alice's quadrature values (a) q - quadrature, (b) p - quadrature.

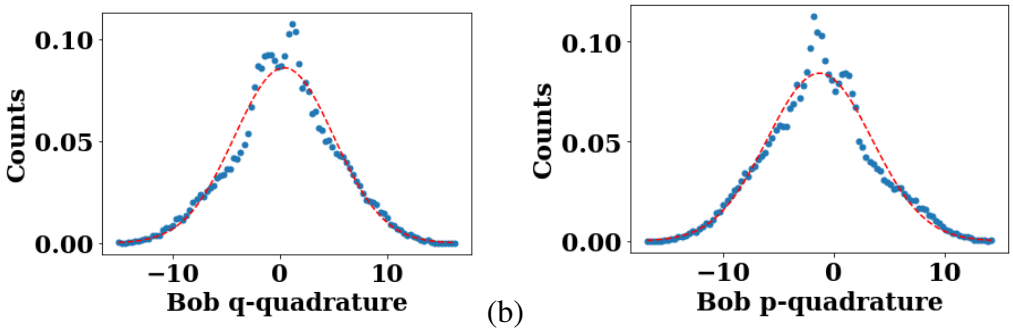

Figure 6.7: Probability distributions for Bob's quadrature values (a) q - quadrature, (b) p - quadrature.

We estimated the experimental parameters. The channel transmissivity is 95.23 % and the detection efficiency is 76 %. We calculated SNR and mutual information shared between Alice and Bob and the results are shown in Table 6.2. The excess noise

Paramters	Values
Signal processed (pulses)	$2x10^5$
Sifted key (pulses)	$2x10^5$
SNR	2.69
Mutual information (bits/pulse)	0.94

Table 6.2: Showing the experimental parameters including the SNR and mutual information obtained from the collected data for 200 milliseconds.

ξ is mainly assumed to be contributed due to the electronic noise only. The mutual information between Alice and Bob obtained from the experiment is **0.94 bits/pulse**. We are designing an algorithm for the reconciliation of Alice and Bob's Data. Further, post-processing of the data is under progress to compare the performance of this particular implementation with the other implementations. A few of the limitations of the described setup include instabilities due to the interferometer, limited resolution of Alice's modulation, and a limit on the LO power available for performing the detection. We are currently designing an improved setup to address these challenges. These studies would help in the field implementation of the protocol.

6.5 Conclusion

In summary, the free space GM-CVQKD was demonstrated successfully in the lab. The obtained results from the experimental studies were discussed. The detector shot noise, electronic noise, detection efficiency, delays etc. were carefully calibrated. The data were successfully transmitted and recorded. The mutual information was extracted from the experimental data. The processing of the data is under progress to assess the efficacy of this particular implementation to compare it to other imple-

mentations. The study of the protocol over free space would help in field tests over atmospheric channels and to check the feasibility of satellite communication.

Chapter 7

Atmospheric CVQKD

In the previous Chapters, we performed a demonstration of the discrete modulation and Gaussian modulation CVQKD in the laboratory. In this Chapter, we have attempted the atmospheric CVQKD to learn what issues will have to be addressed for a real-life application of quantum communication. Compared to fiber CVQKD, atmospheric link offers a possibility of broader geographical coverage and more flexible transmission [199–202]. However, many negative features of the atmospheric channel will reduce the achievable secure key rate, such as beam extinction and a variety of turbulence effects [203].

We carried out the field experiments during the monsoon season in the month of June. While performing the experiment over the atmospheric channel in heavily rainy and windy weather, several challenges are faced. The beam quality gets deteriorated after transmitting through free space. Due to the effect of the wind, the beam coupled to the detector in small proportion leading to coupling losses. Besides, the phase noise in the system is enhanced due to atmospheric disturbances [204]. Considering these

parameters into account, we extracted some results from the field experiments. Further studies in this direction are going on. The details of the field experiment are discussed in the upcoming sections.

7.1 State Preparation

In this section, we will study the state preparation for the discrete modulation (DM) and Gaussian modulation (GM) CVQKD. Alice encodes her quantum bit information in phase in case of DM-CVQKD (discussed in Chapter 5) and in both amplitude and phase in case of GM-CVQKD (discussed in Chapter 6).

State Preparation for Discrete Modulation

In case of DM-CVQKD, Alice does the phase modulation of the signal and transmits the signal and LO to Bob through a channel. Bob performs homodyne detection to retrieve the phase information. The acquisition system for the protocol is shown in Fig. 7.1. It consists of Alice's and Bob's phase modulators (PM). The random voltages are fed to the modulators using an arbitrary waveform generator (AWG). High voltage amplifiers (AMP) drive the modulators. A copy of the signal fed to modulators is also given to the oscilloscope that will give the time information of the signal. The modulation is performed at 1 MHz. The random voltages generated for Alice's and Bob's PM are converted to the phase values and are shown in Fig. 7.2.

State Preparation for Gaussian Modulation

In GM-CVQKD, Alice does both the amplitude and phase modulation of the signal. Whereas, Bob performs homodyne detection and requires only the phase modulator.

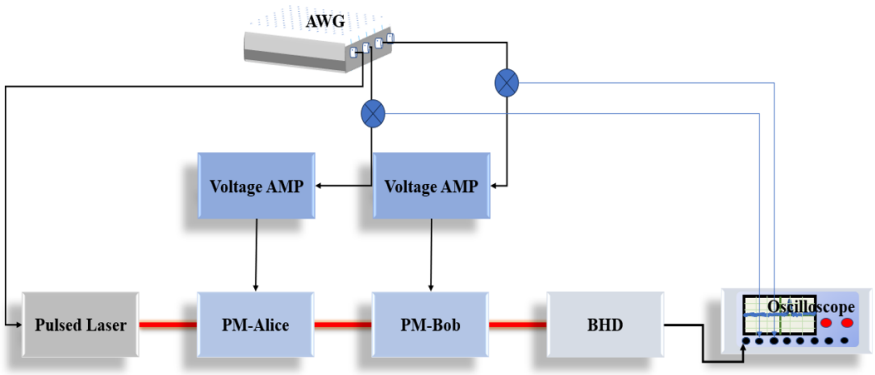

Figure 7.1: Acquisition system for DM-CVQKD; AWG: Arbitrary Waveform Generator; AMP: Voltage Amplifier; PM: Phase Modulator; BHD: Balanced Homodyne Detector.

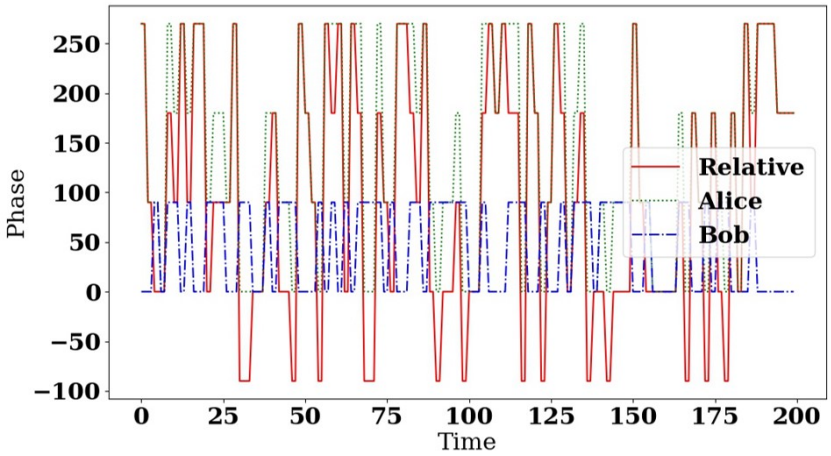

Figure 7.2: Random phase values obtained after converting the random voltages of Alice and Bob into phases.

The random voltages fed to Alice's amplitude and phase modulator are selected from the Rayleigh distribution (fed to AM) and the uniform distribution (fed to PM). The acquisition system for GM-CVQKD is shown in Fig. 7.3. The modulation is performed at 500 kHz. The random voltage signals generated at Alice's and Bob's end are shown in Fig. 7.4.

An overview of the data acquisition system used in the field is shown in Fig. 7.5.

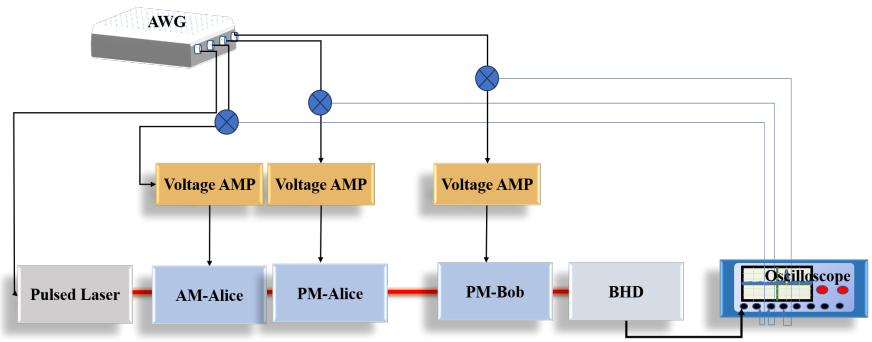

Figure 7.3: Data Acquisition system for GM-CVQKD; AWG: Arbitrary Waveform Generator; AMP: Voltage Amplifier; AM: Amplitude Modulator; PM: Phase Modulator; BHD: Balanced Homodyne Detector.

