Information Security and Quantum Communication

A thesis submitted in partial fulfilment of

the requirements for the degree of

Doctor of Philosophy

by

Tanya Sharma

(Roll No. 19330019)

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

2024

To

My Family and Friends

Declaration

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

Signature

Name: Tanya Sharma

(Roll No: 19330019)

CERTIFICATE

It is certified that the work in the thesis titled **"Information Security and Quantum Communication"** by Ms Tanya Sharma (Roll No. 19330019) has been carried out under my supervision and 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
(Thesis Supervisor)
Senior Professor
Atomic, Molecular and Optical Physics Division,
Physical Research Laboratory,
Ahmedabad, India.

Acknowledgments

These research years have been a collaborative endeavour, and I am deeply grateful to everyone who has been a part of this enriching experience. From insightful discussions to unwavering support, each individual has been crucial in shaping my learning and unlearning process. I want to take this opportunity to thank everyone who has been a part of this amazing journey.

My first note of gratitude to my family is from the bottom of my heart. Maa, you didn't just raise me with love and care but became my confidante and closest friend. Papa, you have always been my biggest cheerleader, so thank you for chanting encouragement in my heart. I thank Baba and Maa for their love and support. Adi, you're not just my life partner but the source of my strength. I promise to always be your biggest supporter, just like you are mine. I love you all and will always chase your proud smiles, no matter how big or small the win.

My deepest gratitude goes to Prof. R.P. Singh for this opportunity to work with him and for believing in me. You embody the true spirit of 'simple living and high thinking'. Thank you for setting such a high standard of integrity and dedication. Working alongside you and being inspired by your actions is an honour.

I sincerely thank my DSC members, Prof. G.K. Samanta, Prof. Varun Sheel, and Dr. Satyajit Seth, for thoroughly reviewing my work. I deeply appreciate your support, patience, and expert guidance throughout this journey. Our discussions during the DSC and area seminar always helped me to have a deeper understanding of my research work.

I sincerely appreciate the faculty members of PRL who instructed me during coursework and inspired my pursuit of research. Special recognition goes to all my teachers at various stages of my educational journey for their contribution to my journey

I extend my gratitude to all members of the Academic Committee for their insightful comments and encouragement throughout my research period. I am deeply thankful to Director Prof. Anil Bhardwaj, Dean Prof. D. Pallamraju, and Head of Academic Services Dr. Bhushit Vaishnav for their unwavering support during my Ph.D. tenure. I appreciate the academic and administrative staff of IIT Gandhinagar for their assistance with registration procedures.

Furthermore, I wish to acknowledge the invaluable assistance provided by personnel from the accounts, purchasing, library, computer centre, administration, canteen, CMD, dispensary, transport, and housekeeping departments throughout my doctoral studies.

I would also like to thank my thesis reviewers for their time, effort, and constructive feedback on my thesis. Their insightful comments and suggestions have been invaluable in improving the quality of my work. I appreciate their careful consideration of my research and their contributions to its enhancement.

The inspiration, assistance, and collaborative efforts my fellow group members extended to me transcend the conventional bounds of acknowledgement. I wish to convey my profound gratitude to each group member for their support throughout my PhD journey. I am grateful to Pravin, Shashi, Nijil, Anindya, Satyajeet, Sarika, Anju, Vardaan, Anirban, Vimlesh, Sandeep, and Chahat for their insightful discussions.

I extend my heartfelt gratitude to Jayanth for the invaluable learnings and support provided at every juncture. I thank Dr. Rutvij, my collaborator, for engaging in valuable discussions. I would also like to extend my immense gratitude to Pooja and J.K. Their contribution to fostering a positive and enjoyable working environment has been invaluable. A special thanks to Ayan and Shefali for their consistent moral reinforcement and unwavering support, both personally and professionally, which played a pivotal role in facilitating a smooth progression through my doctoral studies.

This work would be incomplete without acknowledging the love and support of my friends Anshika, Daya, Meghna, Shreya, Saumya, Madhu, Vinitha, Namita, and Yash. Their friendship brought joy and made this journey truly enjoyable. Special thanks to my best friend, Pranav, for his calming presence.

Lastly, I extend my deepest gratitude to God, above all.

Tanya Sharma

Abstract

While numerous theoretical security proofs back up quantum key distribution (QKD), its practical implementation introduces vulnerabilities that adversaries can exploit. Many proofs assume idealistic, perfect devices, neglecting the imperfections present in real-world setups. These device imperfections become loopholes, potentially leaking partial key information to eavesdroppers. The theoretical advantage of QKD lies in detecting attacks, not their absolute prevention. However, it is possible that an adversary may exploit the loopholes present in practical implementations to gain information without alerting the authenticated parties.

The primary objective of this thesis is to attempt to bridge the gap between the theoretical and experimental QKD. Proper characterization of our devices is essential to account for this information leakage in key rate estimation. The studies have been performed at both the detection and the source end, concluding by proposing a protocol to achieve our goal.

The receiver's end is highly prone to an attack by the adversary. We have examined the effects of detection coupling mismatch at the receiver's end, finding possible information leakage. We observed how high coupling mismatch leads to information leakage, even for symmetrical modes. We compared low and high coupling mismatch cases employing cross-correlation and quantified the mutual information between the receiver and eavesdropper.

Many practical QKD protocols employ weak coherent laser pulses, following Poissonian statistics implying a non-zero probability of more than one photon per pulse. Rigorous characterization of photon statistics facilitates attack detection and secure key rate estimation, enhancing overall QKD system security. We have characterized our source to estimate the mean photon number using multiple detectors for

comparison against single detector measurements. Additionally, we studied intensity fluctuations to identify and mitigate potential information leakage due to state preparation flaws. As detailed in the following paragraph, we have addressed practical QKD implementation constraints using weak coherent pulses.

Enhancing the key rate in the practical implementation of QKD settings is challenging. To overcome this challenge, we proposed the Entrapped Pulse Coincidence Detection (EPCD) protocol that does not require additional resources beyond those for BB84 and decoy state protocol. Here, we employ random pulses between the encoded pulses as well as monitor coincidences that aid in the detection of sophisticated attacks, leading to higher key rates. We performed a comparative analysis of key rates using different protocols and assessed their effectiveness. We have used the convex optimisation problem to optimize key rates, providing tight bounds on asymptotic key rates. This method yields reasonable bounds and is adaptable for schemes requiring further tightening. Results from field implementation illustrate substantial enhancements in asymptotic key rates, with plans for future finite-size analysis of the proposed protocol.

This research addresses the challenges of information leakage due to imperfect devices in practical QKD implementations. The studies propose methods to improve key rate estimation by characterizing source imperfections and detector coupling mismatch. Here, we introduce an integrated approach to get tighter bounds on the key rate. The aim is to bridge the gap between theoretical security and practical QKD, paving the way for secure quantum communication.

Keywords: Quantum Key Distribution (QKD), Quantum Communication, Quantum Cryptography, Discrete Variable QKD, Information Leakage, Cross Correlation, BB84 Protocol.

Abbreviations

QKD	Quantum Key Distribution
SPS	Single Photon Source
HWP	Half Wave Plate
QWP	Quarter Wave Plate
SPCM	Single Photon Counting Module
FC	Fiber Coupler
BS	Beam Splitter
PBS	Polarizing Beam Splitter
EPCD	Entrapped Pulse Coincidence Detection
PNS	Photon Number Splitting
SDP	Semi-Definite Programming
LDC	Laser Driving Circuit
OD	Optical Density
WCP	Weak Coherent Pulse
QBER	Quantum Bit Error rate
FPGA	Field Programmable Gated Array

Contents

List of Figures

List of Tables

List of Algorithms

Chapter 1

Introduction

When you know your WHY, you'll know your WAY

- Michael Hyatt

1.1 Information Security

The threat to information security by unauthorized access to confidential data and private information is appalling, not only for commercial and defence applications but also for human dignity. Since ancient times, many cryptographic techniques have been employed to ensure the secrecy of communication. Cryptography and cryptanalysis are two integral facets of cryptology (Fig. 1.1). While cryptography involves designing algorithms for secure data protection, cryptanalysis plays a crucial role in identifying vulnerabilities in these algorithms. This back-and-forth process of recognizing weaknesses and designing algorithms to overcome them empowers us to enhance the security of our cryptographic systems.

Cryptography involves cryptographic primitives, algorithms, protocols, and schemes.

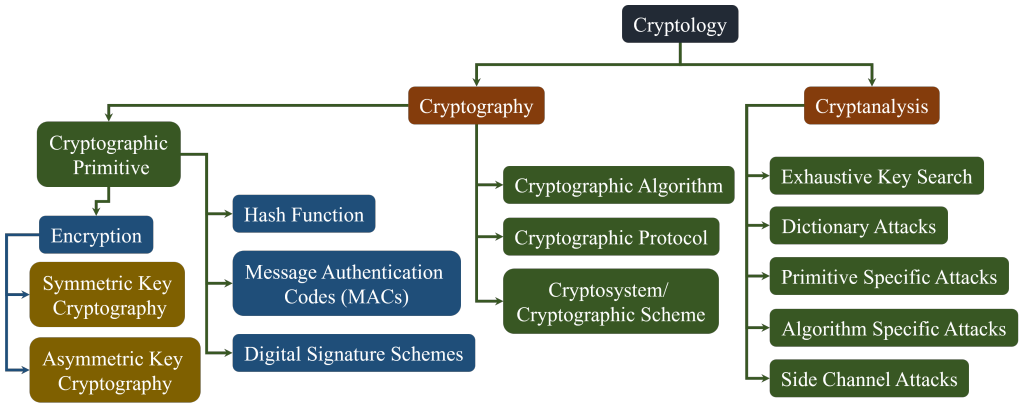


Figure 1.1: Cryptology classification: Cryptography and Cryptanalysis, with Cryptography branching into Symmetric and Asymmetric techniques.

Cryptographic primitives are the tools in the cryptography toolkit, including encryption, hash functions, message authentication codes and digital signatures. Encryption is classified as symmetric and asymmetric key cryptography, as discussed in Sec.1.2. Encryption provides confidentiality; however, we need additional tools to ensure data integrity and user authentication. Hash functions, message authentication codes (MACs), and digital signature schemes help overcome such challenges. Hash functions convert input data into a fixed-size string of characters, acting like digital fingerprints to ensure data integrity. Message Authentication Codes (MACs) and digital signatures are used to verify the authenticity and integrity of data; MACs use secret keys, while digital signatures use a public-private key pair. Cryptographic algorithms are the recipe for the steps involved, and protocols are a sequence of message exchanges achieving the security goals. A cryptographic scheme refers to the implementation of cryptographic primitives and their infrastructure. However, potential attacks exist on these cryptosystems, like exhaustive key search, dictionary attacks, primitive-specific attacks, algorithm-specific attacks, and side-channel attacks. Investigation of these cryptographic schemes is a crucial aspect of cryptanalysis for developing strong security systems.

1.2 Cryptography

The primary objective of cryptography is to facilitate a secure exchange of information between two parties, the sender and receiver, commonly known as Alice and Bob, in the presence of an adversary, Eve. Cryptography provides a means to uphold the privacy of the message through cryptographic tools, ensuring secure communication. When Alice wishes to communicate with Bob securely, she employs **encryption** to transform her message (**plaintext**) into an unreadable ciphertext using a secret key. This ciphertext is incomprehensible to anyone lacking the proper key. Afterwards, Alice transmits this encrypted message to Bob, who utilizes the corresponding key to perform **decryption**. Decryption is extracting the original plaintext message from the encrypted **ciphertext**.

Cryptography is broadly classified into two categories based on the tools and algorithms employed in encryption and decryption: **Symmetric-key cryptography** and **Asymmetric-key cryptography**.

1.2.1 Symmetric-key cryptography

Symmetric-key cryptography employs identical keys for both encryption and decryption (Fig. 1.2).

The drawback of symmetric-key cryptography is that Alice and Bob must agree on a shared key in advance, which becomes challenging when they are geographically separated. Asymmetric-key cryptography offers a potential resolution by eliminating the need for a pre-established secret key.