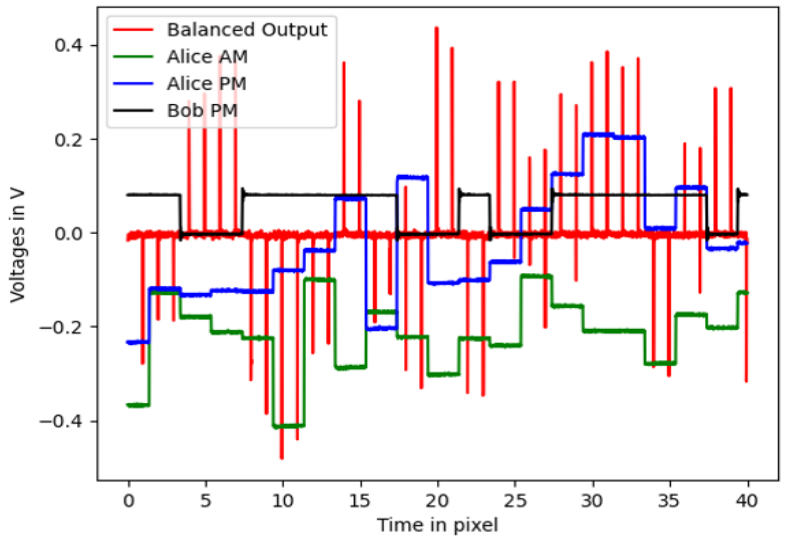

Figure 7.4: The recorded signals consisting of the random voltages generated at Alice's and Bob's end and the output signal of the balanced detector.

7.2 Transmission Through Channel

The encoded signal and the LO are transmitted to the atmosphere over free space. The beam diverges while transmitting over free space, and the beam size increases along with the propagation distance. To manage the actual beam size, we used launching and collecting optics in order to compensate for the divergence effect.

Figure 7.5: An illustration of the devices used during the field implementation for data acquisition for DM-CVQKD and GM-CVQKD.

Launching and Receiving Optics

The launching optics consists of a combination of two lenses with different focal lengths. The beam is expanded at the launching end to reduce the beam's divergence as the beam size is related to divergence by the relation $w_o = 1/\theta$. To expand the beam, the configuration of lenses is selected such that $f_2 > f_1$ and the beam size after the second lens is expanded.

The expanded beam is collected at receiving (Bob) end using another lens combination. The first lens at Bob's end is of a larger focal length, and the second lens is of a smaller focal length to reduce the beam size. After passing through both lenses, the beam is guided to Bob's detection setup. For very large distances, instead of a lens combination, one needs to go for the telescope due to the higher divergence of the beam.

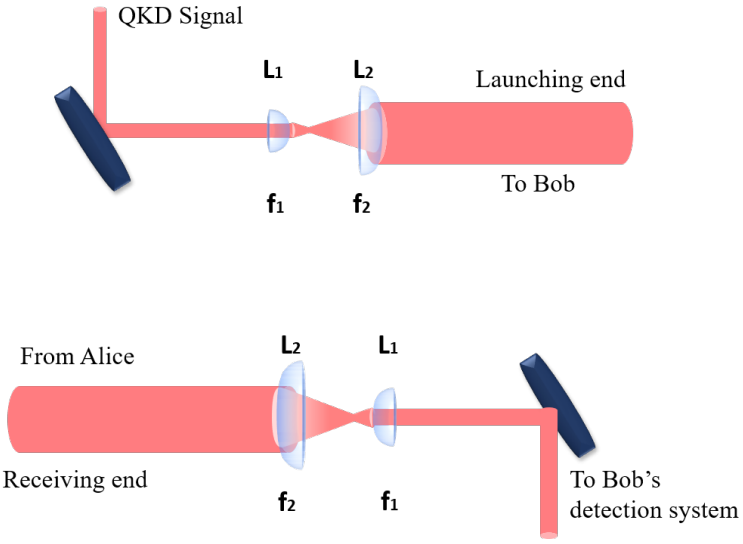

Figure 7.6: Schematic of launching and receiving optics. L_1 and L_2 are the lenses with focal length f_1 and f_2.

Beacon Laser

The signal used for QKD applications is a weak signal which can not be monitored properly during transmission in the atmosphere. A beacon beam is sent along with the signal. For this, we use a visible laser of strong intensity. Both the QKD signal and Beacon laser are aligned along the common path and sent to Bob over free space.

7.3 Detection

Bob received the transmitted signal multiplexed with the LO. He separates the signal and LO and performs the projective measurements on the LO beam to measure in either q-basis or p-basis. This is achieved by doing the random phase selection using the phase modulator on Bob's end which is shown in Fig. 7.1 for DM-CVQKD and Fig. 7.3 for GM-CVQKD. Bob records the data by using an oscilloscope for a certain acquisition window. Once sufficient data is collected, Alice and Bob further do the post-processing to obtain the secure key.

The procedure for post-processing for both DM-CVQKD and GM-CVQKD is discussed in Chapter 5 and Chapter 6.

7.4 Experimental Results from Field Study

We performed the field demonstration for DM-CVQKD and GM-CVQKD. The experimental setup for both configurations is embedded in a single setup and is shown in Fig. 7.7. The illustration of the field view is shown in Fig. 7.8 and Fig. 7.9. We

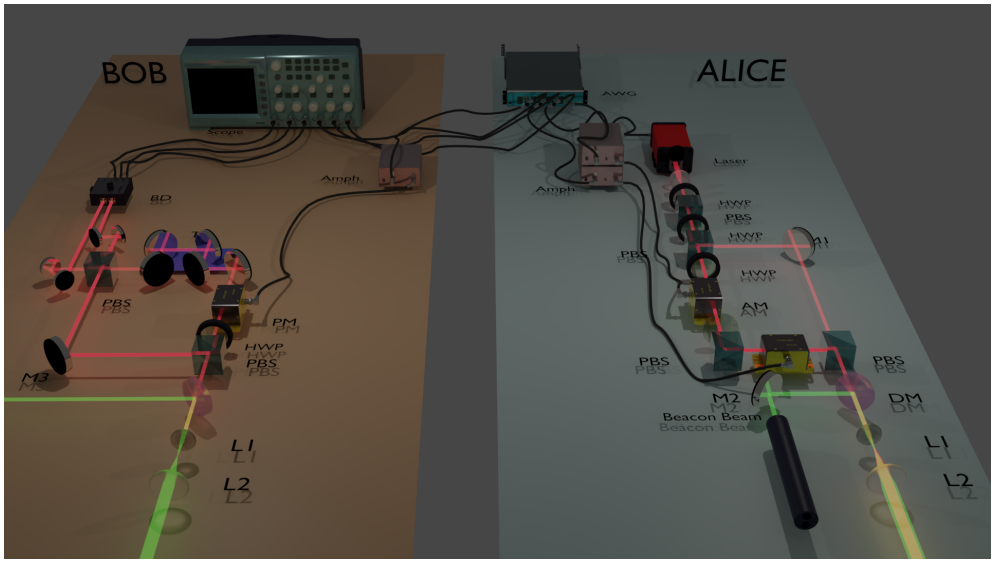

Figure 7.7: Experimental setup for CVQKD consisting of transmitter and receiver.

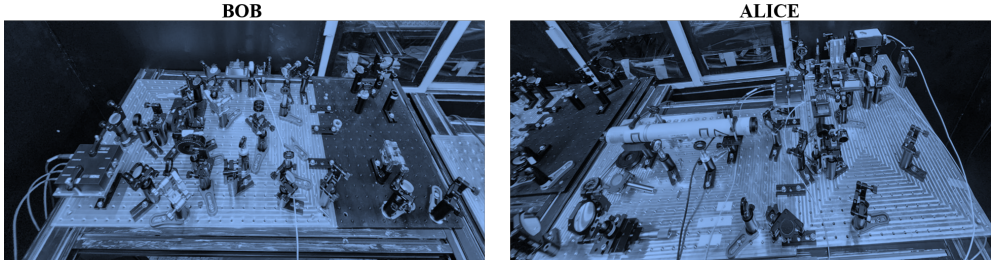

Figure 7.8: An illustration of the transmitter and receiver setup during field implementation.

performed 35 m CVQKD in the daytime on 9th June 2023, at PRL, Thaltej campus,

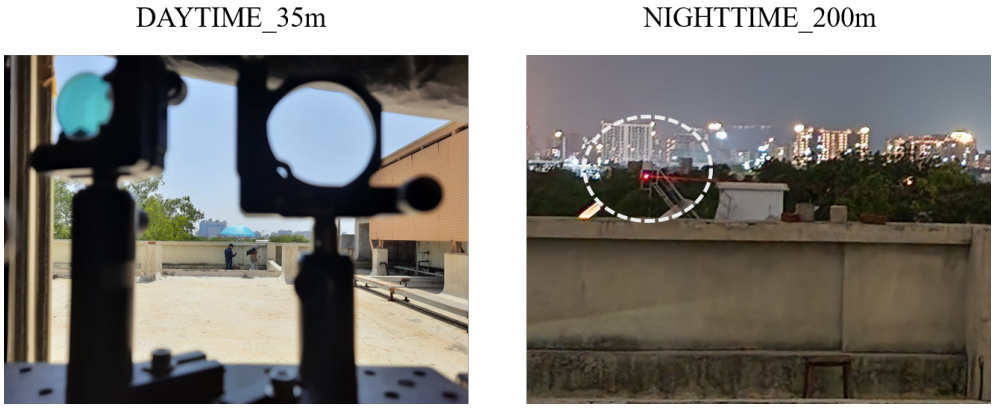

Figure 7.9: Daytime and nighttime view of the experiment performed over 35 m and 200 m in the field.