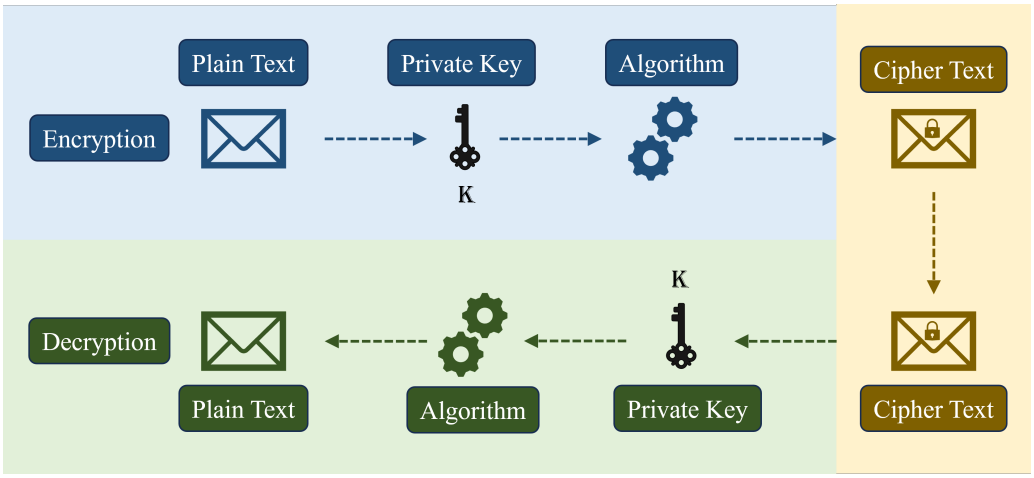


Figure 1.2: Symmetric-key cryptography using the same key, K, for encoding and decoding, that is secret to sender and receiver.

1.2.2 Asymmetric-key cryptography

In 1976, Diffie and Hellman [1] introduced the concept of employing two distinct keys in cryptographic operations. They suggested the use of a public key, which is distributed openly through a communication channel and employed for encryption, and a private key, which is kept confidential for decryption purposes (Fig. 1.3). The renowned asymmetric key cryptosystem, developed by Rivest, Shamir, and Adleman (RSA) in 1978 [2], relies on the computational complexity of the prime factorization problem.

However, Peter Shor, in 1997 [3], proposed an algorithm for solving the prime factorization problem in polynomial time using a quantum computer. The classical cryptographic techniques based on computational complexity cannot offer information-theoretic security. The advancement in quantum technology poses a substantial threat to the existing cryptosystems[4–6].

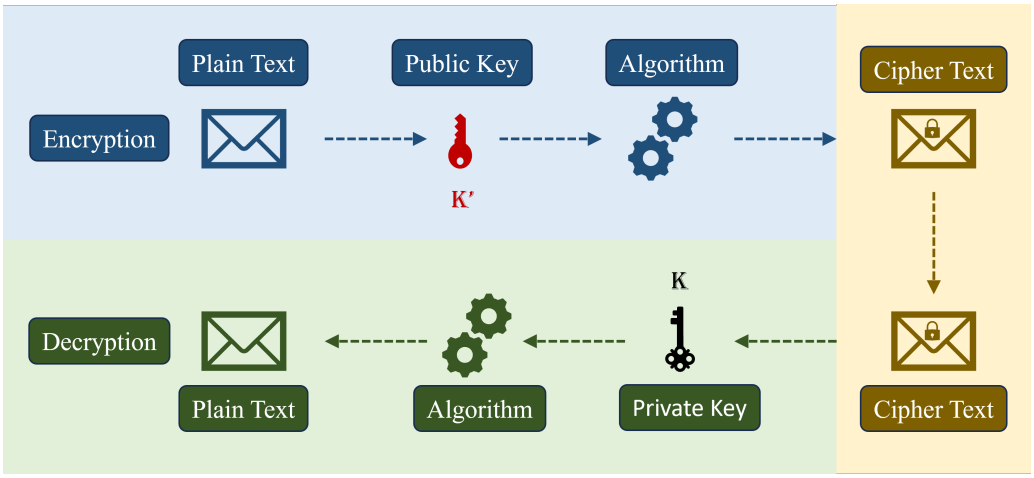


Figure 1.3: Asymmetric-key cryptography: Sender uses the public key to encode the message, and the receiver decodes it using the private key.

1.3 Cryptanalysis

Cryptanalysis involves analyzing cryptographic systems to identify weaknesses and develop methods to break their security. In cryptography, security encompasses three key aspects: the attack model, adversarial goal, and security level. The attack model specifies the adversary's knowledge about the cryptosystem. We follow Kerckhoff's principle [7, 8], which assumes the adversary knows the protocol and the scheme of the cryptosystem. The adversarial goal defines what the adversary seeks to obtain from the cryptographic system, specifying the information it aims to acquire. Ultimately, the security level dictates the effort to compromise the cryptographic system, encompassing both computational resources and the time required for a successful attack. A security statement for a cryptographic scheme affirms that a specific adversarial goal cannot be attained within a defined attack model, considering specified computational resources.

Computational security means it is practically impossible to breach a cryptographic system within a reasonable time frame, given the available computational

resources. We aim for the **unconditional security**, which implies that the cryptosystem stands impervious to any attack without making any assumptions about the extent of Eve's power. This level of security represents the utmost assurance in safeguarding sensitive information. It is important to note that asymmetric key cryptography provides computational security and does not guarantee information-theoretic security. The advent of quantum computers significantly threatens existing cryptographic algorithms, and we can no longer guarantee the security of sensitive information with classical communication.

Forward Secrecy is crucial for ensuring the confidentiality of past communications even if current encryption keys are compromised, guaranteeing future security. Consider the duration x (in years) required for classical cryptographic keys to remain secure, referred to as the security shelf-life. Next, let y denote the time needed to migrate from the existing classical infrastructure to quantum-secure encryption, known as the migration time. Finally, let z be the collapse time, representing the period needed to develop a large quantum computer. If the sum $x + y > z$, then it is a concerning issue for future security. Developing cryptographic tools resistant to quantum attacks is essential to guarantee the long-term security of encrypted data. According to [9], the need to develop quantum-safe solutions is urgent due to projected timelines for quantum computing's potential impact on cryptography. This urgency stems from concerns about how long encrypted data must remain secure and the rapid advancements in quantum computing technology.

1.4 One Time Pad

In 1926, Vernam introduced the **One-Time Pad (OTP)** [10]. In 1949, Claude Shannon provided formal validation in "Communication Theory of Secrecy System" [11] and demonstrated the information-theoretical security of the OTP; it necessitates

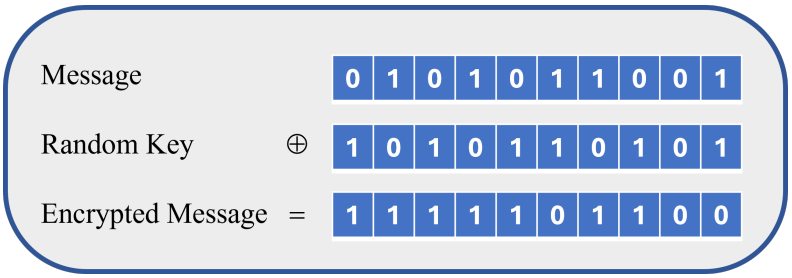


Figure 1.4: Encryption using One Time Pad (OTP): A secure and random key of the same length as the message used to encrypt the message.

several conditions:

1. The key must be entirely random.
2. The key must match the length of the message.
3. The key must be distributed securely.
4. The key must never be used again.

The randomness and security of this key ensures that only someone possessing it can decrypt the encoded message, rendering it unintelligible to anyone else (Fig. 1.4). However, the requirements of OTP pose challenges for practical implementation. While symmetric key cryptography employing the OTP achieves information-theoretic security, it ultimately faces the challenge of key distribution, especially when Alice and Bob are geographically separated.

1.5 Quantum Key distribution

The problem of cryptography ultimately melts down to the **key distribution problem**. When the key is secure, the adversary cannot deduce any information from the ciphertext. Quantum Key Distribution (QKD) enables the authenticated parties to

establish such secure keys. QKD, combined with OTP, opens the door for unconditionally secure communications. The security of QKD protocols is based on the fundamental laws of physics and assumes no limits on the adversary's technological power [12–19]. It offers a secure key distribution not because it forbids an adversary from attacking the system but because we can detect an attack when it occurs. Bennett and Brassard proposed the first QKD protocol in 1984 [20], followed by many other protocols [21–26]. BB84 was first demonstrated in 1992 [27]. Since then, there have been great advances in QKD both in theory and practice [28–33].

The QKD relies on several fundamental principles of quantum mechanics to ensure secure communication. These principles include:

1. **Uncertainty Principle**: We cannot precisely measure two canonically conjugate variables simultaneously.
2. **No Cloning Theorem**: It is impossible to clone an arbitrary quantum state perfectly [34].
3. **Perturbation**: Any measurement on a quantum system perturbs the quantum state.
4. **Entanglement Monogamy**: For two systems to be maximally entangled with each other, they must not be entangled with any third system.

The aforementioned statements highlight a pessimistic perspective, emphasizing the inability to measure two conjugate variables simultaneously, clone a quantum state, measure a quantum state without perturbing the system, and establish entanglement with a third party. Nonetheless, these intrinsic properties of quantum systems provide an opportunity for unconditionally secure communications. Using mutually unbiased bases and no-cloning theorem enables us to detect the presence

of an eavesdropper in an ideal QKD system. QKD encompasses various branches, as depicted in Fig. 1.5.

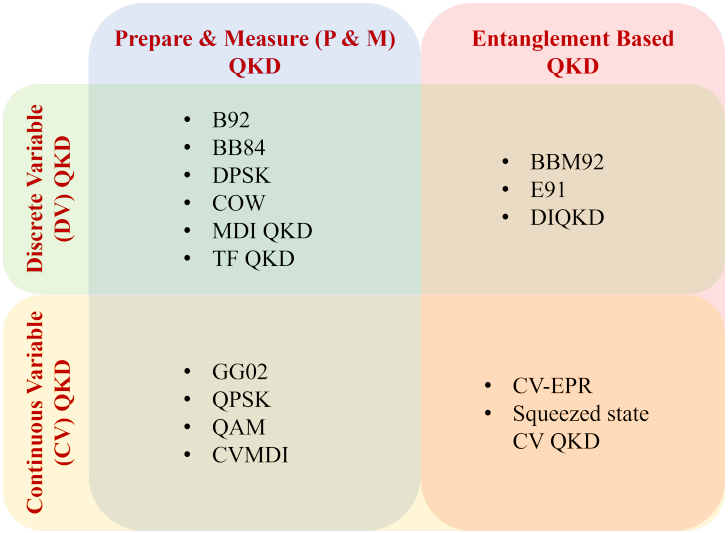


Figure 1.5: Classification of Quantum Key Distribution (QKD) based on four categories: Prepare and measure (P & M) QKD, Entanglement Based QKD, Discrete Variable (DV) QKD and Continuous variable (CV) QKD.

1.6 Theoretical QKD v/s Practical QKD

The experimental implementation of QKD protocols uses imperfect devices that act as Achilles' heel. Though QKD's theoretical advantage lies in detecting attacks, not their absolute prevention, practical implementations with imperfect devices might not raise sufficient red flags. Fig. 1.6 represents how the theoretical security assumptions of the components do not hold for practical implementations of a standard BB84 protocol. These assumptions may vary from protocol to protocol and must be considered during the experimental implementation. Eavesdroppers could leverage these imperfections to extract partial information without triggering alarms. This poses a significant concern, highlighting the discrepancy between theoretical promises and real-world capabilities. While numerous theoretical security

proofs back up quantum key distribution (QKD), many of them assume idealistic, perfect devices, neglecting the imperfections present in real-world setups. The practical implementation introduces vulnerabilities that adversaries can exploit [35–50].

The loopholes due to device imperfections need to be acknowledged, and countermeasures to the potential attacks must be proposed. We could improve our QKD system by using better single photon sources, high-efficiency detectors, and a low-loss channel. However, we could not reach the ideal limit since the real devices are bound to have imperfections. An eavesdropper may exploit device imperfections to gain partial information about the key without alerting the authenticated users, which makes us question the security of QKD protocols. The security analyses of device imperfections have been studied in [17, 19, 51]. Device-independent QKD [52], and measurement device-independent QKD [53], [54] protocols have helped to overcome these device imperfections. Another solution is security patching, where we can characterize and monitor our QKD system to estimate the information leakage. It is critical when we work with imperfect devices to detect Eve's presence and improve the performance of the QKD system. The ultimate goal is to attain unconditional security, but until then, we must acknowledge the flaws in our implementation.