New building. We extracted the data for DM-CVQKD. The data plot for shot noise measurement is shown in Fig. 7.10. The probability distributions for the measured quadrature values of Bob's relative phases for different mean photon numbers of the signal are shown in Fig. 7.11. From Fig. 7.10, we can see, the data for shot noise mea-

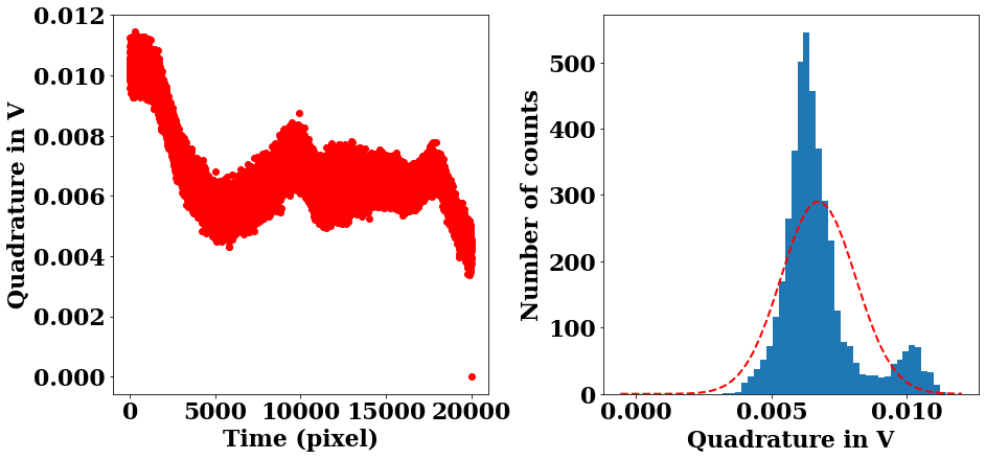

Figure 7.10: The plot of the shot noise data. The left side shows the plot of the integrated pulse values and the right side plots the probability of these integrated values at a fixed LO power of the receiver.

surement is highly noisy. This could be due to harsh weather conditions. The weather was very humid and windy due to the monsoon season. The probability distributions obtained for Bob's measurement shown in Fig. 7.11 overlap with each other for both

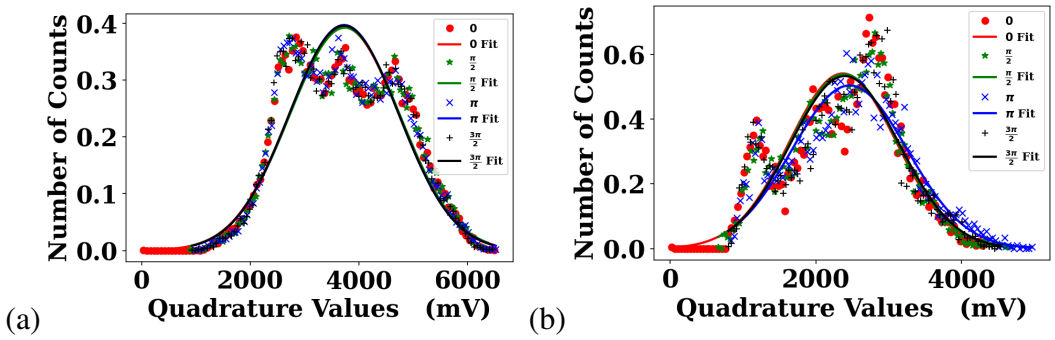

Figure 7.11: Probability distributions for Bob's quadrature values for four relative phases for different mean values of photons. (a) mean photon number is 11.2 and (b) mean photon number is 1.12.

cases. The error in data is quite high and no key rate is extracted. This is because of the reason that the phase noise in the system is enhanced due to atmospheric disturbances. To improve the performance of the protocol, we are working on the resolution of the various problems accounted for during the implementation. To compensate for the phase, we are working on the live monitoring of the data so that the phase shift can be corrected during the protocol execution itself.

We extracted the data for GM-CVQKD for 35 m on the same day during the evening time. The probability distributions obtained at Alice and Bob's end after the process of sifting are given in Fig. 7.12 and Fig. 7.13. From the graphs, we see that the correlation between Alice and Bob's data is weak. One of the possible reasons for this could be the atmospheric disturbances and the transmission losses over the atmospheric channel which was more than 50 %. The signal-to-noise ratio and the mutual information calculated between Alice and Bob have values $8.23\text{x}10^{-4}$ and $5.9\text{x}10^{-4}$ for 35 m GM-CVQKD.

The demonstration of 200 m CVQKD was carried out on 3rd July 2023 between the Astro building and the New building at Thaltej campus PRL. The atmospheric losses for 200 m were very high. For the transmitted power of 1 mW the received

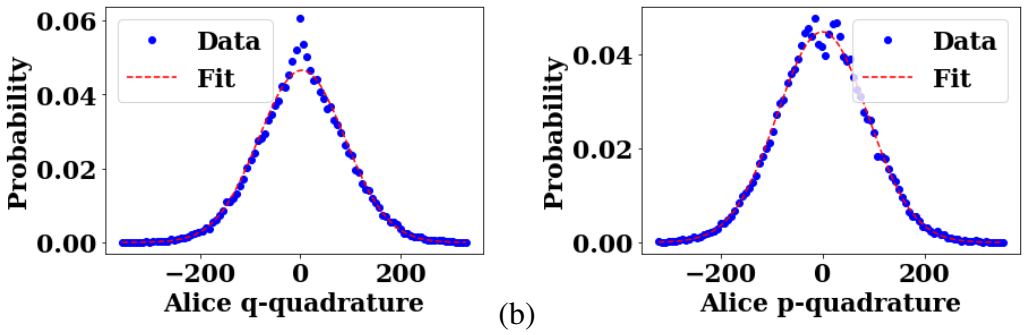

Figure 7.12: Probability distributions for Alice's quadrature values (a) q - quadrature, (b) p - quadrature.

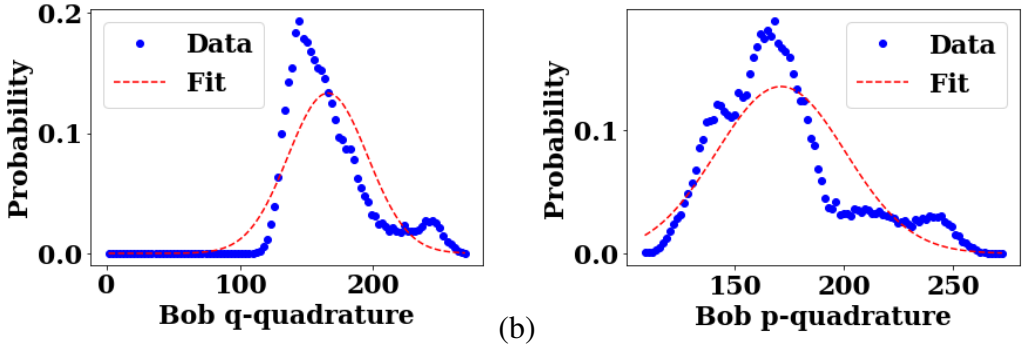

Figure 7.13: Probability distributions for Bob's quadrature values (a) q - quadrature, (b) p - quadrature.

power was just 50 μW. And after passing the aperture (used for mode cleaning), the power left was only 7-8 μW. This does not fulfill the requirement of the strong local oscillator. The power losses in the atmosphere could be due to high humidity present in the weather and high absorption losses or several other experimental parameters. To resolve the issues, we are doing further investigations in this direction. We will perform the demonstrations after the problems are being resolved.

7.5 Conclusion

The free atmospheric CVQKD was attempted to learn what issues will have to be addressed for a real-life application of quantum communication. The results are not

promising. This could be due to the harsh weather condition, humidity, monsoon season, or several other experimental parameters. The power losses were unexpectedly high during the propagation through the channel. We are trying to figure out the reasons for the losses. We are exploring the effects of atmospheric parameters affecting the key rate. Due to the monsoon season, we could not continue with the experiment. We will repeat the experiment to resolve the various issues faced during the implementation of the atmospheric CVQKD.

Chapter 8

Summary

The demand for secure communication has given massive popularity to quantum communication over the past few decades. The laws of Quantum Mechanics (QM) make it strong evidence of practical application in quantum cryptography thanks to the no-cloning theorem and Heisenberg's Uncertainty principle. These properties ensure the security of the information transfer between the communicating parties. QKD is the future of modern secure communication with the assistance of classical communication. QKD not only provides unconditional security [20, 21] but also helps detect eavesdroppers' presence in real-time. QKD works better than conventional cryptography as its security is based on the laws of QM rather than on the system's computational hardness [15, 23]. This point is crucial to prevent any attack or information leakage during communication.

The increase in demand for quantum communication has given origin to various classes of QKD protocols, including DVQKD and CVQKD. DVQKD protocols have been experimentally implemented over long distances, whereas CVQKD protocols

are proven as a faithful candidate for large metropolitan area networks due to their high compatibility with current classical infrastructure as well as the high key rate achievable.

In my thesis, we have implemented different classes of QKD protocols and have studied the impact of various parameters on the secure key rate. The thesis includes the demonstration of the two different classes of CVQKD based on discrete modulation (DM) and Gaussian modulation (GM).

Chapter 2 provided a theoretical understanding of the various steps involved in implementing QKD protocols. We begin with a discussion on the basic concepts of QM. We further build a theoretical understanding of quantising the electromagnetic field and describe its possible states. The idea of quantum entanglement and the generation and detection of photons is discussed in brief. The Chapter also deals with the basics of balanced homodyne detection and its mathematical understanding, which is a part of the detection system in CVQKD. The Chapter explains mutual information and secret key extraction from a practical aspect. In Chapter 3, we discuss the implementation of BB84 QKD protocol using heralded single-photons generated by the SPDC process. The various steps involved in the experimental implementation are discussed in detail with the results.

In Chapter 4, we performed the initial characterisation of the setup for CV applications to QKD, which deals with measuring the shot noise of the source. We accounted for various imperfections present in the detection system and provided a theoretical and experimental understanding. In Chapter 5, we demonstrated free space CVQKD using DM. For this demonstration, a simulation has been performed, which includes the effects of various parameters on the secure key rate extraction. A noise model has been proposed, and a trade-off between the mean photon number and QBER is ob-

tained. The key rate is evaluated for several distances, including transmittance and excess noise. These simulated results help in the verification of the experimental results. In Chapter 6, a free space demonstration of GM-CVQKD has been done in the lab. The protocol gives a much higher key rate and is one of the best possible candidates for the metropolitan area network. A complete characterisation of the setup is done in the lab, including amplitude and phase modulator characteristics. We discussed the obtained results from the experimental studies.