Precisely characterizing device imperfections is essential to bridge the gap between theory and practical implementations. This would enable us to define the protocol's operational and security limits. A comprehensive security analysis, considering realistic device parameters and potential attack scenarios, is essential to any Quantum Key Distribution (QKD) protocol.

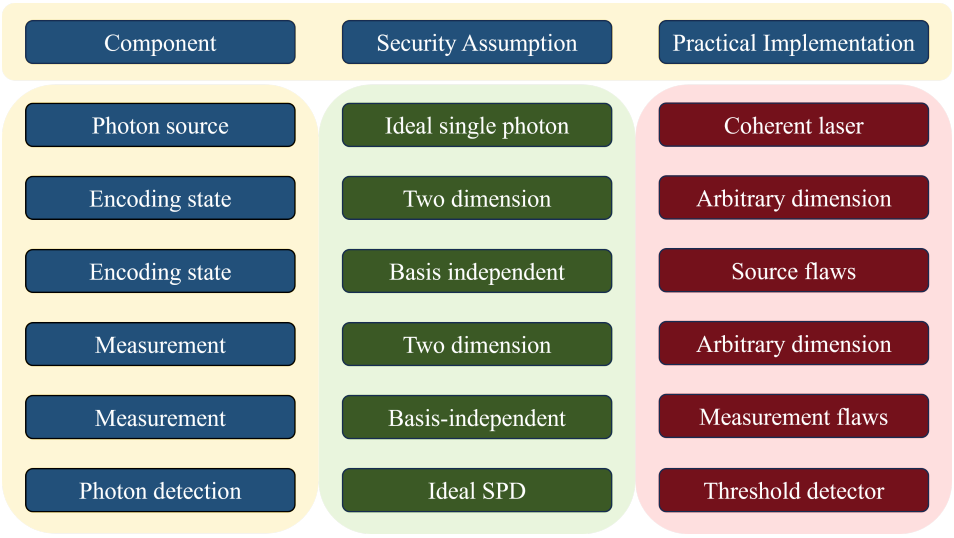


Figure 1.6: Comparison between the theoretical security assumption and experimental implementation parameters for standard BB84 protocol

1.7 Thesis

1.7.1 Objective

The primary objective of this thesis is to attempt to bridge the gap between the theoretical and experimental QKD. While QKD offers theoretical information security, its real-world implementation poses challenges due to device imperfections, potentially leading to information leakage. Therefore, it is crucial to thoroughly characterize these devices to accurately estimate key rates while considering information leakage. This study focuses on investigating vulnerabilities at both the detection and source end. We aim to enhance the practicality of QKD while maintaining its security. To achieve this, we have proposed a new protocol designed to advance this objective.

1.7.2 Overview

We have examined the effects of detection coupling mismatch between detectors, revealing potential information leakage. We gain insights into mitigating this leakage by comparing low and high coupling mismatch cases using cross-correlation and mutual information.

Additionally, we have rigorously characterized the photon statistics of weak coherent laser pulses commonly used in practical QKD protocols. Understanding these statistics, especially in protocols like decoy state and coincidence detection, aids in detecting information leakage and estimating secure key rates. Our characterization includes estimating mean photon numbers using multiple detectors and studying intensity fluctuations to address potential information leakage due to state preparation flaws, thereby enhancing information-theoretic security.

Furthermore, we have addressed practical implementation constraints using weak coherent pulses by integrating conventional decoy pulse approaches with coincidence detection protocols. This integration allows the detection of sophisticated attacks and leads to higher key rates. Optimization of key rates using Semi-Definite Programming (SDP) provides tight bounds and demonstrates significant enhancements in asymptotic key rates in field implementations.

1.7.3 Organisation

- Chapter-1: Introduction

  This chapter provides a foundation in cryptography, progressively establishing the necessity for quantum cryptography. It explores the practical limitations of implementing quantum key distribution (QKD). Subsequently, the

chapter outlines the motivation for the research conducted within this thesis. Finally, the primary research objectives are articulated.

- Chapter-2: Theoretical Background

  This chapter introduces the fundamental concepts and methods used in this study. It explains the key ideas and frameworks that the research builds upon. The chapter also explores the concept of qubits and how they are represented, manipulated and measured. It describes the specific equipment and detectors used in practical implementations of QKD protocols. Finally, the chapter details the chosen research methods, including the techniques used to gather and analyze information. This chapter provides a clear understanding of the research approach and its components.

- Chapter-3: Vulnerability due to detection coupling mismatch

  This chapter examines the impact of coupling mismatch between detectors on information security. It assesses the extent to which a potential eavesdropper can access information due to coupling mismatch at the receiver's detectors, specifically analyzing the mutual information between Eve and the receiver. The chapter discusses experiments conducted with Gaussian and Laguerre-Gaussian signal modes. It underscores the significance of considering detection coupling mismatch to prevent potential side-channel attacks.

- Chapter-4: Mitigating the source-side channel vulnerability

  This chapter highlights the critical role of precise measurement and characterization of photon statistics in enhancing the overall security of the Quantum Key Distribution (QKD) system. It details a meticulous characterization of the photon source to determine the average photon number using multiple detectors, allowing for comparison against measurements obtained with a single detector. Additionally, the analysis of intensity fluctuations aids in

the identification and mitigation of potential information leakage arising from imperfections in the state preparation process. Ultimately, this chapter strives to bridge the gap between theoretical concepts and practical implementation to achieve information-theoretic security in QKD systems.

- Chapter-5: Decoy and Coincidence Detection QKD Protocol
  This chapter addresses limitations encountered in practical implementations of Quantum Key Distribution (QKD) utilizing weak coherent pulses. It examines enhancing the conventional method of employing decoy pulses by incorporating it with coincidence detection (CD) protocols. Furthermore, it presents a straightforward algorithm for computing asymptotic key rates applicable to this protocol. The chapter also delves into experimental implementations, illustrating that monitoring coincidences in the decoy state protocol yields improved key rates in real-world experimental scenarios.

- Chapter-6: Summary and Future Perspective
  This chapter presents a concise summary of the overall research. It examines the principal findings, their significance and implications. Moreover, it offers an overview of the key takeaways from each chapter of the thesis, integrating them with the current state of knowledge within the field. Additionally, the chapter acknowledges the inherent limitations and proposes avenues for future research endeavours.

1.8 Summary

This chapter explored the critical role of information security on both a personal and national scale. It introduced the two main branches of cryptology: cryptography, the art of securing information, and cryptanalysis, the art of breaking such codes.

The chapter then delved into symmetric and asymmetric key distribution methods, highlighting their limitations. Furthermore, it discussed the potential vulnerabilities of classical cryptography to advancements in algorithms and the rise of quantum computers. The concept of the one-time pad (OTP) was introduced, demonstrating how secure communication hinges on the secure distribution of keys. Following this, the chapter explored Quantum Key Distribution (QKD) as a method for secure key exchange, leveraging the fundamental principles of quantum mechanics to eliminate reliance on assumptions about an eavesdropper's capabilities. The chapter acknowledged potential loopholes arising from device imperfections, thereby motivating further research in this domain. Finally, the objective, overview and structure of the thesis are outlined.

Chapter 2

Theoretical Background

Everything should be made as simple as possible, but no simpler

- Albert Einstein

2.1 Information Theory

Information is an organized arrangement of letters, numbers, or symbols following a set of rules for communication. In 1837, Samuel Morse demonstrated the electrical telegraph employing sequences of dots and dashes to represent the alphabetic characters, known as Morse codes. Claude Shannon's seminal work "Mathematical Theory of Communication" in 1948 [55] laid the groundwork for the digitization of information. In modern times, electronics enable us to encode information using **bits**, a binary digit that can take values 0 or 1. Bits are the basic building blocks for digital information storage, transmission, and processing. Information theory quantifies the fundamental limits of data compression and channel capacity. Following are several essential tools that aid in this quantification.

2.1.1 Shannon Entropy

Shannon entropy is the key concept of information theory. If X is a random variable, then Shannon entropy is the measure of information we gain by learning about X. In an alternative view, Shannon entropy measures uncertainty before we learn the value of X. If $p(x)$ is the probability distribution of X, with $x \in X$ then Shannon entropy is given as:

$$H\left(X\right) = -\sum_{x \in X} p(x) \log p(x). \tag{2.1}$$

Entropy is a function of the probability distribution of X and not of its values. Hence, it is also represented as $H(p)$. Throughout this study, the log is to the base at 2, and the unit of entropy is bits unless specified otherwise.

Binary entropy

The entropy of a random variable having a binary probability distribution, just two probable outcomes, is called the binary entropy. If p and $(1-p)$ are the probabilities of the two outcomes, then the binary entropy (H_{bin}) is given as:

$$H_{\text{bin}}\left(p\right) = -p \log p - (1-p) \log(1-p). \tag{2.2}$$

Joint Entropy

If (X, Y) are a pair of random variables with joint probability distribution $p(x, y)$, with $x \in X$ and $y \in Y$, then their joint entropy $H(X, Y)$ is defined as:

$$H(X, Y) = -\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) \log p(x, y). \tag{2.3}$$

Conditional entropy

The conditional entropy $H(Y|X)$ of a pair of X and Y, is given as:

$$\begin{aligned} H(Y|X) &= -\sum_{x\in\mathcal{X}} p(x)H(Y|X=x), && (2.4)\\ &= -\sum_{x\in\mathcal{X}} p(x)\sum_{y\in\mathcal{Y}} p(y|x)\log p(y|x), && (2.5)\\ &= -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log p(y|x). && (2.6) \end{aligned}$$

where, $p(x,y)$ is the joint probability and $p(y|x)$ & $p(x|y)$ are the conditional probabilities.

2.1.2 Relative entropy

Relative entropy, also known as the Kullback-Leibler (KL) divergence, is the asymmetric measure of the difference between two probability distributions. If $p(x)$ and $q(x)$ are two probability distribution functions, then their relative entropy $D\left(p||q\right)$ is defined as:

$$D\left(p||q\right) = \sum_{x\in\mathcal{X}} p(x)\log\frac{p(x)}{q(x)}. \quad (2.7)$$

KL-divergence quantifies the additional bits needed to represent an event from a distribution $q(x)$ instead of $p(x)$.

2.1.3 Mutual Information

Mutual information is the amount of information one random variable has about the other. Alternatively, mutual information quantifies how the knowledge of one random variable reduces the uncertainty of the other. Mutual information between

two random variables (X, Y) is the relative entropy between the product of their probability distributions and the joint probability (Eq. (2.8)).

$$\begin{aligned} I(X:Y) &= D(p(x,y)||p(x)p(y)) \\ &= \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log\frac{p(x,y)}{p(x)p(y)}. \end{aligned} \tag{2.8}$$

Relation Between Entropy and Mutual Information

In Eq. (2.9), we establish the relationship between mutual information and entropy of two random variables.

$$\begin{aligned} I(X:Y) &= \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log\frac{p(x,y)}{p(x)p(y)} \\ &= \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log\frac{p(x|y)}{p(x)} \\ &= -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log p(x) + \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log p(x|y) \\ &= -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x)\log p(x) - (-\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log p(x|y)) \\ &= H(X) - H(X|Y). \end{aligned} \tag{2.9}$$

Hence, mutual information is rightly defined as reducing the uncertainty of one random variable with the knowledge of another. The symmetry of joint distribution $p(x, y)$ implies that the Mutual information is symmetric, i.e.

$$\begin{aligned} I(X:Y) &= H(X) - H(X|Y) = H(Y) - H(Y|X), \\ I(X:Y) &= I(Y:X). \end{aligned} \tag{2.10}$$

2.2 Quantum Information Theory

Quantum information theory encompasses a broad spectrum of topics. This discussion will focus on areas pertinent to our interests, including qubits, their manipulation, measurement, and the no-cloning theorem.

2.2.1 Qubits

Quantum binary digits or qubits are the building blocks of quantum information science. Here, we take a mathematical approach to understand qubits and will discuss their physical realization in Sec. 2.3. A qubit is a pure quantum state represented by a vector $|\psi\rangle$ in the two-dimensional Hilbert space ($\mathcal{H}^2$). Any qubit can be represented as a superposition of two states $|0\rangle$ & $|1\rangle$.