In Chapter 7, we performed the field demonstration of the DM-CVQKD and GM-CVQKD over an atmospheric channel. The free space field studies assist us in assessing the feasibility of CVQKD protocols for satellite-based applications and offering various advantages over fiber. We further discussed the experimental challenges faced in the field with some of the results.

Scope for Future Work

In my thesis, we have studied two different classes of QKD protocols, which include the study of DV and CV protocols. Both have their own experimental challenges and limitations. In SPDC-based DVQKD, the obtained key rate is relatively low but provides a more secure way compared to prepare and measure protocols implemented with weak laser pulses. In prepare and measure protocols, the key rate is high with compromised security due to sophisticated attacks possible due to the experimental imperfections. We need to look for protocols that include the advantages of both DV and CV protocols. The state preparation can be done using DV techniques, which is easier, whereas detection can be performed using homodyne detection, which is an efficient detection technique.

In Chapter 3, we study the various imperfections present in the balanced detection

for shot noise measurements. These imperfections could lead to security loopholes for CVQKD applications and affect the outcomes of the optical homodyne detection used to measure the quantum state of light. In addition, the imperfection in shot noise measurement could affect the quality of QRNGs based on shot noise measurement for pulsed laser. So, we can study in detail the effect of imperfections on the security of CVQKD and optical homodyne tomography. In Chapter 5, we demonstrated DM-CVQKD, and the field demonstration for the same is performed in Chapter 7. These protocols work well even at low SNR. There are various classes for DM-CVQKD protocols. One of the works in this direction could be to check the sustainability of various protocols over free space in an atmospheric channel at low SNR and compare their performances.

In Chapters 6 and 7, we performed the demonstration of the GM-CVQKD in a laboratory setting and in the field. There are numerous challenges faced during the field implementation of CVQKD. However, implementation of CVQKD at long distances is a challenging task and has various practical limitations to go beyond hundreds of kilometers [205]. Besides the imperfections of transmitter and receiver devices, the main physical limitations in long-distance CVQKD are path loss and environmental noise. To address these limitations and extend the secure distance of QKD, an alternative approach involves using satellite-based communication links [206, 207]. By deploying a network of satellites with corresponding ground stations, large terrestrial losses can be overcome [88, 208, 209], and excessive noise can be minimised, as the noisy portion of the free-space communication link is primarily limited to the first ten kilometers of the atmosphere. One of the global solutions contributing towards quantum cryptography network, and hence, quantum internet could be achieved by coupling the satellite-based QKD with a reliable quantum repeater (QR) infrastructure [210–212]. The use of noiseless linear amplifiers (NLA) and QR can help to increase the distance

over which CVQKD protocols can be performed. Hence, by exploring the potential integration of existing CVQKD proposals like GG02 with QRs and satellite technology, we hope to achieve substantial secret key rates over long distances [213, 214].

Furthermore, the motivation for my study is to check the practical applicability of the CVQKD protocols for satellite quantum communication and quantum networking [192, 215]. My further aim is to work in the direction of quantum networking and satellite quantum communication [216, 217].

Appendix A

Noise Model

Consider the field operator $\hat{a}_{\text{sig}}$ of the signal and $\hat{b}_{\text{env}}$ of the environment (Fig. 5.1). The signal is in a coherent state which is given by $|\alpha\rangle_{\text{sig}}$

The action of the beam splitter on the field operators are given by

$$\begin{pmatrix} \hat{a}'_{\text{sig}} \\ \hat{b}_{\text{out}} \end{pmatrix} = \begin{pmatrix} \sqrt{T} & \sqrt{1-T} \\ -\sqrt{1-T} & \sqrt{T} \end{pmatrix} \begin{pmatrix} \hat{a}_{\text{sig}} \\ \hat{b}_{\text{env}} \end{pmatrix}. \tag{A.1}$$

The mode represented by the field operator $\hat{a}_{\text{out}}$ is received by Bob, who performs a measurement on the corresponding quantum state. Since we are dealing with Gaussian states and the noise model represents a Gaussian transformation on the modes, we can utilize the elegant variance matrix formalism to understand the effect of the quantum channel on the state. The covariance matrix of a single-mode Gaussian state is given by

$$V_{ij} = \frac{1}{2}\left\langle \{\hat{x}_i, \hat{x}_j\} \right\rangle - \langle \hat{x}_i \rangle \langle \hat{x}_j \rangle, \tag{A.2}$$

where $\hat{\mathbf{x}} = [\hat{q}, \hat{p}]^{\text{T}}$ are the quadrature operators of the signal mode given by $\hat{q} = \frac{1}{2}(\hat{a}_{\text{sig}} +$

$\hat{a}^{\dagger}_{\text{sig}}$) and $\hat{p} = \dfrac{i}{2}(\hat{a}^{\dagger}_{\text{sig}} - \hat{a}_{\text{sig}})$, and $\{\hat{A},\hat{B}\} = \hat{A}\hat{B} + \hat{B}\hat{A}$ denotes the anti-commutator of operators $\hat{A}$ and $\hat{B}$. For the example of a coherent state the covariance matrix reduces to

$$V = \frac{1}{4}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{A.3}$$

Using Eq. ((A.1)), the quadrature operators of the output signal can be written as

$$\hat{q}'_{\text{sig}} = \sqrt{T}\,\hat{q}_{\text{sig}} + \sqrt{1-T}\,\hat{q}_{\text{env}} \quad \text{and} \tag{A.4}$$

$$\hat{p}'_{\text{sig}} = \sqrt{T}\,\hat{p}_{\text{sig}} + \sqrt{1-T}\,\hat{p}_{\text{env}}. \tag{A.5}$$

The combined covariance matrix of the signal and the environment after the action of the beam splitter is given by

$$\Sigma = \text{BS}\begin{pmatrix} \frac{1}{4}\text{I}_2 & 0_2 \\ 0_2 & N_0\text{I}_2 \end{pmatrix}\text{BS}^T, \tag{A.6}$$

where N_0 denotes the channel noise and the matrix BS is defined as

$$\text{BS} = \begin{pmatrix} \sqrt{T}\text{I}_2 & \sqrt{1-T}\text{I}_2 \\ -\sqrt{1-T}\text{I}_2 & \sqrt{T}\text{I}_2 \end{pmatrix}. \tag{A.7}$$

Evaluating the expression given in Eq. A.6, the covariance matrix of the singal reaching Bob is given by

$$V_{\text{Bob}} = \begin{pmatrix} T\dfrac{|\alpha|^2}{2} + \dfrac{1}{4} + \xi_{\text{ch}} & 0 \\ 0 & T\dfrac{|\alpha|^2}{2} + \dfrac{1}{4} + \xi_{\text{ch}} \end{pmatrix}, \tag{A.8}$$

where $N_0 = \dfrac{1}{4} + (\xi_{\text{ch}}/(1-T))$.

Bibliography

[1] S. Aaronson, *Quantum computing since Democritus* (Cambridge University Press, 2013).

[2] S. Singh, *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography* (Doubleday, USA, 1999), 1st ed.

[3] C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners* (Springer Publishing Company, Incorporated, 2009), 1st ed.

[4] D. R. Stinson, *Cryptography: theory and practice* (Chapman and Hall/CRC, 2005).

[5] D. Boneh and V. Shoup, *A graduate course in applied cryptography,* (2020).

[6] C. E. Shannon, *Communication theory of secrecy systems,* The Bell System Technical Journal **28**, 656–715 (1949).

[7] H. Feistel, W. Notz, and J. Smith, *Some cryptographic techniques for machine-to-machine data communications,* Proceedings of the IEEE **63**, 1545–1554 (1975).

[8] A. Biryukov and D. Khovratovich, *Related-key cryptanalysis of the full aes-192 and aes-256,* Cryptology ePrint Archive, Report 2009/317 (2009). https://ia.cr/2009/317.

[9] W. Diffie and M. Hellman, *New directions in cryptography,* IEEE Transactions on Information Theory **22**, 644–654 (1976).

[10] R. L. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems,* Commun. ACM **21**, 120–126 (1978).

[11] P. W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,* SIAM Journal on Computing **26**, 1484–1509 (1997).

[12] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Quantum cryptography,* Rev. Mod. Phys. **74**, 145–195 (2002).

[13] C.-Y. Lu, D. E. Browne, T. Yang, and J.-W. Pan, *Demonstration of a compiled version of shor's quantum factoring algorithm using photonic qubits,* Phys. Rev. Lett. **99**, 250504 (2007).

[14] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, *Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance,* Nature **414**, 883–887 (2001).

[15] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, USA, 2011), 10th ed.

[16] A. Calderbank, E. Rains, P. Shor, and N. Sloane, *Quantum error correction via codes over gf(4),* IEEE Transactions on Information Theory **44**, 1369–1387 (1998).

[17] S. Wiesner, *Conjugate coding,* ACM Sigact News **15**, 78–88 (1983).

[18] M. HAYASHI, *QUANTUM INFORMATION THEORY: Mathematical Foundation* (SPRINGER, 2018).

[19] C. Kollmitzer and M. Pivk, *Applied quantum cryptography*, vol. 797 (Springer, 2010).

[20] N. Lütkenhaus, *Estimates for practical quantum cryptography,* Physical Review A **59**, 3301 (1999).

[21] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, *Secure quantum key distribution with realistic devices,* Rev. Mod. Phys. **92**, 025002 (2020).

[22] A. Molina, T. Vidick, and J. Watrous, *Optimal counterfeiting attacks and generalizations for wiesner's quantum money,* in "Theory of Quantum Computation, Communication, and Cryptography," , K. Iwama, Y. Kawano, and M. Murao, eds. (Springer Berlin Heidelberg, Berlin, Heidelberg, 2013), pp. 45–64.

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

[24] M. Fox, *Quantum Optics An Introduction* (Oxford University Press, ISBN 0198566735, 2006).

[25] C. Gerry and P. Knight, *Introductory Quantum Optics* (Cambridge University Press, 2004).

[26] W. K. Wootters and W. H. Zurek, *A single quantum cannot be cloned,* Nature **299**, 802–803 (1982).

[27] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, *A proof of the security of quantum key distribution,* Journal of cryptology **19**, 381–439 (2006).

[28] V. Coffman, J. Kundu, and W. K. Wootters, *Distributed entanglement,* Phys. Rev. A **61**, 052306 (2000).

[29] Z.-Y. Jeff Ou, *Quantum Optics for Experimentalist* (World Scientific, 2017).

[30] G. Van Assche, *Quantum cryptography and secret-key distillation* (Cambridge University Press, 2006).

[31] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, *Experimental quantum cryptography,* Journal of cryptology **5**, 3–28 (1992).

[32] R. G.-P. Sanchez and N. J. Cerf, *Quantum information with optical continuous variables: from bell tests to key distribution,* (2007).

[33] T. F. Da Silva, G. B. Xavier, and J. P. Von Der Weid, *Real-time characterization of gated-mode single-photon detectors,* IEEE Journal of Quantum Electronics **47**, 1251–1256 (2011).

[34] A. Yoshizawa, R. Kaji, and H. Tsuchida, *Quantum efficiency evaluation method for gated-mode single-photon detector,* Electronics Letters **38**, 1468–1469 (2002).

[35] F. Raffaelli, G. Ferranti, D. H. Mahler, P. Sibson, J. E. Kennard, A. Santamato, G. Sinclair, D. Bonneau, M. G. Thompson, and J. C. F. Matthews, *A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers,* Quantum Science and Technology **3**, 025003 (2018).

[36] U. Leonhardt, *Measuring the Quantum State of Light* (Cambridge University Press, 1997).

[37] B. Qi, P. Lougovski, and B. P. Williams, *Characterizing photon number statistics using conjugate optical homodyne detection,* Optics Express **28**, 2276 (2020).

[38] H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M. Fejer, K. Inoue, and Y. Yamamoto, *Differential phase shift quantum key distribution experiment over 105 km fibre,* New Journal of Physics **7**, 232 (2005).

[39] C. H. Bennett, *Quantum cryptography using any two nonorthogonal states,* Phys. Rev. Lett. **68**, 3121–3124 (1992).

[40] I. Devetak and A. Winter, *Distillation of secret key and entanglement from quantum states,* Proceedings of the Royal Society A: Mathematical, Physical and engineering sciences **461**, 207–235 (2005).

[41] A. K. Ekert, *Quantum cryptography based on bell's theorem,* Phys. Rev. Lett. **67**, 661–663 (1991).

[42] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, *Quantum cryptography with entangled photons,* Physical review letters **84**, 4729 (2000).

[43] C. H. Bennett and G. Brassard, *Proceedings of the ieee international conference on computers, systems and signal processing,* (1984).

[44] S. Mishra, A. Biswas, S. Patil, P. Chandravanshi, V. Mongia, T. Sharma, A. Rani, S. Prabhakar, S. Ramachandran, and R. P. Singh, *Bbm92 quantum key distribution over a free space dusty channel of 200 meters,* Journal of Optics **24**, 074002 (2022).

[45] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, *Continuous-variable quantum key*

distribution with gaussian modulation-the theory of practical implementations, Advanced Quantum Technologies **1**, 1800011 (2018).

[46] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, *Gaussian quantum information,* Rev. Mod. Phys. **84**, 621–669 (2012).

[47] A. Leverrier and P. Grangier, *Continuous-variable quantum-key-distribution protocols with a non-gaussian modulation,* Phys. Rev. A **83**, 042312 (2011).

[48] T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, *Quantum cryptography using pulsed homodyne detection,* Physical Review A **68**, 042331 (2003).

[49] M. Sayat, B. Shajilal, S. P. Kish, S. M. Assad, P. K. Lam, N. Rattenbury, and J. Cater, *Satellite-to-ground discrete modulated continuous variable quantum key distribution: The m-psk and m-qam protocols in low earth orbit,* (2022).

[50] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Proposed experiment to test local hidden-variable theories,* Physical review letters **23**, 880 (1969).

[51] J. F. Clauser and M. A. Horne, *Experimental consequences of objective local theories,* Physical review D **10**, 526 (1974).

[52] J. S. Bell, *On the einstein podolsky rosen paradox,* Physics Physique Fizika **1**, 195 (1964).

[53] A. Aspect, J. Dalibard, and G. Roger, *Experimental test of bell's inequalities using time-varying analyzers,* Physical review letters **49**, 1804 (1982).

[54] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera,

Quantum privacy amplification and the security of quantum cryptography over noisy channels, Phys. Rev. Lett. **77**, 2818–2821 (1996).

[55] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, *Concentrating partial entanglement by local operations,* Phys. Rev. A **53**, 2046–2052 (1996).

[56] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, *Mixed-state entanglement and quantum error correction,* Phys. Rev. A **54**, 3824–3851 (1996).

[57] C. H. Bennett, *Quantum cryptography using any two nonorthogonal states,* Physical review letters **68**, 3121 (1992).

[58] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, *Unconditional quantum teleportation,* Science **282**, 706–709 (1998).

[59] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, *Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables,* Quantum Inf. Comput. **3**, 535–552 (2003).

[60] 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).

[61] F. Grosshans and P. Grangier, *Continuous variable quantum cryptography using coherent states,* Physical Review Letters **88**, 057902 (2002).

[62] S. Du, Z. Li, W. Liu, X. Wang, and Y. Li, *High-speed time-domain balanced homodyne detector for nanosecond optical field applications,* J. Opt. Soc. Am. B **35**, 481–486 (2018).

[63] H. Hansen, T. Aichele, C. Hettich, P. Lodahl, A. I. Lvovsky, J. Mlynek, and S. Schiller, *Ultrasensitive pulsed, balanced homodyne detector:â€fapplication to time-domain quantum measurements,* Opt. Lett. **26**, 1714–1716 (2001).

[64] Y. Pan, H. Wang, Y. Shao, Y. Pi, Y. Li, B. Liu, W. Huang, and B. Xu, *Experimental demonstration of high-rate discrete-modulated continuous-variable quantum key distribution system,* Opt. Lett. **47**, 3307–3310 (2022).

[65] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. Towery, and S. Ten, *High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres,* New Journal of Physics **11**, 075003 (2009).

[66] T. Wang, P. Huang, Y. Zhou, W. Liu, H. Ma, S. Wang, and G. Zeng, *High key rate continuous-variable quantum key distribution with a real local oscillator.* Optics express **26 3**, 2794–2806 (2018).

[67] D. Lin, D. Huang, P. Huang, J. Peng, and G. Zeng, *High performance reconciliation for continuous-variable quantum key distribution with ldpc code,* International Journal of Quantum Information **13**, 1550010 (2015).

[68] C. Zhou, X. Wang, Y. Zhang, Z. Zhang, S. Yu, and H. Guo, *Continuous-variable quantum key distribution with rateless reconciliation protocol,* Phys. Rev. Appl. **12**, 054013 (2019).

[69] S. Ren, R. Kumar, A. Wonfor, X. Tang, R. Penty, and I. White, *Noise and security analysis of trusted phase noise continuous variable quantum key distribution using a local local oscillator,* in "2019 IEEE 20th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)," (2019), pp. 1–5.

[70] H. Wang, Y. Pi, W. Huang, Y. Li, Y. Shao, J. Yang, J. Liu, C. Zhang, Y. Zhang, and B. Xu, *High-speed gaussian-modulated continuous-variable quantum key distribution with a local local oscillator based on pilot-tone-assisted phase compensation,* Optics Express **28**, 32882 (2020).

[71] R. Namiki and T. Hirano, *Practical limitation for continuous-variable quantum cryptography using coherent states,* Physical Review Letters **92**, 117901 (2004).

[72] R. Namiki and T. Hirano, *Efficient-phase-encoding protocols for continuous-variable quantum key distribution using coherent states and postselection,* Phys. Rev. A **74**, 032302 (2006).

[73] A. Leverrier, F. Grosshans, and P. Grangier, *Finite-size analysis of a continuous-variable quantum key distribution,* Physical Review A **81**, 062343 (2010).

[74] T. Hirano, T. Ichikawa, T. Matsubara, M. Ono, Y. Oguri, R. Namiki, K. Kasai, R. Matsumoto, and T. Tsurumaru, *Implementation of continuous-variable quantum key distribution with discrete modulation,* Quantum Science and Technology **2**, 024010 (2017).

[75] M. D. Reid, P. D. Drummond, W. P. Bowen, E. G. Cavalcanti, P. K. Lam, H. A. Bachor, U. L. Andersen, and G. Leuchs, *Colloquium: The einstein-podolsky-rosen paradox: From concepts to applications,* Rev. Mod. Phys. **81**, 1727–1751 (2009).

[76] T. C. Ralph, *Continuous variable quantum cryptography,* Phys. Rev. A **61**, 010303 (1999).

[77] D. Gottesman and J. Preskill, *Secure quantum key distribution using squeezed states,* Phys. Rev. A **63**, 022309 (2001).

[78] R. García-Patrón and N. J. Cerf, *Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution,* Phys. Rev. Lett. **97**, 190503 (2006).

[79] M. Navascués, F. Grosshans, and A. Acín, *Optimality of gaussian attacks in continuous-variable quantum cryptography,* Phys. Rev. Lett. **97**, 190502 (2006).

[80] F. Grosshans, *Collectiveattacks and unconditional security in continuous variable quantum keydistribution,* Phys. Rev. Lett. **94**, 020504 (2005).

[81] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, *Air-to-ground quantum communication,* Nature Photonics **7**, 382–386 (2013).

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

[83] H.-K. Lo and H. F. Chau, *Unconditional security of quantum key distribution over arbitrarily long distances,* Science **283**, 2050–2056 (1999).