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{2.11}$$

Here, $\{|0\rangle\,, |1\rangle\} \in \mathcal{H}^2$ and are orthogonal to each other, i.e. $\langle 0|1\rangle = 0$. The coefficients α and β are complex numbers representing the amplitudes of $|0\rangle$ & $|1\rangle$, respectively. For a normalized state $\langle\psi|\psi\rangle = 1$, $|\alpha|^2+|\beta|^2= 1$, ensuring the total probability of finding the qubit in either state is unity. Examples of qubits include photon polarization states, electron spin states, and two-level energy states.

2.2.2 Bloch Sphere Representation

For a two-dimensional qubit system, $\{\mathbb{1}, \sigma_x, \sigma_y, \sigma_z\}$ form the basis set. These are called the Pauli Basis, and any operator can be written as a linear combination of

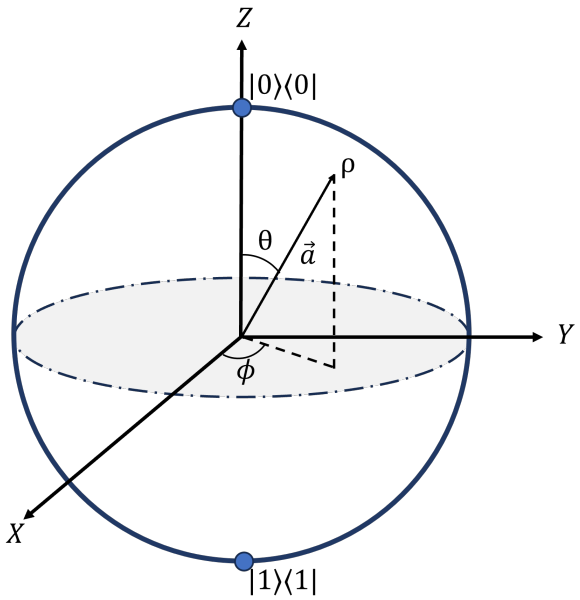


Figure 2.1: The Bloch sphere: Pure states lie at the surface with Bloch vector $\vec{a}$ of unit magnitude $|\vec{a}|= 1$. The center represents maximally mixed state $\rho = \frac{1}{2}\mathbb{1}$.

operators in Pauli Basis. Any unit trace qubit density operator ρ can be written as:

$$\rho = \frac{1}{2}(\mathbb{1} + a_X\sigma_x + a_Y\sigma_y + a_Z\sigma_z), \tag{2.12}$$

where, a_X, a_Y and a_Z are components of a vector $\vec{a}$. We introduce a vector $\vec{\sigma}$ having components σ_x, σ_y and σ_z operators.

$$\rho = \frac{1}{2}(\mathbb{1} + \vec{a}\cdot\vec{\sigma}). \tag{2.13}$$

The vector $\vec{a}$ is the block vector for the density operator ρ.

The Bloch vectors representing pure states form a sphere in real 3-D space, known as the Bloch sphere (Fig. 2.1). The orthogonal state vectors $|0\rangle$ and $|1\rangle$ correspond to antipodal points on the Bloch sphere.

A qubit can be represented as a point on a unit three-dimensional sphere known as

the Bloch sphere (Fig. 2.1). We can rewrite Eq. (2.11) as:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle\,, \tag{2.14}$$

where the angles θ and ϕ define the specific point on the Bloch sphere, with $0 \leq \theta \leq \pi$ and $0 \leq \phi < 2\pi$. The measurements performed in the $\{|0\rangle, |1\rangle\}$ basis will yield these basis states with probabilities of $\cos^2\left(\frac{\theta}{2}\right)$ and $\sin^2\left(\frac{\theta}{2}\right)$.

2.2.3 Basis for a Qubit

Any quantum state can be represented as a superposition of the basis vectors within a Hilbert space. The choice of basis is not unique, and the same quantum state can be represented using different basis vectors:

- **Standard/Computational Basis**: $|0\rangle$ & $|1\rangle$ form the standard basis vectors of the two-dimensional Hilbert space and are orthogonal to each other, i.e. $\langle 0|1\rangle = 0$.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2.15}$$

- **Hadamard Basis:** Another commonly used basis is the Hadamard basis, i.e. $|+\rangle$ & $|-\rangle$, where $\langle +|-\rangle = 0$. The Hadamard basis vectors are represented in terms of standard basis vectors as:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{2.16}$$

From Eq. (2.15) and Eq. (2.16) we get,

$$|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \qquad |-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}. \tag{2.17}$$

- **General Basis:** In terms of computational basis, we define the general basis as:

$$\begin{aligned} |V(\theta,\phi)\rangle &= \cos(\theta/2)\,|0\rangle + e^{i\phi}\sin(\theta/2)\,|1\rangle\,, \\ |V^{\perp}(\theta,\phi)\rangle &= -e^{i\lambda}\sin(\theta/2)\,|0\rangle + e^{i(\lambda+\phi)}\cos(\theta/2)\,|1\rangle\,. \end{aligned} \tag{2.18}$$

From Eq. (2.15) and Eq. (2.18) we get,

$$|V(\theta,\phi)\rangle = \begin{pmatrix} \cos(\theta/2) \\ e^{i\phi}\sin(\theta/2) \end{pmatrix}, \qquad |V^{\perp}(\theta,\phi)\rangle = \begin{pmatrix} -e^{i\lambda}\sin(\theta/2) \\ e^{i(\lambda+\phi)}\cos(\theta/2)) \end{pmatrix}. \tag{2.19}$$

2.2.4 Manipulating Qubits

Quantum gates are used to manipulate the quantum state and are unitary ($\hat{U}$), i.e. $\hat{U}^{\dagger}\hat{U} = \hat{\mathbb{I}}$. Here, $\hat{U}^{\dagger}$ is the Hermitian conjugate of $\hat{U}$ obtained by transposing U and taking the complex conjugate of each element. A single qubit quantum operator is usually represented as a 2×2 unitary matrix ($\hat{U}$).

$$|\psi'\rangle = \hat{U}\,|\psi\rangle\,. \tag{2.20}$$

The most general form of a single qubit unitary operator is,

$$\hat{U}_{\lambda,\theta,\phi} = \begin{pmatrix} \cos(\theta/2) & -e^{i\lambda}\sin(\theta/2) \\ e^{i\phi}\sin(\theta/2) & e^{i(\lambda+\phi)}\cos(\theta/2) \end{pmatrix}, \tag{2.21}$$

where,

$0 \leq \theta \leq \pi$,

$0 \leq \phi < 2\pi$, &

$0 \leq \lambda < 2\pi$.

With different values of θ, ϕ, and λ, many single qubit operators can be constructed (Table 2.1). We can visualize a single qubit unitary as rotation on the Bloch sphere using the angles θ, ϕ and λ. The transformation comprises three rotations, with the first rotation about the z-axis by an angle λ, followed by a rotation about the y-axis by an angle θ and then about the z-axis by an angle ϕ (see Fig. 2.2).

Operator	λ	θ	ϕ	Matrix
Identity	0	0	0	$\hat{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Pauli X(bit flip)	π	π	0	$\hat{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Pauli Y(bit and phase flip)	$\frac{\pi}{2}$	π	$\frac{\pi}{2}$	$\hat{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
Pauli Z(phase flip)	π	0	0	$\hat{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Hadamard	π	$\frac{\pi}{2}$	0	$\hat{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Table 2.1: Examples of Single qubit Unitary Operators $\hat{U}_{\lambda,\theta,\phi}$

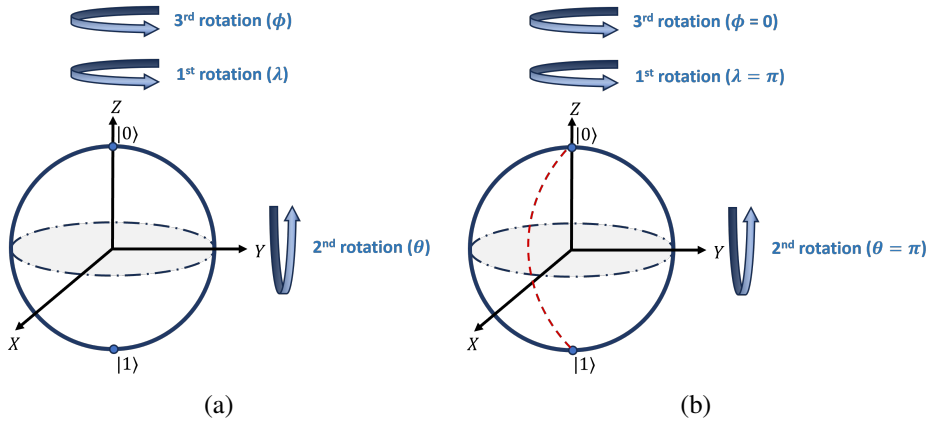


Figure 2.2: (a) Visualisation of a Unitary transformation $\hat{U}_{\lambda,\theta,\phi}$ as a rotation on the Block sphere. (b) An example of $\hat{X}$ transformation on a block sphere where, $\hat{X} = \hat{U}_{\pi,\pi,0}$

2.2.5 Measuring Qubits

A set of measurement operators, $\{M_m\}$, characterizes a quantum state measurement. These operators satisfy the completeness relation $\sum_x M_m^\dagger M_m = \mathbb{I}$, where $\mathbb{I}$ is the identity operator. When the quantum state $|\psi\rangle$ is measured with measurement operator, M_m it collapses to a state given by $|\psi_m\rangle$ with a probability, p_m:

$$|\psi_m\rangle = \frac{M_m |\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}, \tag{2.22}$$

$$p_m = \langle\psi|M_m^\dagger M_m|\psi\rangle\,. \tag{2.23}$$

Let us consider the measurement of the state $|\psi\rangle$ in standard basis (Eq. (2.11)) with two measurement operators, M_0 & M_1 (Eq. (2.24)).

$$M_0 = |0\rangle\langle 0|\,, \qquad\qquad M_1 = |1\rangle\langle 1|\,. \tag{2.24}$$

Operating the measurement operator M_0 and M_1 on $|\psi\rangle$ we get,

$$\begin{aligned} M_0 |\psi\rangle &= \alpha |0\rangle\,, \\ M_1 |\psi\rangle &= \beta |1\rangle\,. \end{aligned} \tag{2.25}$$

The normalised states $|\psi_0\rangle$ & $|\psi_1\rangle$ and the probabilities p_0 & p_1 are given in Eq. (2.26) and Eq. (2.27) respectively.

$$\begin{aligned} |\psi_0\rangle &= \frac{M_0 |\psi\rangle}{\sqrt{\langle\psi|M_0^\dagger M_0|\psi\rangle}} = \frac{\alpha |0\rangle}{|\alpha|}, \\ |\psi_1\rangle &= \frac{M_1 |\psi\rangle}{\sqrt{\langle\psi|M_1^\dagger M_1|\psi\rangle}} = \frac{\beta |1\rangle}{|\beta|}. \end{aligned} \tag{2.26}$$

$$\begin{aligned} p_0 &= \langle\psi|M_0^\dagger M_0|\psi\rangle = |\alpha|^2, \\ p_1 &= \langle\psi|M_1^\dagger M_1|\psi\rangle = |\beta|^2. \end{aligned} \tag{2.27}$$

Similarly, one can perform the measurements in the Hadamard basis. Where the measurement operators are given as $M_+ = |+\rangle\langle+|$ and $M_- = |-\rangle\langle-|$. We first write our state in the Hadamard basis (Eq. (2.16)) and then use the measurement operators.

2.2.6 Multiple qubits

Let us consider a two-qubit state. The general two-qubit state is represented as:

$$\psi_{A,B} = \alpha_{00}\,|0\rangle_A\,|0\rangle_B + \alpha_{01}\,|0\rangle_A\,|1\rangle_B + \alpha_{10}\,|1\rangle_A\,|0\rangle_B + \alpha_{11}\,|1\rangle_A\,|1\rangle_B\,, \tag{2.28}$$

where $\{|0\rangle_A, |1\rangle_A\}$ and $\{|0\rangle_B, |1\rangle_B\}$ are computational basis of qubit A and B respectively. Considering the two-qubit system as one system, it has four computational basis states ($\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$). Similar to the single qubit case, the state on measurement collapses to $|m\rangle$, $m = (00, 01, 10, 11)$ with probability $|\alpha_m|^2$.