[84] M. Koashi and J. Preskill, *Secure quantum key distribution with an uncharacterized source,* Phys. Rev. Lett. **90**, 057902 (2003).

[85] H.-K. Lo, M. Curty, and K. Tamaki, *Secure quantum key distribution,* Nature Photonics **8**, 595–604 (2014).

[86] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, M.-J. Li, H. Chen, H. Li, L. You, Z. Wang, X.-B. Wang,

Q. Zhang, and J.-W. Pan, *Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km,* Phys. Rev. Lett. **124**, 070501 (2020).

[87] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity *et al.*, *Experimental demonstration of free-space decoy-state quantum key distribution over 144 km,* Physical Review Letters **98**, 010504 (2007).

[88] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li *et al.*, *Satellite-to-ground quantum key distribution,* Nature **549**, 43–47 (2017).

[89] R. König, R. Renner, A. Bariska, and U. Maurer, *Small accessible quantum information does not imply security,* Phys. Rev. Lett. **98**, 140502 (2007).

[90] R. Renner and R. König, *Universally composable privacy amplification against quantum adversaries,* in "Theory of Cryptography," , J. Kilian, ed. (Springer Berlin Heidelberg, Berlin, Heidelberg, 2005), pp. 407–425.

[91] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, *Tight finite-key analysis for quantum cryptography,* Nature Communications **3**, 634 (2012).

[92] R. RENNER, *Security of quantum key distribution,* International Journal of Quantum Information **06**, 1–127 (2008).

[93] H. Inamori, N. Lütkenhaus, and D. Mayers, *Unconditional security of practical quantum key distribution,* The European Physical Journal D **41**, 599–627 (2007).

[94] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, *Security of quantum key distribution with imperfect devices,* in "International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.", (IEEE, 2004), p. 136.

[95] W.-Y. Hwang, *Quantum key distribution with high loss: toward global secure communication,* Physical Review Letters **91**, 057901 (2003).

[96] X.-B. Wang, *Beating the photon-number-splitting attack in practical quantum cryptography,* Physical review letters **94**, 230503 (2005).

[97] H.-K. Lo, X. Ma, and K. Chen, *Decoy state quantum key distribution,* Physical review letters **94**, 230504 (2005).

[98] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, *Overcoming the rate–distance limit of quantum key distribution without quantum repeaters,* Nature **557**, 400–403 (2018).

[99] E. Diamanti and A. Leverrier, *Distributing secret keys with quantum continuous variables: Principle, security and implementations,* Entropy **17**, 6072–6092 (2015).

[100] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, *Long-distance continuous-variable quantum key distribution with a gaussian modulation,* Physical Review A **84** (2011).

[101] 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).

[102] D. Huang, D. kai Lin, C. Wang, W. Liu, S. Fang, J. Peng, P. Huang, and G. Zeng, *Continuous-variable quantum key distribution with 1 mbps secure key rate.* Optics express **23 13**, 17511–9 (2015).

[103] D. J. Griffiths, *Introduction to Electrodynamics* (Cambridge University Press, 2017), 4th ed.

[104] G. S. Agarwal, *Quantum optics* (Cambridge University Press, 2012).

[105] G. S. Vernam, *Cipher printing telegraph systems: For secret wire and radio telegraphic communications,* Journal of the AIEE **45**, 109–115 (1926).

[106] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, *Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations,* Phys. Rev. Lett. **92**, 057901 (2004).

[107] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, *Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations,* Physical review letters **92**, 057901 (2004).

[108] S. E. Harris, M. K. Oshman, and R. L. Byer, *Observation of tunable optical parametric fluorescence,* Phys. Rev. Lett. **18**, 732–734 (1967).

[109] B. Mollow and R. Glauber, *Quantum theory of parametric amplification. i,* Physical Review **160**, 1076 (1967).

[110] S. Karan, S. Aarav, H. Bharadhwaj, L. Taneja, A. De, G. Kulkarni, N. Meher, and A. K. Jha, *Phase matching in β-barium borate crystals for spontaneous parametric down-conversion,* Journal of Optics **22**, 083501 (2020).

[111] H. Bachor and T. Ralph, *A Guide to Experiments in Quantum Optics* (John Wiley and Sons, Ltd., 2004).

[112] C. M. Natarajan, M. G. Tanner, and R. H. Hadfield, *Superconducting nanowire single-photon detectors: physics and applications,* Superconductor Science and Technology **25**, 063001 (2012).

[113] L. You, *Superconducting nanowire single-photon detectors for quantum information,* Nanophotonics **9**, 2673–2692 (2020).

[114] I. Charaev, D. A. Bandurin, A. T. Bollinger, I. Y. Phinney, I. Drozdov, M. Colangelo, B. A. Butters, T. Taniguchi, K. Watanabe, X. He, O. Medeiros, I. Božović, P. Jarillo-Herrero, and K. K. Berggren, *Single-photon detection using high-temperature superconductors,* Nature Nanotechnology **18**, 343–349 (2023).

[115] R. Kumar, E. Barrios, A. MacRae, E. Cairns, E. Huntington, and A. Lvovsky, *Versatile wideband balanced detector for quantum optical homodyne tomography,* Optics Communications **285**, 5259–5267 (2012).

[116] T. M. Cover and J. A. Thomas, *Elements of information theory second edition solutions to problems,* Internet Access pp. 19–20 (2006).

[117] S. M. Moser and P.-N. Chen, *A student's guide to coding and information theory* (Cambridge University Press, 2012).

[118] M. M. Wilde, *Quantum information theory* (Cambridge University Press, 2013).

[119] C. Bennett, *G. brassard 'quantum cryptography: Public key distribution and coin tossing',* in "Proceedings of IEEE International Conference on Computers, Systems & Signal Processing, Bangalore," (1984), pp. 175–179.

[120] Ekert, *Quantum cryptography based on Bell's theorem.* Physical review letters **67 6**, 661–663 (1991).

[121] C. H. Bennett, G. Brassard, and N. D. Mermin, *Quantum cryptography without Bell's theorem,* Physical Review Letters **68**, 557–559 (1992).

[122] K. Inoue, E. Waks, and Y. Yamamoto, *Differential Phase Shift Quantum Key Distribution,* Physical Review Letters **89**, 037902 (2002).

[123] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, *Fast and simple one-way quantum key distribution,* Applied Physics Letters **87**, 1–3 (2005).

[124] H.-K. Lo and H. F. Chau, *Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances,* Science **283**, 2050–2056 (1999).

[125] P. W. Shor and J. Preskill, *Simple Proof of Security of the BB84 Quantum Key Distribution Protocol,* Physical Review Letters **85**, 441–444 (2000).

[126] D. Gottesman, Hoi-Kwong Lo, N. Lutkenhaus, and J. Preskill, *Security of quantum key distribution with imperfect devices,* in "International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.", (IEEE, 2004), pp. 135–135.

[127] B. Huttner and A. K. Ekert, *Information gain in quantum eavesdropping,* Journal of Modern Optics **41**, 2455–2466 (1994).

[128] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, *Limitations on Practical Quantum Cryptography,* Physical Review Letters **85**, 1330–1333 (2000).

[129] V. Makarov * and D. R. Hjelme, *Faked states attack on quantum cryptosystems,* Journal of Modern Optics **52**, 691–705 (2005).

[130] H.-K. Lo, M. Curty, and B. Qi, *Measurement-device-independent quantum key distribution,* Phys. Rev. Lett. **108**, 130503 (2012).

[131] M. Schiavon, G. Vallone, F. Ticozzi, and P. Villoresi, *Heralded single-photon sources for quantum-key-distribution applications,* Physical Review A **93** (2016).

[132] F. Steinlechner, P. Trojek, M. Jofre, H. Weier, D. Perez, T. Jennewein, R. Ursin, J. Rarity, M. W. Mitchell, J. P. Torres, H. Weinfurter, and V. Pruneri, *A high-*

brightness source of polarization-entangled photons optimized for applications in free space, Optics Express **20**, 9640 (2012).

[133] N. Lal, A. Banerji, A. K. Biswas, A. Anwar, and R. Singh, *Single photon sources with different spatial modes,* arXiv: Quantum Physics (2019).

[134] A. Biswas, A. Banerji, P. Chandravanshi, R. Kumar, and R. P. Singh, *Experimental side channel analysis of bb84 qkd source,* IEEE Journal of Quantum Electronics **57**, 1–7 (2021).

[135] V. Mannalatha, S. Mishra, and A. Pathak, *A comprehensive review of quantum random number generators: concepts, classification and the origin of randomness,* Quantum Information Processing **22** (2023).

[136] T. Gehring, C. Lupo, A. Kordts, D. S. Nikolic, N. Jain, T. Rydberg, T. B. Pedersen, S. Pirandola, and U. L. Andersen, *Homodyne-based quantum random number generator at 2.9 gbps secure against quantum side-information,* Nature Communications **12** (2021).

[137] A. Shokrollahi, *Ldpc codes: An introduction,* in "Coding, cryptography and combinatorics," (Springer, 2004), pp. 85–110.

[138] M. Tomlinson, C. J. Tjhai, M. A. Ambroze, M. Ahmed, and M. Jibril, *Error-Correction Coding and Decoding: Bounds, Codes, Decoders, Analysis and Applications* (Springer Nature, 2017).

[139] R. W. Hamming, *Error detecting and error correcting codes,* The Bell System Technical Journal **29**, 147–160 (1950).

[140] S. Roman, *Coding and Information Theory* (Springer-Verlag, Berlin, Heidelberg, 1992).

[141] D. J. MacKay and D. J. Mac Kay, *Information theory, inference and learning algorithms* (Cambridge university press, 2003).

[142] C. H. Bennett, G. Brassard, and J.-M. Robert, *Privacy amplification by public discussion,* SIAM journal on Computing **17**, 210–229 (1988).

[143] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, *Generalized privacy amplification,* IEEE Transactions on Information theory **41**, 1915–1923 (1995).