There are multiqubit operators/gates; one of the famous examples is a controlled-NOT gate. This gate has two inputs: the control qubit and the target qubit. In Fig. 2.3, the top and bottom lines represent the control qubit and the target qubit, respectively. In a controlled-NOT (CNOT) operation, if the control qubit is $|0\rangle$, then the target qubit remains unchanged, and if the control qubit is $|1\rangle$, then the target qubit is flipped (valid for computational basis).

$$|00\rangle \to |00\rangle\,; |01\rangle \to |01\rangle\,; |10\rangle \to |11\rangle\,; |11\rangle \to |10\rangle\,. \tag{2.29}$$

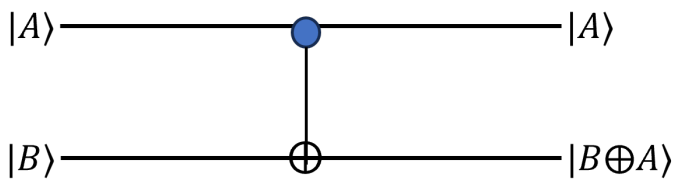


Figure 2.3: Controlled not gate with $|A\rangle$ as the control qubit and $|B\rangle$ as the target qubit. Input state $|A\rangle\,|B\rangle$ are in computational basis.

Following is the matrix representation of the C-NOT ($\hat{C}_X$) operator:

$$\hat{C}_X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{2.30}$$

2.2.7 Entangled States

We have explored qubits, which are closed systems. While a closed system is useful for analysis, achieving perfect isolation is impossible in practice. The universe, as a whole, might be the only truly closed system.

Consider a closed, isolated system comprising two subsystems: A and B with quantum state $|\Psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ of subsystems A and B,

$$|\Psi_{AB}\rangle = \sum_{i=1}^{n}\sum_{j=1}^{m} \alpha_{ij}\,|a_i\rangle\,|b_j\rangle\,, \qquad \alpha_{ij} = \langle a_i, b_j|\Psi_{AB}\rangle\,, \tag{2.31}$$

where, $\{|a_i\rangle\}(i = 1, 2, \cdots, n)$ and $\{|b_j\rangle\}$ $(i = 1, 2, \cdots, m)$ are orthonormal basis vectors of subsystems A and B [56].

If the subsystems A and B are not correlated then $\alpha_{ij} = \alpha_i^{(A)}\alpha_j^{(B)}$. In this case,

$$|\Psi_{AB}\rangle = \Big[\sum_{i=1}^{n} \alpha_i^{(A)} |a_i\rangle\Big]\Big[\sum_{j=1}^{n} \alpha_i^{(B)} |b_j\rangle\Big] \equiv |\psi_A\rangle\,|\psi_B\rangle\,, \tag{2.32}$$

where, $|\psi_A\rangle$ ($|\psi\rangle_B$) is the state vector of subsystem A(B).

If the systems A and B are correlated, then $\alpha_{ij} \neq \alpha_i^{(A)}\alpha_j^{(B)}$, which means that we cannot write Ψ_{AB} as in Eq. (2.32). Such a state is called an entangled state.

Among the simplest and most well-known entangled states are the Bell states. These states represent the maximum degree of entanglement between two qubits and serve as a resource for many quantum information protocols. Bell states are given by,

- $|\beta_{00}\rangle = \dfrac{|00\rangle + |11\rangle}{\sqrt{2}}$,
- $|\beta_{01}\rangle = \dfrac{|01\rangle + |10\rangle}{\sqrt{2}}$,
- $|\beta_{10}\rangle = \dfrac{|00\rangle - |11\rangle}{\sqrt{2}}$, &
- $|\beta_{11}\rangle = \dfrac{|01\rangle - |10\rangle}{\sqrt{2}}$.

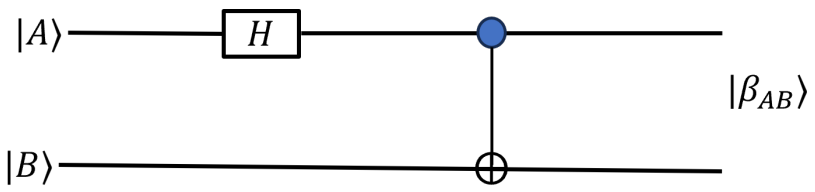


Figure 2.4: Circuit comprising a Hadamard (H) gate and a controlled not (CNOT) gate to generate the Bell states. Depending on the control qubit $|A\rangle$ and the target qubit $|B\rangle$, we generate the Bell state β_{AB}.

The Bell states can be generated by using two qubits, a Hadamard and C-NOT gate as shown in Fig. 2.4. The circuit begins with the control qubit $|A\rangle$ and the target

qubit $|B\rangle$. Let us consider the initial state $|A\rangle\,|B\rangle = |0\rangle\,|0\rangle$. The Hadamard gate is applied to the control qubit $|A\rangle$, creating a superposition state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Next, the CNOT gate is applied, which flips the state of the target qubit $|B\rangle$ if the control qubit $|A\rangle$ is in the state $|1\rangle$, is applied. This results in the entangled Bell state $\beta_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Depending on the initial states of $|A\rangle$ and $|B\rangle$, different Bell states can be generated.

2.2.8 Mixed States

Consider a case where the quantum state Q results from a random process, such that the state $|\psi_\alpha\rangle$ is prepared with a probability p_α. The possible states $|\psi_\alpha\rangle$ do not have to be orthogonal. This ensemble Q of such individual systems is called a mixed state.

Consider measuring an observable A on the system. For a particular subset of the ensemble where the system is in state $|\psi_\alpha\rangle$, the average value of the measurement for that state is given by $\langle A\rangle_\alpha = \langle\psi_\alpha|A|\psi_\alpha\rangle$. To find the average value over the entire ensemble, we need to consider the probability p_α of each state $|\psi_\alpha\rangle$. This gives us:

$$\langle A\rangle = \sum_\alpha p_\alpha \langle A_\alpha\rangle = \sum_\alpha p_\alpha \langle\psi_\alpha|A|\psi_\alpha\rangle\,. \tag{2.33}$$

Using $\text{Tr}(A\,|\psi_\alpha\rangle\langle\psi_\alpha|) = \langle\psi_\alpha|A|\psi_\alpha\rangle$, we get,

$$\begin{aligned}\langle A\rangle &= \sum_\alpha p_\alpha \text{Tr}(A\,|\psi_\alpha\rangle\langle\psi_\alpha|) \\ &= \text{Tr}(\hat{\rho}A).\end{aligned} \tag{2.34}$$

Where, $\hat{\rho}$ is the density operator defined as:

$$\hat{\rho} = \sum_{\alpha} p_\alpha |\psi_\alpha\rangle\langle\psi_\alpha|. \tag{2.35}$$

This density matrix ρ encapsulates the statistical mixture of the states.

2.2.9 Generalised states and measurements

Firstly, we discuss some mathematical prerequisites for understanding the general representation of quantum states and their measurements. These definitions are as follows:

- **Linear Operator:** Consider a complex vector space $\mathbb{C}^d$ of dimension d. A linear operator $L : \mathbb{C}^d \to \mathbb{C}^{d'}$ can be represented as a $d' \times d$ matrix,

$$L = \begin{pmatrix} L_{11} & L_{12} & \cdots & L_{1d} \\ L_{21} & \cdots & \cdots & L_{2d} \\ \vdots & \vdots & \ddots & \vdots \\ L_{d'1} & L_{d'2} & \cdots & L_{d'd} \end{pmatrix} \tag{2.36}$$

  where, $L_{ij} \in \mathbb{C}$ and the set of linear operators denoted as $\mathscr{L}(\mathbb{C}^d, \mathbb{C}^{d'})$

- **Hermitian Operator:** A linear operator $M \in \mathscr{L}(\mathbb{C}^d, \mathbb{C}^d)$ is Hermitian if $M^\dagger = M$. A hermitian operator has real eigenvalues ($\{\lambda_j\}$) for the orthonormal basis $\{\{v_j\}\}$. We can write a hermitian operator in its diagonalised form as: $M = \sum_j \lambda_j |v_j\rangle\langle v_j|$.

- **Positive Semi-definite Matrix:** A positive semi-definite matrix is a hermitian matrix having all the eigenvalues $\{\lambda_i\}_i$ as non-negative ($\lambda_i \geq 0$) and is denoted as $M \geq 0$

- **Trace of a matrix:** The trace of a matrix is given as:

$$tr(M) = \sum_j \langle v_j|M|v_j\rangle \,. \tag{2.37}$$

Density operator

The state vectors can only describe pure states. However, in many situations, we encounter mixtures of states. Density matrix formalism provides a generalized representation of pure and mixed states. It is also useful for dealing with subsystems of a non-separable (entangled) state. A density operator is a linear operator $\hat{\rho} \in \mathscr{L}(\mathbb{C}^d, \mathbb{C}^d)$ used to represent a quantum system in $\mathbb{C}^d$. In (2.35), we defined the density operator for a mixed state. It satisfies the following conditions:

1. $\hat{\rho} \geq 0$, meaning ρ is positive semi-definite, and
2. $\text{tr}(\hat{\rho}) = 1$, indicating that the trace of ρ is equal to 1.
3. $\mathbf{tr}(\hat{\rho}^2) \leq 1$. For pure states $\mathbf{tr}(\hat{\rho}^2) = 1$

POVMs

A positive operator valued measurement (POVM) on $\mathbb{C}^d$ is a set of positive semi-definite operators $\{M_x\}_{x\in X}$ such that

$$\sum_x M_x = \mathbb{I}_{\mathbb{C}^d},$$

where $\mathbb{I}_{\mathbb{C}^d}$ is the identity operator on $\mathbb{C}^d$. The subscript x labels the measurement outcome and the probability p_x of observing outcome x is:

$$p_x = \text{tr}(M_x\rho). \tag{2.38}$$

Kraus Operators

Consider a POVM operator, $M = \{M_x\}$ on C_d. A Kraus operator representation of M consists of a set of linear operators $A_x \in \mathscr{L}(\mathbb{C}^d, \mathbb{C}^d)$ such that $M_x = A_x^\dagger A_x$ for each x. Karus decomposition is the positive square root of M_x, i.e., $A_x = \sqrt{M_x}$. It is not unique since for any unitary U_x on $\mathbb{C}^d$, $A'_x = U_x\sqrt{M_x}$, is also a valid decomposition. If $M_x = |u_x\rangle\langle u_x|$ is a projector, then $\sqrt{M_x} = M_x$ and hence $A_x = M_x$

Post-Measurement state

Let ρ be a density matrix and $M = \{M_x\}$ a POVM with Kraus decomposition given by the operators $\{A_x\}$. If a measurement is performed and the outcome x is obtained, the state of the system after the measurement, conditioned on the outcome x, is given by

$$\rho_{|x} = \frac{A_x \rho A_x^\dagger}{\text{tr}(A_x^\dagger A_x \rho)}. \tag{2.39}$$

Projective Measurements

A projective measurement, also known as a von Neumann measurement, is defined by a set of orthogonal projectors $M_x = \Pi_x$ such that $\sum_x \Pi_x = \mathbb{I}$ and Kraus decomposition is $A_x = \Pi_x$. The probability q_x of obtaining the measurement outcome x is given by

$$q_x = \text{tr}(\Pi_x \rho), \tag{2.40}$$

and the post-measurement state is:

$$\rho_{|x} = \frac{\Pi_x \rho \Pi_x}{\text{tr}(\Pi_x \rho)}. \tag{2.41}$$

2.2.10 von Neumann entropy

The von Neumann entropy measures the uncertainty or disorder in a quantum system. For a density matrix ρ, it is defined as:

$$S(\rho) = -\text{Tr}(\rho \log_2 \rho). \tag{2.42}$$

If λ_x are the eigenvalues of ρ we also express von Neumann entropy as:

$$S(\rho) = -\sum_x \lambda_x \log \lambda_x. \tag{2.43}$$

The entropy quantifies the uncertainty or disorder in the system. For a pure state (where $\rho = |\psi\rangle\langle\psi|$), the entropy is zero, indicating no uncertainty. For mixed states, the entropy is positive, reflecting the average uncertainty or missing information about the system's precise state. Unlike classical entropy, quantum entropy can be influenced by entanglement. For example, in a maximally entangled pair of qubits, each qubit has an entropy of 1, but the combined system has zero entropy, illustrating that quantum entropy can be less for the whole system than for its parts due to entanglement.