[144] M. Stewart, *A superfast toeplitz solver with improved numerical stability,* SIAM journal on matrix analysis and applications **25**, 669–693 (2003).

[145] P. Shor and J. Preskill, *Simple proof of security of the bb84 quantum key distribution protocol,* Physical review letters **85**, 441—444 (2000).

[146] M. Sasaki, *Quantum key distribution and its applications,* IEEE Security & Privacy **16**, 42–48 (2018).

[147] Y. Zhang, Y. Huang, Z. Chen, Z. Li, S. Yu, and H. Guo, *One-time shot-noise unit calibration method for continuous-variable quantum key distribution,* Physical Review Applied **13**, 024058 (2020).

[148] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, *Long-distance continuous-variable quantum key distribution over 202.81 km of fiber,* Physical Review Letters **125**, 010502 (2020).

[149] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, *Experimental demonstration of continuous-variable quantum key distribution over 80 km of standard telecom fiber,* in "2013 Conference on Lasers & Electro-Optics Europe & International Quantum Electronics Conference CLEO EUROPE/IQEC," (2013), pp. 1–1.

[150] J. Lodewyck, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, *Controlling excess noise in fiber-optics continuous-variable quantum key distribution,* Physical Review A **72**, 050303 (2005).

[151] D. Huang, P. Huang, D. kai Lin, and G. Zeng, *Long-distance continuous-variable quantum key distribution by controlling excess noise,* Scientific Reports **6** (2016).

[152] G. L. Abbas, V. W. S. Chan, and T. K. Yee, *Local-oscillator excess-noise suppression for homodyne and heterodyne detection.* Optics letters **8 8**, 419–21 (1983).

[153] S. Kunz-Jacques and P. Jouguet, *Robust shot-noise measurement for continuous-variable quantum key distribution,* Physical Review A **91**, 022307 (2015).

[154] X. Zhang, Y. Zhang, Z. Li, S. Yu, and H. Guo, *1.2-ghz balanced homodyne detector for continuous-variable quantum information technology,* IEEE Photonics Journal **10**, 1–10 (2018).

[155] H. Duan, F. Jian, W. Chao, H. Peng, and Z. Guihua, *A 300-mhz bandwidth balanced homodyne detector for continuous variable quantum key distribution,* Chinese Physics Letters **30**, 114209–114209 (2013).

[156] A. Margarida, P. Daniel, F. Margarida, P. Armando, and N. A. N. Silva, *Impact of imperfect homodyne detection on measurements of vacuum states shot noise.* Optical and Quantum Electronics **52**, 503 (2020).

[157] H. Yuen and V. Chan, *Noise in homodyne and heterodyne detection,* Optics Letters **8**, 177–179 (1983).

[158] B. L. Schumaker, *Noise in homodyne detection.* Optics letters **9 5**, 189–91 (1984).

[159] J. Appel, D. Hoffman, E. Figueroa, and A. I. Lvovsky, *Electronic noise in optical homodyne tomography,* Phys. Rev. A **75**, 035802 (2007).

[160] A. Zavatta, M. Bellini, P. L. Ramazza, F. Marin, and F. T. Arecchi, *Time-domain analysis of quantum states of light: noise characterization and homodyne tomography,* Journal of The Optical Society of America B-optical Physics **19**, 1189–1194 (2002).

[161] M. Cooper, C. Söller, and B. J. Smith, *High-stability time-domain balanced homodyne detector for ultrafast optical pulse applications,* in "2012 Conference on Lasers and Electro-Optics (CLEO)," (2012), pp. 1–2.

[162] M. Esposito, *Design and experimental realization of a pulsed homodyne detector for optical quantum states characterization,* Ph.D. thesis, Dipartimento di Fisica, Universita' degli Studi di Trieste, Via Valerio (2016).

[163] Y. Guo, X. Fang, H. Zhang, T. Zhao, M. Virte, and X. Guo, *Chaotic time-delay signature suppression using quantum noise,* Optics Letters **46**, 4888 (2021).

[164] P. W. Shor, *Algorithms for quantum computation: discrete logarithms and factoring,* in "Proceedings 35th annual symposium on foundations of computer science," (Ieee, 1994), pp. 124–134.

[165] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Quantum cryptography,* Reviews of modern physics **74**, 145 (2002).

[166] D. Mayers, *Unconditional security in quantum cryptography,* Journal of the ACM (JACM) **48**, 351–406 (2001).

[167] J. Yin, Y. Cao, Y.-H. Li, J.-G. Ren, S.-K. Liao, L. Zhang, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, M. Li, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, *Satellite-to-ground entanglement-based quantum key distribution,* Physical Review Letters **119**, 200501 (2017).

[168] G. Ribordy, J. Brendel, J.-D. Gautier, N. Gisin, and H. Zbinden, *Long-distance entanglement-based quantum key distribution,* Physical Review A **63**, 012309 (2000).

[169] S.-K. Liao, J. Lin, J.-G. Ren, W.-Y. Liu, J. Qiang, J. Yin, Y. Li, Q. Shen, L. Zhang, X.-F. Liang, H.-L. Yong, F.-Z. Li, Y.-Y. Yin, Y. Cao, W.-Q. Cai, W.-Z. Zhang, J.-J. Jia, J.-C. Wu, X.-W. Chen, S.-C. Zhang, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, L. Ma, L. Li, G.-S. Pan, Q. Zhang, Y.-A. Chen, C.-Y. Lu, N.-L. Liu, X. Ma, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, *Space-to-ground quantum key distribution using a small-sized payload on tiangong-2 space lab,* Chinese Physics Letters **34**, 090302 (2017).

[170] R. Ursin, T. Jennewein, J. Kofler, J. M. Perdigues, L. Cacciapuoti, C. J. de Matos, M. Aspelmeyer, A. Valencia, T. Scheidl, A. Acin *et al.*, *Space-quest, experiments with quantum entanglement in space,* Europhysics News **40**, 26–29 (2009).

[171] J. Yin, Y.-H. Li, S.-K. Liao, M. Yang, Y. Cao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, S.-L. Li *et al.*, *Entanglement-based secure quantum cryptography over 1,120 kilometres,* Nature **582**, 501–505 (2020).

[172] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, *Secure quantum key distribution with realistic devices,* Reviews of Modern Physics **92** (2020).

[173] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, *Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations,* Advanced Quantum Technologies **1**, 1800011 (2018).

[174] T.C.Ralph, *Continuous variable quantum cryptography,* (1999).

[175] S. Pirandola, *Composable security for continuous variable quantum key distribution: Trust levels and practical key rates in wired and wireless networks,* Physical Review Research **3**, 043014 (2021).

[176] A. Leverrier and P. Grangier, *Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation,* Phys. Rev. Lett. **102**, 180504 (2009).

[177] B. Schrenk, F. Laudenbach, C.-H. F. Fung, C. Pacher, A. Poppe, R. Lieger, D. Hillerkuss, E. Querasser, G. Humer, M. Hentschel, M. Peev, and H. Hübel, *High-rate continuous-variables quantum key distribution with piloted-disciplined local oscillator,* 2017 European Conference on Optical Communication (ECOC) pp. 1–3 (2017).

[178] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, *Asymptotic security of continuous-variable quantum key distribution with a discrete modulation,* Phys. Rev. X **9**, 021059 (2019).

[179] R. Namiki and T. Hirano, *Security of quantum cryptography using balanced homodyne detection,* Physical Review A **67**, 022308 (2003).

[180] M. Sayat, B. Shajilal, S. P. Kish, S. M. Assad, P. K. Lam, N. Rattenbury, and J. Cater, *Satellite-to-ground discrete modulated continuous variable quantum key distribution: The m-psk and m-qam protocols in low earth orbit,* (2022).

[181] A. Denys, P. Brown, and A. Leverrier, *Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation,* Quantum **5**, 540 (2021).

[182] D. Huang, D. Lin, C. Wang, W. Liu, S. Fang, J. Peng, P. Huang, and G. Zeng, *Continuous-variable quantum key distribution with 1 mbps secure key rate,* Opt. Express **23**, 17511–17519 (2015).

[183] Y. Zheng, H. Shi, W. Pan, Q. Wang, and J. Mao, *Quantum hacking on an integrated continuous-variable quantum key distribution system via power analysis,* Entropy **23** (2021).

[184] X.-C. Ma, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, *Local oscillator fluctuation opens a loophole for eve in practical continuous-variable quantum-key-distribution systems,* Phys. Rev. A **88**, 022339 (2013).

[185] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, *Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution,* Physical Review A **87**, 062313 (2013).

[186] S. Ren, S. Yang, A. Wonfor, I. White, and R. Penty, *Demonstration of high-speed and low-complexity continuous variable quantum key distribution system with local local oscillator,* Scientific Reports **11** (2021).

[187] H. Wang, Y. Pi, W. Huang, Y. Li, Y. Shao, J. Yang, J. Liu, C. Zhang, Y. Zhang, and B. Xu, *High-speed gaussian-modulated continuous-variable quantum key distribution with a local local oscillator based on pilot-tone-assisted phase compensation,* Opt. Express **28**, 32882–32893 (2020).

[188] Y. Pi, H. Wang, Y. Pan, Y. Shao, Y. Li, J. Yang, Y. Zhang, W. Huang, and

B. Xu, *Sub-mbps key-rate continuous-variable quantum key distribution with local local oscillator over 100-km fiber,* Opt. Lett. **48**, 1766–1769 (2023).

[189] D. Dequal, L. T. Vidarte, V. R. Rodriguez, G. Vallone, P. Villoresi, A. Leverrier, and E. Diamanti, *Feasibility of satellite-to-ground continuous-variable quantum key distribution,* npj Quantum Information **7**, 1–10 (2020).

[190] S. Pirandola, *Satellite quantum communications: Fundamental bounds and practical security,* Physical Review Research **3**, 023130 (2021).

[191] D. Dequal, L. Trigo Vidarte, V. Roman Rodriguez, G. Vallone, P. Villoresi, A. Leverrier, and E. Diamanti, *Feasibility of satellite-to-ground continuous-variable quantum key distribution,* npj Quantum Information **7**, 3 (2021).

[192] L. de Forges de Parny, O. Alibart, J. Debaud, S. Gressani, A. Lagarrigue, A. Martin, A. Metrat, M. Schiavon, T. Troisi, E. Diamanti, P. Gélard, E. Kerstel, S. Tanzilli, and M. V. D. Bossche, *Satellite-based quantum information networks: use cases, architecture, and roadmap,* Communications Physics **6** (2023).

[193] G. Moody, V. J. Sorger, D. J. Blumenthal, P. W. Juodawlkis, W. Loh, C. Sorace-Agaskar, A. E. Jones, K. C. Balram, J. C. F. Matthews, A. Laing, M. Davanco, L. Chang, J. E. Bowers, N. Quack, C. Galland, I. Aharonovich, M. A. Wolff, C. Schuck, N. Sinclair, M. Lončar, T. Komljenovic, D. Weld, S. Mookherjea, S. Buckley, M. Radulaski, S. Reitzenstein, B. Pingault, B. Machielse, D. Mukhopadhyay, A. Akimov, A. Zheltikov, G. S. Agarwal, K. Srinivasan, J. Lu, H. X. Tang, W. Jiang, T. P. McKenna, A. H. Safavi-Naeini, S. Steinhauer, A. W. Elshaari, V. Zwiller, P. S. Davids, N. Martinez, M. Gehl, J. Chiaverini, K. K. Mehta, J. Romero, N. B. Lingaraju, A. M. Weiner, D. Peace, R. Cernansky, M. Lobino, E. Diamanti, L. T. Vidarte, and R. M. Camacho, *2022*

roadmap on integrated quantum photonics, Journal of Physics: Photonics **4**, 012501 (2022).

[194] N. Hosseinidehaj, A. M. Lance, T. Symul, N. Walk, and T. C. Ralph, *Finite-size effects in continuous-variable quantum key distribution with gaussian postselection,* Phys. Rev. A **101**, 052335 (2020).

[195] T. Matsuura, K. Maeda, T. Sasaki, and M. Koashi, *Finite-size security of continuous-variable quantum key distribution with digital signal processing,* Nature Communications **12** (2020).

[196] Y. Zheng, P. Huang, A. Huang, J. Peng, and G. Zeng, *Practical security of continuous-variable quantum key distribution with reduced optical attenuation,* Phys. Rev. A **100**, 012313 (2019).

[197] Y. Zheng, P. Huang, J. Peng, Y. Zhu, and G. Zeng, *Performance analysis of practical continuous-variable quantum key distribution systems with weak randomness,* Journal of Physics B: Atomic, Molecular and Optical Physics **53**, 095501 (2020).

[198] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. Braunstein, S. Lloyd, T. Gehring, C. Jacobsen, and U. Andersen, *High-rate measurement-device-independent quantum cryptography,* Nature Photonics **9**, 397–402 (2015).

[199] M. Li, T. Wang, J. Han, Z. Yu, M. Cvijetic, H. Ye, and Y. Liu, *Free space continuous-variable quantum key distribution with practical links,* J. Opt. Soc. Am. B **37**, 3690–3697 (2020).

[200] S.-Y. Shen, M.-W. Dai, X.-T. Zheng, Q.-Y. Sun, G.-C. Guo, and Z.-F. Han, *Free-space continuous-variable quantum key distribution of unidimensional gaussian*

modulation using polarized coherent states in an urban environment, Phys. Rev. A **100**, 012325 (2019).

[201] B. Heim, C. Peuntinger, N. Killoran, I. Khan, C. Wittmann, C. Marquardt, and G. Leuchs, *Atmospheric continuous-variable quantum communication,* New Journal of Physics **16**, 113018 (2014).

[202] D. Elser, T. Bartley, B. Heim, C. Wittmann, D. Sych, and G. Leuchs, *Feasibility of free space quantum key distribution with coherent polarization states,* New Journal of Physics **11**, 045014 (2009).

[203] S. Wang, P. Huang, T. Wang, and G. Zeng, *Atmospheric effects on continuous-variable quantum key distribution,* New Journal of Physics **20**, 083037 (2018).

[204] S. Wang, P. Huang, M. Liu, T. Wang, P. Wang, and G. Zeng, *Phase compensation for free-space continuous-variable quantum key distribution,* Opt. Express **28**, 10737–10745 (2020).

[205] 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).

[206] C. Bonato, A. Tomaello, V. D. Deppo, G. Naletto, and P. Villoresi, *Feasibility of satellite quantum key distribution,* New Journal of Physics **11**, 045017 (2009).

[207] J.-P. Bourgoin, E. Meyer-Scott, B. L. Higgins, B. Helou, C. Erven, H. Hübel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, and T. Jennewein, *A comprehensive design and performance analysis of low earth orbit satellite quantum communication,* New Journal of Physics **15**, 023006 (2013).

[208] J.-G. Ren, P. Xu, H.-L. Yong, L. Zhang, S.-K. Liao, J. Yin, W.-Y. Liu, W.-Q. Cai, M. Yang, L. Li, K.-X. Yang, X. Han, Y.-Q. Yao, J. Li, H.-Y. Wu, S. Wan, L. Liu,

D.-Q. Liu, Y.-W. Kuang, Z.-P. He, P. Shang, C. Guo, R.-H. Zheng, K. Tian, Z.-C. Zhu, N.-L. Liu, C.-Y. Lu, R. Shu, Y.-A. Chen, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, *Ground-to-satellite quantum teleportation,* Nature **549**, 70–73 (2017).

[209] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, S.-L. Han, Q. Yu, K. Liang, F. Zhou, X. Yuan, M.-S. Zhao, T.-Y. Wang, X. Jiang, L. Zhang, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, C.-Y. Lu, R. Shu, J.-Y. Wang, L. Li, N.-L. Liu, F. Xu, X.-B. Wang, C.-Z. Peng, and J.-W. Pan, *An integrated space-to-ground quantum communication network over 4,600 kilometres,* Nature **589**, 214–219 (2021).

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

[211] H. J. Kimble, *The quantum internet,* Nature **453**, 1023–1030 (2008).

[212] R. Trényi, K. Azuma, and M. Curty, *Beating the repeaterless bound with adaptive measurement-device-independent quantum key distribution,* New Journal of Physics **21**, 113052 (2019).

[213] M. Gündoğan, J. S. Sidhu, V. Henderson, L. Mazzarella, J. Wolters, D. K. L. Oi, and M. Krutzik, *Proposal for space-borne quantum memories for global quantum networking,* npj Quantum Information **7** (2021).

[214] S. Ecker, B. Liu, J. Handsteiner, M. Fink, D. Rauch, F. Steinlechner, T. Scheidl, A. Zeilinger, and R. Ursin, *Strategies for achieving high key rates in satellite-based qkd,* npj Quantum Information **7**, 1–7 (2020).

[215] D. Dequal, L. T. Vidarte, V. R. Rodriguez, G. Vallone, P. Villoresi, A. Leverrier,

and E. Diamanti, *Feasibility of satellite-to-ground continuous-variable quantum key distribution,* npj Quantum Information **7** (2021).

[216] S. Khatri, A. J. Brady, R. A. Desporte, M. P. Bart, and J. P. Dowling, *Spooky action at a global distance: analysis of space-based entanglement distribution for the quantum internet,* npj Quantum Information **7** (2021).

[217] C.-Y. Lu, Y. Cao, C.-Z. Peng, and J.-W. Pan, *Micius quantum experiments in space,* Rev. Mod. Phys. **94**, 035001 (2022).

List of Publications

Thesis related Publications

1. **Anju Rani**, Jayanth Ramakrishnan, Tanya Sharma, Pooja Chandravanshi, Ayan Biswas, Ravindra P. Singh, "Experimental shot noise measurement using the imperfect detection- A special case for pulsed laser," IEEE Journal of Quantum Electronic **59**, (2023).
   DOI:10.1109/JQE.2023.3308263.

2. **Anju Rani**, Pooja Chandravanshi, Jayanth Ramakrishnan, Pravin Vaity, Madhusudan P., Tanya Sharma, Pranav Bhardwaj, Ayan Biswas, Ravindra P. Singh "Free space CVQKD with Discrete Phases," Physics Open **17**, 2666-0326 (2023).
   DOI: https://doi.org/10.1016/j.physo.2023.100162

3. **Anju Rani**, and R. P. Singh, "Passive QRNG based BB84 QKD protocol using heralded single photon source," (Submitted to Journal of Optics).

4. **Anju Rani**, and R. P. Singh, "Demonstration of free space CVQKD over 200 m using Gaussian Modulation" (under preparation).

5. **Anju Rani**, and R. P. Singh, "Sustainability of various discrete modulation CVQKD protocols over turbulent space" (under preparation).

Other Publications

6. Sarika Mishra, Ayan Biswas, Satyajeet Patil, Pooja Chandravanshi, Vardaan Mongia, Tanya Sharma, **Anju Rani**, Shashi Prabhakar, S Ramachandran, and Ravindra Pratap Singh, "BBM92 quantum key distribution over a free space dusty channel of 200 meters", Journal of Optics **24**, 074002 (2022).
   DOI: https://doi.org/10.1088/2040-8986/ac6f0b

7. Nijil Lal, Sarika Mishra, **Anju Rani**, Anindya Banerji, C. Perumangattu, and R. P. Singh, "Polarization-orbital angular momentum duality assisted entanglement observation for indistinguishable photons", Quantum Inf Process 22, 90 (2023).
   DOI:https://doi.org/10.1007/s11128-022-03815-z

8. Patnala Vanitha, Nijil Lal, **Anju Rani**, Salla Gangi Reddy, R. P. Singh, "Correlations in scattered perfect optical vortices", J. Opt. **23** 095601.
   DOI: https://doi.org/10.1088/2040-8986/ac094f