2.2.11 No-Cloning Theorem

In 1982, W.K. Wootters and W.H. Zurek [34] showed that it is impossible to clone an unknown quantum state. We first define a cloning process, which consists of three aspects: the quantum state (ψ), the blank state ($|b\rangle$), and a quantum clone ($|M_b\rangle$). The joint state of the composite system is given as:

$$|\Psi\rangle = |\psi\rangle \otimes |b\rangle \otimes |M_b\rangle\,. \tag{2.44}$$

We consider that the entire system is informationally isolated, and the action of the quantum clone can be represented as a unitary time evolution operator U_c acting on the joint state of the composite system. After the cloning, the quantum state remains unchanged, and the blank state becomes an exact copy of the quantum state. The final state is:

$$|\Psi'\rangle = |\psi\rangle \otimes |\psi\rangle \otimes |M_\psi\rangle \,. \tag{2.45}$$

No Cloning Theorem: The no-cloning theorem implies that such a cloning machine, which can create identical copies of an arbitrary unknown quantum state, cannot exist. Here, we prove the no-cloning theorem. Consider two quantum states ϕ_1 and ϕ_2. The initial composite system for these states can be written as:

$$\begin{aligned} |\Phi_1\rangle &= |\phi_1\rangle \otimes |b\rangle \otimes |M_b\rangle \,, \\ |\Phi_2\rangle &= |\phi_2\rangle \otimes |b\rangle \otimes |M_b\rangle \,. \end{aligned} \tag{2.46}$$

After the cloning process, the final state is given as:

$$\begin{aligned} |\Phi_1'\rangle &= |\phi_1\rangle \otimes |\phi_1\rangle \otimes |M_{\phi_2}\rangle \,, \\ |\Phi_2'\rangle &= |\phi_2\rangle \otimes |\phi_2\rangle \otimes |M_{\phi_2}\rangle \,. \end{aligned} \tag{2.47}$$

Now consider a state ϕ_+ which is a superposition of the states ϕ_1 and ϕ_2.

$$|\phi_+\rangle = \frac{1}{\sqrt{2}}(|\phi_1\rangle + |\phi_2\rangle). \tag{2.48}$$

The composite state of Φ_+ before and after the cloning process is given by Φ_+ and Φ'_+, respectively.

$$|\Phi_+\rangle = |\phi_+\rangle \otimes |b\rangle \otimes |M_b\rangle \,, \tag{2.49}$$

$$|\Phi'_+\rangle = |\phi_+\rangle \otimes |\phi_+\rangle \otimes |M_{\phi_+}\rangle \,. \tag{2.50}$$

Using (2.47) and (2.48) in (2.49) we get:

$$\begin{aligned} |\Phi'_+\rangle &= \frac{1}{\sqrt{2}}(|\Phi'_1\rangle + |\Phi'_2\rangle) \\ &= \frac{1}{\sqrt{2}}(|\phi_1\rangle \otimes |\phi_1\rangle \otimes |M_{\phi_1}\rangle + |\phi_2\rangle \otimes |\phi_2\rangle \otimes |M_{\phi_2}\rangle). \end{aligned} \tag{2.51}$$

This is not the correct cloned state since Eq. (2.51) is not equal to (2.50). This concludes the proof of the no-cloning theorem.

2.3 Photonic Qubits and Polarization Encoding

Photons are an excellent resource for quantum information and communication protocols due to their ease of generation and manipulation. They are an indispensable part of communication systems and are often called "flying qubits". The development of efficient single-photon detectors has significantly simplified photonic quantum information processing. The versatility of photons in quantum information processing stems from the availability of multiple degrees of freedom, such as polarization, orbital angular momentum, path, position, momentum, time, or frequency, for carrying information. While all these modalities offer potential for information encoding, in our study, we utilize the polarization degree of freedom of photons.

2.3.1 Quantization of Electromagnetic Field

Quantization of the electromagnetic (EM) field involves treating the EM field as a collection of quantized harmonic oscillators, where each mode of the field corresponds to a quantized energy level. Photons are the elementary excitations of the normal mode of the field. We now start our discussion on field quantization. In free space, the electromagnetic field satisfies the classical Maxwell's equations:

$$\nabla \cdot \mathbf{E} = 0, \tag{2.52}$$

$$\nabla \cdot \mathbf{B} = 0, \tag{2.53}$$

$$\nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t}, \tag{2.54}$$

$$\nabla \times \mathbf{B} = \mu_0 \epsilon_0 \frac{\partial \mathbf{E}}{\partial t}. \tag{2.55}$$

The electric field $\mathbf{E}$ and magnetic field $\mathbf{B}$ can be expressed in terms of the vector potential $\mathbf{A}$. Specifically, the magnetic field is given by:

$$\mathbf{B} = \nabla \times \mathbf{A}. \tag{2.56}$$

The corresponding electric field can be derived from the vector potential using:

$$\mathbf{E} = -\nabla\phi - \frac{\partial \mathbf{A}}{\partial t}, \tag{2.57}$$

where ϕ is the scalar potential, which can be set to zero in the absence of free charges, simplifying the expression for $\mathbf{E}$, giving

$$\mathbf{E} = -\frac{\partial \mathbf{A}}{\partial t}. \tag{2.58}$$

Now, we impose the Coulomb gauge condition:

$$\nabla \cdot \mathbf{A} = 0. \tag{2.59}$$

Under these conditions, the vector potential $\mathbf{A}$ satisfies the wave equation:

$$\nabla^2 \mathbf{A} - \mu_0 \epsilon_0 \frac{\partial^2 \mathbf{A}}{\partial t^2} = 0. \tag{2.60}$$

Using $c^2 = \dfrac{1}{\mu_0 \epsilon_0}$, this simplifies to:

$$\nabla^2 \mathbf{A} - \frac{1}{c^2} \frac{\partial^2 \mathbf{A}}{\partial t^2} = 0. \tag{2.61}$$

This is a three-dimensional wave equation, and we can find electric and magnetic fields by finding the vector potential $\mathbf{A}$.

In a cubic box of side length L with periodic boundary conditions, the general solution for the vector potential can be written as a superposition of all possible modes:

$$\mathbf{A}(\mathbf{r},t) = \sum_{\mathbf{k},s} \mathbf{e}_{\mathbf{k}s} \left(A_{ks}(t) e^{i\mathbf{k}\cdot\mathbf{r}} + A^*_{ks}(t) e^{-i\mathbf{k}\cdot\mathbf{r}} \right). \tag{2.62}$$

$$A_{ks}(t) = A_{ks} e^{-i\omega_k t}. \tag{2.63}$$

$$\mathbf{A}(\mathbf{r},t) = \sum_{\mathbf{k},s} \mathbf{e}_{\mathbf{k}s} \left(A_{ks} e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} + A^*_{ks} e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} \right), \tag{2.64}$$

where the wave vectors $\mathbf{k}$ are quantized as:

$$\mathbf{k} = \frac{2\pi}{L}(n_x, n_y, n_z), \tag{2.65}$$

with n_x, n_y, and n_z being integers, and $\omega = c|\mathbf{k}|$. Each $\mathbf{k}$ has two independent polarization states denoted by s, with corresponding polarization vectors $\mathbf{e}_{\mathbf{k},s}$ and $\mathbf{e}_{\mathbf{k},s'}$. From the gauge condition of Eq. (2.59), we get,

$$\mathbf{k}\cdot\mathbf{e}_{\mathbf{k}s} = \mathbf{k}\cdot\mathbf{e}_{\mathbf{k}s'} = 0, \tag{2.66}$$

The polarization vectors $\mathbf{e}_{\mathbf{k},s}$ and $\mathbf{e}_{\mathbf{k},s'}$ are orthogonal to $\mathbf{k}$ and to each other,

$$\mathbf{e}_{\mathbf{k}s}\cdot\mathbf{e}_{\mathbf{k}s'} = \delta_{ss'}. \tag{2.67}$$

The electric and magnetic fields can be deduced from the solution for vector potential given in Eq. (2.64) using Eq. (2.58) and Eq. (2.56)

$$E(\mathbf{r},t) = i\sum_{\mathbf{k},s} \omega_k \mathbf{e}_{\mathbf{k},s} \left(A_{ks} e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} - A^*_{ks} e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} \right), \tag{2.68}$$

$$B(\mathbf{r},t) = \frac{i}{c}\sum_{\mathbf{k},s}\omega_k(\boldsymbol{\kappa}\times\mathbf{e}_{\mathbf{k},s})\left(A_{ks}e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} - A^*_{ks}e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)}\right). \quad (2.69)$$

where, $\boldsymbol{\kappa} = \mathbf{k}/|\mathbf{k}|$.

The Hamiltonian for the EM wave is given by:

$$H = \frac{1}{2}\int_V \left(\epsilon_0\mathbf{E}\cdot\mathbf{E} + \frac{1}{\mu_0}\mathbf{B}\cdot\mathbf{B}\right). \quad (2.70)$$

Using the periodic boundary condition and the solutions for the electric and magnetic fields we obtain the final Hamiltonian as:

$$H = 2\epsilon_0 V\sum_{\mathbf{k},s}\omega_k^2 A_{\mathbf{k},s}A^*_{\mathbf{k},s}. \quad (2.71)$$

We now introduce the canonical conjugate variables to quantize the system.

$$A_{\mathbf{k}s} = \frac{1}{2\omega_k(\epsilon_0 V)^{1/2}}\left[\omega_k q_{\mathbf{k}s} + ip_{\mathbf{k}s}\right], \quad (2.72)$$

$$A^*_{\mathbf{k}s} = \frac{1}{2\omega_k(\epsilon_0 V)^{1/2}}\left[\omega_k q_{\mathbf{k}s} - ip_{\mathbf{k}s}\right]. \quad (2.73)$$

Upon substitution of (2.72) and (2.73) in (2.71) we get:

$$H = \frac{1}{2}\sum_{\mathbf{k},s}\left(p^2_{\mathbf{k}s} + \omega_k^2 q^2_{\mathbf{k}s}\right). \quad (2.74)$$

The quantization of the field is achieved by requiring that the canonical variables transform into operators that obey the following commutation relations:

$$[\hat{q}_{\mathbf{k}s}, \hat{q}_{\mathbf{k}'s'}] = 0, \quad (2.75)$$

$$[\hat{p}_{\mathbf{k}s}, \hat{p}_{\mathbf{k}'s'}] = 0, \quad (2.76)$$

$$[\hat{q}_{\mathbf{k}s}, \hat{p}_{\mathbf{k}'s'}] = i\hbar\delta_{kk'}\delta_{ss'}. \quad (2.77)$$

We define the single-mode annihilation and creation operators as

$$\hat{a}_{\mathbf{k}s} = \frac{1}{(2\hbar\omega_k)^{1/2}} \left[\omega_k \hat{q}_{\mathbf{k}s} + i\hat{p}_{\mathbf{k}s}\right], \tag{2.78}$$

$$\hat{a}^{\dagger}_{\mathbf{k}s} = \frac{1}{(2\hbar\omega_k)^{1/2}} \left[\omega_k \hat{q}_{\mathbf{k}s} - i\hat{p}_{\mathbf{k}s}\right]. \tag{2.79}$$

and they satisfy,

$$[\hat{a}_{\mathbf{k}s}, \hat{a}_{\mathbf{k}'s'}] = 0, \tag{2.80}$$

$$[\hat{a}^{\dagger}_{\mathbf{k}s}, \hat{a}^{\dagger}_{\mathbf{k}'s'}] = 0, \tag{2.81}$$

$$[\hat{a}_{\mathbf{k}s}, \hat{a}^{\dagger}_{\mathbf{k}'s'}] = \delta_{\mathbf{k}\mathbf{k}'}\delta_{ss'}. \tag{2.82}$$

The total energy of the electromagnetic field is given by:

$$\hat{H} = \sum_{\mathbf{k}s} \hbar\omega_k \left(\hat{a}^{\dagger}_{\mathbf{k}s}\hat{a}_{\mathbf{k}s} + \frac{1}{2}\right) \tag{2.83}$$

$$= \sum_{\mathbf{k}s} \hbar\omega_k \left(\hat{n}_{\mathbf{k}s} + \frac{1}{2}\right), \tag{2.84}$$

where, $\hat{n}_{\mathbf{k}s}$ is the number operator for mode $\mathbf{k}s$.

$$\hat{n}_{\mathbf{k}s} = \hat{a}^{\dagger}_{\mathbf{k}s}\hat{a}_{\mathbf{k}s}. \tag{2.85}$$

Number states (Fock States)

Each of the modes is independent of each other and has eigenstate $|n_{\mathbf{k}s}\rangle$. Let us denote a single mode $\mathbf{k}s$ as j such that, $\hat{a}_{\mathbf{k}_j s_j} = \hat{a}_j$ and $\hat{a}^{\dagger}_{\mathbf{k}_j s_j} = \hat{a}^{\dagger}_j$. Then the Hamiltonian is,

$$\hat{H} = \sum_j \hbar\omega_j \left(\hat{n}_j + \frac{1}{2}\right). \tag{2.86}$$

The photon number state of multi modes is a product state of all the modes given as,

$$|n_1\rangle|n_2\rangle|n_3\rangle\ldots \equiv |n_1, n_2, n_3, \ldots\rangle = |\{n_j\}\rangle, \tag{2.87}$$

which is an eigenstate of $\hat{H}$ such that,

$$\hat{H}|\{n_j\}\rangle = E|\{n_j\}\rangle, \tag{2.88}$$

and the eigenvalue E is,

$$E = \sum_j \hbar\omega_j \left(n_j + \frac{1}{2}\right). \tag{2.89}$$

Each mode j is quantized with quanta of energy $\hbar\omega_j$.

Quantized electric and magnetic field

Based on the classical depiction of the electromagnetic field and the correspondence principle, the quantized electric and magnetic fields can be formulated using the non-Hermitian operators $\hat{a}$ and $\hat{a}^\dagger$:

$$\hat{\mathbf{E}}(\mathbf{r}, t) = \sum_{\mathbf{k},s} \sqrt{\frac{\hbar\omega_k}{2\epsilon_0 V}} \mathbf{e}_{\mathbf{k}s} \left(i\hat{a}_{\mathbf{k}s} e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} + \text{H.c.}\right), \tag{2.90}$$

$$\hat{\mathbf{B}}(\mathbf{r}, t) = \frac{1}{c}\sum_{\mathbf{k},s} (\boldsymbol{\kappa} \times \mathbf{e}_{\mathbf{k},s}) \sqrt{\frac{\hbar\omega_k}{2\epsilon_0 V}} \mathbf{e}_{\mathbf{k}s} \left(i\hat{a}_{\mathbf{k}s} e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} + \text{H.c.}\right), \tag{2.91}$$

where, H.c. stands for hermitian conjugate.

2.3.2 Coherent States

The coherent states are the eigenstates of annihilation operator $a^\dagger$, satisfying,

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle\,. \tag{2.92}$$

where, α is a complex eigenvalues, since $\hat{a}$ is a non-hermitian operator. We also have,

$$\langle\alpha|\,\hat{a^\dagger} = \alpha^*\,\langle\alpha|\,. \tag{2.93}$$

The number states $|n\rangle$ form a complete set and the coherent state is defined as a superposition of these Fock states as,

$$|\alpha\rangle = e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle. \tag{2.94}$$

The probability $P(n)$ of having n photons in a coherent state is obtained by evaluating $\langle n|\alpha\rangle$

$$\begin{aligned}\langle n|\alpha\rangle &= e^{-\frac{|\alpha|^2}{2}}\sum_{m=0}^{\infty}\frac{\alpha^m}{\sqrt{m!}}\langle n|m\rangle \\ &= e^{-\frac{|\alpha|^2}{2}}\frac{\alpha^n}{\sqrt{n!}},\end{aligned} \tag{2.95}$$

where, we have used orthonormality ($\langle n|m\rangle = \delta_{nm}$) of number states. Thus,

$$P(n) \equiv |\langle n|\alpha\rangle|^2 = e^{-|\alpha|^2}\frac{|\alpha|^{2n}}{n!}. \tag{2.96}$$

The mean photon number μ in a coherent state is found using the expectation value of $\hat{n}$,

$$\mu \equiv \langle\alpha|\hat{n}|\alpha\rangle = \langle\alpha|\hat{a}^\dagger\hat{a}|\alpha\rangle = \langle\alpha|\alpha^*\alpha|\alpha\rangle = \alpha^*\alpha. \tag{2.97}$$

Using (2.96) and (2.97) we get,

$$P(n) = \frac{\mu^n}{n!}\mathrm{e}^{-\mu}. \tag{2.98}$$

Hence, we conclude that a coherent state follows the Poissonian distribution.

2.3.3 Polarization

Maxwell's wave theory provides the classical framework for understanding light polarization. According to this theory, the direction of the electric field vector within the electromagnetic wave determines the polarization state. Different types of polarization arise depending on the orientation and relative amplitudes of the electric field's components in the transverse plane. Consider the plane wave propagating along z direction with wave-vector k,

$$E = \hat{x}E_x e^{(-i(\omega t - kz))} + \hat{y}E_y e^{(-i(\omega t - kz))} e^{i\phi}, \tag{2.99}$$

where, E_x and E_y are amplitudes of electric field in x and y direction and ϕ is the phase between the electric field components along x and y direction.

- **Linear Polarization:** The electric field oscillates in a single, fixed direction. Light with fields predominantly in the x or y direction is termed horizontally or vertically polarized, respectively. (ϕ = 0)
- **Circular Polarization:** The electric field vector rotates about the propagation axis as the wave advances. This rotation is classified as right-circular or left-circular, depending on the direction of rotation. ($\phi = \pi/2$, $E_x = E_y$)
- **Elliptical Polarization:** Similar to circular polarization, the electric field rotates during propagation but with unequal amplitudes in its orthogonal components, resulting in an elliptical trajectory. ($\phi \neq 0$, $\phi \neq \pi/2$)
- **Unpolarized Light:** The electric field vector lacks a defined direction and oscillates randomly.

The direction of the electric field vector determines the polarization state. In the

quantized description of the electromagnetic fields, mode operators are associated with the classical field's quantum version. Photons, excitations of the quantized fields, inherit the properties inherent in the classical description. Hence, photon polarization can be treated similarly to the polarization of classical fields.

2.3.4 Polarization Basis

Within this discussion, we focus on utilizing the degree of freedom of polarization to encode and generate qubits.

First, we establish the definitions of polarizations that are about to be used. We consider the wave propagation in the z-direction, with the transverse plane being the x and y. If the electric field points in the x direction, we call it horizontally (H) polarized light; if it points in the y direction, we call it vertically (V) polarized light. We call these rectilinear polarizations, and the Jones vector used to represent these polarization states are:

$$|H\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \tag{2.100}$$

$$|V\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2.101}$$

We further define diagonal and anti-diagonal polarizations for the electric field direction at an angle of $45°$ and $-45°$, with x axis, respectively. We call these diagonal polarizations, and their Jones vector representations are:

$$|D\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \tag{2.102}$$

$$|A\rangle \;=\; \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} \tag{2.103}$$

Acknowledging that any arbitrary polarization state can be effectively constructed through a linear superposition of its basis vectors is crucial. The Jones matrices have a one-to-one correspondence to the basis vectors defined for the qubit states defined in Sec. 2.2.3, where,

- The rectilinear basis aligns with the standard basis, where the states $|0\rangle$ and $|1\rangle$ correspond to $|H\rangle$ and $|V\rangle$ respectively.

- The diagonal basis aligns with the Hadamard basis, where the states represent an equal superposition of horizontal and vertical polarization ($|+\rangle$ & $|-\rangle$) (Eq. (2.16)).

By employing the basis and leveraging the power of superposition, we unlock the potential to encode and manipulate information using the polarization of light, creating the foundation for various quantum information processing applications.

2.3.5 Manipulating Polarization of Photons

Under free-space propagation, the polarization state of light remains unchanged. However, certain anisotropic materials can alter it. These materials possess birefringence, i.e. they have different refractive indices for two orthogonal polarization components (ordinary and extraordinary). Birefringent materials are basic to various optical elements like polarizers, quarter-wave plates, and half-wave plates that manipulate the polarization state.

Polarizers

A polarizer allows only a specific polarization to pass through. Suppose that a polarizer is oriented at 0° with x axis. It lets only the H polarization pass through and completely blocks the V polarization. The Jones matrix of such a polarizer is:

$$U_{p_0} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \tag{2.104}$$

A polarizer kept at an angle θ with the x axis is given as:

$$U_{p_\theta} = R(\theta) U_{p_0} R(-\theta) \tag{2.105}$$

where, $R(\theta)$ is the rotation matrix given by:

$$R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \tag{2.106}$$

Using Eq. (2.104), Eq. (2.106) and Eq. (2.105) we get:

$$U_{p_\theta} = \begin{pmatrix} \cos^2\theta & \sin\theta\cos\theta \\ \sin\theta\cos\theta & \sin^2\theta \end{pmatrix} \tag{2.107}$$

Wave plates

Waveplates are also known as retarders since they slow down one component of polarization with respect to the other. Jones matrix for waveplates with its fast axis aligned to H polarisation is given by:

$$U_W = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{pmatrix} \tag{2.108}$$

Half-wave Plates (HWP)

A half-wave plate (HWP) introduces a phase of $\lambda/2$ between the two orthogonal components of polarization aligned along its fast and slow axis. The Jones matrix for a HWP kept with its fast axis aligned to H polarization is:

$$U_{hwp_0} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.109}$$

The Jones matrix for a HWP kept with its fast axis at an angle θ to H polarization is:

$$\begin{aligned} U_{hwp_\theta} &= R(\theta)U_{hwp_0}R(-\theta) \\ &= \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix} \end{aligned} \tag{2.110}$$

Quarter-Wave Plates (QWP)

A quarter-wave plate (HWP) introduces a phase of $\lambda/4$ between the two orthogonal components of polarisation aligned along its fast and slow axis. The Jones matrix for a QWP kept with its fast axis aligned to H polarisation is:

$$U_{qwp_0} = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} \tag{2.111}$$

The Jones matrix for a QWP kept with its fast axis at an angle θ to H polarization is:

$$U_{qwp_\theta} = R(\theta)U_{qwp_0}R(-\theta) \tag{2.112}$$

$$= \begin{pmatrix} \cos^2\theta + i\sin^2\theta & (1-i)\sin\theta\cos\theta \\ (1-i)\sin\theta\cos\theta & \sin^2\theta + i\cos^2\theta \end{pmatrix}$$

We can choose different angles θ of HWP and QWP to get the desired polarization of the photon. These act as the quantum operators for manipulating our photonic qubits in polarization degree of freedom. For example, $HWP@45°$ and $HWP@22.5°$ act as bit flip and phase flip operators for rectilinear polarization.

2.4 Quantum Key Distribution

Most QKD protocols are classified into Prepare & Measure QKD and entanglement-based QKD (Fig. 1.5). Prepare and measure protocols depend on measurement uncertainty to ensure the secrecy of the key. The entanglement-based protocols leverage the non-local correlations to ensure communication security. Our work focuses on prepare and measure based QKD using polarization degree of freedom in two mutually unbiased bases.

A general prepare and measure QKD protocol involves two main phases: quantum communication and classical post-processing. Alice encodes her random bits in quantum states during quantum communication and sends them to Bob via the quantum channel, such as optical fibre or free space. Eve can intercept this quantum channel to access the information. However, due to the principles of quantum mechanics, Eve cannot perfectly clone the quantum states, and any attempt to gain information disturbs the quantum state. Bob measures the received signal and records bit values.

Alice and Bob perform sifting, keeping only the bits measured in the same basis and discarding those measured in different bases. They then use a portion of the raw data for parameter estimation and conduct error correction (EC) to detect and

fix errors, which is followed by privacy amplification (PA) to minimize the information Eve can extract. We get the final secret key after the quantum communication and classical post-processing. There are two methods for reconciliation: direct reconciliation (DR) or reverse reconciliation (RR). In DR, Bob processes his outcomes to infer Alice's encoding, assisted by forward classical communication (CC) from Alice. In RR, Alice processes her encoding to infer Bob's outcomes, assisted by backward CC from Bob.

Although Eve cannot alter the messages on the authenticated classical channel, she can read all the information without any consequences. Ultimately, the key generated at the end of the QKD protocol emerges from the interactions among Alice, Bob, and Eve. Here, we assume that Alice and Bob exchange an infinite number of states, i.e. the asymptotic limit. The asymptotic key rate can be determined by the difference in mutual information I among the involved parties, as per Csiszar and Korner's classical theorem [57]. In direct reconciliation (DR) and reverse reconciliation (RR) key rate is given as,

$$\begin{aligned} R_{DR} &:= I(A:B) - I(A:E) \\ R_{RR} &:= I(A:B) - I(B:E) \end{aligned} \tag{2.113}$$

We now discuss the steps involved in quantum key distribution, specifically the quantum communication and classical post-processing phases, in detail.

Encoding and Decoding

First, Alice encodes the qubits in the desired degree of freedom, say polarization, by randomly between two non-orthogonal bases. She then transmits the prepared state via a quantum channel to Bob. Bob then makes a choice between the mutually unbiased basis and takes the measurement. The key generated after this is the raw

key R_{raw}.

Sifting

Alice and Bob utilize a public channel to disclose which basis they employed to prepare or measure their qubits and the timing of detection events. However, they refrain from disclosing the measurement results. When Alice and Bob employ the same basis, they should obtain perfectly correlated bits. Discarding bits when different bases are used is termed as **sifting**. The collection of bits remaining after this basis reconciliation constitutes the sifted key of length n_s. If N_t number of bits are transmitted, and s is the sifting parameter [58], then the sifted key generation rate is given as:

$$R_{\text{sifted}} = sR_{\text{raw}} \tag{2.114}$$

The sifted key length, n_s is given as,

$$n_s = N_t R_{\text{sifted}} \tag{2.115}$$

Error Correction and Privacy Amplification

If an adversary attempts to intercept the key, it will induce errors in the system. However, practical implementations often encounter errors due to imperfections in the devices used. Unfortunately, discerning between errors caused by the system and those due to eavesdropping is infeasible. Consequently, solely relying on the premise that any eavesdropping will inevitably lead to errors and expose the intrusion is insufficient as security proof in practical systems.

The Quantum Bit Error Rate (QBER) serves as a key metric in quantum communication, gauging the frequency of errors in transmitted quantum bits (qubits). QBER

denotes the probability that a qubit sent between parties is received inaccurately due to channel noise or adversarial interference. Lower QBER values signify enhanced fidelity and security in quantum communication setups.

Practical QKD systems mitigate system errors and potential eavesdropping by incorporating two vital additional procedures: **error correction** and **privacy amplification**. Both of these steps can be conducted using a public channel. Error correction aims to ensure that Alice and Bob possess the same key, while privacy amplification focuses on ensuring their shared key's confidentiality.

Error correction enables the estimation of the error rate, denoted as e, and subsequently corrects errors at the cost of a few bits. The minimum number of bits (κ) to be exchanged publicly to perform error correction [55].

$$\lim_{n_s \to \infty} \frac{\kappa}{n_s} = -e \log_2 e - (1-e) \log_2 (1-e) \equiv h(e) \tag{2.116}$$

The inefficiency of practical error correction algorithms is accounted by $f(e)$, thus Eq. (2.116) is rewritten as:

$$\lim_{n_s \to \infty} \frac{\kappa}{n_s} = -f(e) \left[e \log_2 e + (1-e) \log_2 (1-e) \right] \equiv f(e) h(e) \tag{2.117}$$

Privacy amplification compresses the error-corrected key into a final secure key, adjusting for potential information leakage to the eavesdropper during prior transmission phases. It is conducted using generalized privacy amplification theory [59], assuming that all errors are potentially attributed to eavesdropping. It states that the length of the final key is:

$$r = n_s \tau - \kappa - t \tag{2.118}$$

where, n_s is sifted key length, κ is the number of bits disclosed during error correc-

tion, t is the security parameter and τ is the shrinking factor given by:

$$\tau = -\frac{\log_2 p_c}{n_s} \tag{2.119}$$

where p_c is the average collision probability, quantifying Eve's mutual information with Alice and Bob. The parameter t quantifies the level of security by determining how much information about the final key can be known by an eavesdropper. The security parameter t ensures that the eavesdropper's probability of successfully guessing the key is at most 2^{-t}. Given N_t as the total number of transmitted bits, n_s as the number of sifted bits, and r as the length of the secure key, we can determine the secure key generation rate R using Eq. (2.115) and Eq. (2.118). The secure key generation rate R is expressed as:

$$R = \lim_{N_t \to \infty} \frac{r}{N_t} = \lim_{n_s \to \infty} R_{\text{sifted}} \left(\tau - \frac{\kappa}{n_s} - \frac{t}{n_s} \right). \tag{2.120}$$

As the length of n_s becomes very large, it can be shown that $\dfrac{t}{n_s} = 0$. Using Eq. (2.117) we get the secure key rate as,

$$R = R_{\text{sifted}} \left(\tau - f(e) h(e) \right). \tag{2.121}$$

The values of R_{sifted} and τ depend on the system parameters and the QKD protocol.

2.4.1 Security of QKD

In 1999, Lo and Chau [14] gave a security framework for QKD based on entanglement distillation. Later on, Shor and Preskill [16] employed Calderbank Shor Steane (CSS) code [60, 61] simplifying entanglement-based security proof for prepare and measure protocol. Significant contributions to the security proofs of QKD were made by Biham et al. (2000) [62], Mayers (2001) [18], Devetak and Winter

(2005)[63], and Koashi (2009) [64]. The concept of composable security was integrated into quantum cryptography, establishing a rigorous definition of secure keys in [65, 66]. Further, the effects due to finite key size were addressed in security proofs by Renner [67], Scarani [68], and Tomamichel [69].

In an ideal scenario where the QKD protocol is flawless, without implementation errors or eavesdropping, the resulting sifted key would be perfectly secure. However, practical QKD implementations often encounter errors due to imperfections in the devices used. Security analyses have thoroughly investigated device imperfections in practical QKD systems, with foundational work by Lütkenhaus (2000) [17]; Inamori, Lütkenhaus, and Mayers (2007) [51]; and Gottesman et al. (2004) [19] that established a significant framework for analyzing realistic devices.

New protocols were developed to address these imperfections, including the decoy state protocol [70–73], the differential phase shift protocol [24], the Scarani-Acín-Ribordy-Gisin (SARG) protocol [25], the coherent one-way (COW) protocol [26], and the measurement-device-independent (MDI) protocol [53]. Notably, the decoy state protocol allows secure QKD using weak coherent pulses, and the MDI protocol eliminates all detection side channels.

Security Criteria

To establish the security of QKD, we first need to define the security criteria. Ideally, a secure key must meet two conditions: **1. Correctness** i.e. the key bit strings shared between Alice and Bob are identical; **2. Secrecy** i.e. the key bit string shared between Alice and Bob remains secret, unknown to the adversary.

Let k_A and k_B be the key bit strings for Alice and Bob, respectively, and ρ_E represent Eve's quantum state. In an ideal scenario, $k_A = k_B = k$ (ensuring correctness),

and ρ_E is independent of k (ensuring secrecy). The classical-classical-quantum (c-c-q) state of Alice, Bob, and Eve is described by:

$$\rho_{ABE}^{\text{ideal}} = 2^{-m} \sum_{k} |k\rangle_A\langle k| \otimes |k\rangle_B\langle k| \otimes \rho_E. \tag{2.122}$$

However, in practical situations, k_A may not equal k_B, and Eve might be correlated with the key. Thus, the joint c-c-q state is:

$$\rho_{ABE} = \sum_{k_A,k_B} P(k_A,k_B)|k_A\rangle\langle k_A| \otimes |k_B\rangle\langle k_B| \otimes \rho_E^{(k_A,k_B)}. \tag{2.123}$$

where, $P(k_A,k_B)$ is the probability distribution of the final state ρ_{ABE}. Due to practical limitations such as finite data size and imperfect error correction, Alice and Bob cannot always produce a perfect key. Instead, it is reasonable to allow for a small failure probability [65, 66]. If the key bit strings shared between Alice and Bob are identical, with a failure probability of ϵ_{corr} and remain secret with a failure probability of ϵ_{sec}, then A QKD protocol is considered ϵ secure. Where, ϵ is the overall failure probability given by $\epsilon = \epsilon_{corr} + \epsilon_{sec}$.

The key concept of composable security [65, 66] is to define a perfectly secure ideal protocol and then prove that the real protocol is almost identical to the ideal one in every possible scenario. The measure of distinguishability is the trace distance between the ideal ($\rho_{ABE}^{\text{ideal}}$) and real state ($\rho_{ABE}$). The composable security of QKD protocol [65] is defined as ϵ secure if:

$$\min_{\rho_E} \frac{1}{2}(1 - p_{\text{abort}})\|\rho_{ABE} - \rho_{ABE}^{\text{ideal}}\|_1 \leq \epsilon \tag{2.124}$$

where p_{abort} is the probability of aborting the protocol and $\|A\|_1 \equiv Tr[\sqrt{A^\dagger A}]$ is the trace norm.

The expressions of key rates in (2.113) and (2.120) account for the non-ideal sce-

narios; however, they fail to model all the device imperfections. Modelling these device imperfections and including them in the key rate requires rigorous knowledge about their workings and is outside the scope of this work. Here we have measured the vulnerabilities of the devices used and quantified their side channel, which helps to precisely estimate the key. This can be quantified by calculating the mutual information between Alice and Eve or Bob and Eve by knowing the vulnerabilities in the system. The modified key rates, according to Csiszar and Korner [57], will be

$$R = I(A:B) - I(A:E) - I_s(A,B:E) \tag{2.125}$$

$I_s(A,B:E)$ is the information leakage due to a side channel arising from system vulnerabilities at Alice and Bob's end. This thesis aims to quantify this information leakage, be it due to device imperfections at the source or the detector. Additionally, it gives estimates on the key rate in real implementation.

2.4.2 Strategies for Eavesdropping

QKD protocols have been extensively studied for their security against various types of attacks. Initially, the BB84 protocol addressed intercept and resend attacks, wherein an eavesdropper intercepts qubits sent by the sender, measures them, and then resends them to the intended receiver. As illustrated in Fig. 2.5, if Eve performs such an attack, it will introduce an error of about 25%. The upper limit on the error for BB84 is 11%. Hence, Alice and Bob will detect the interception.

Subsequent exploration of generalized delayed measurements led to the identification of three categories of attacks: individual, collective, and coherent.

- Individual Attacks: In individual attacks (Fig. 2.6(a)), Eve entangles a quan-

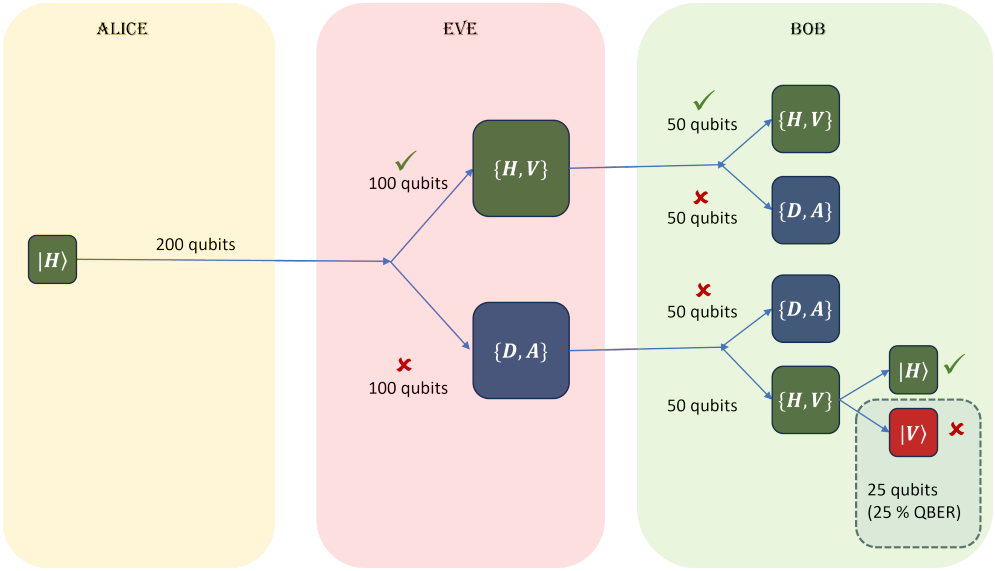


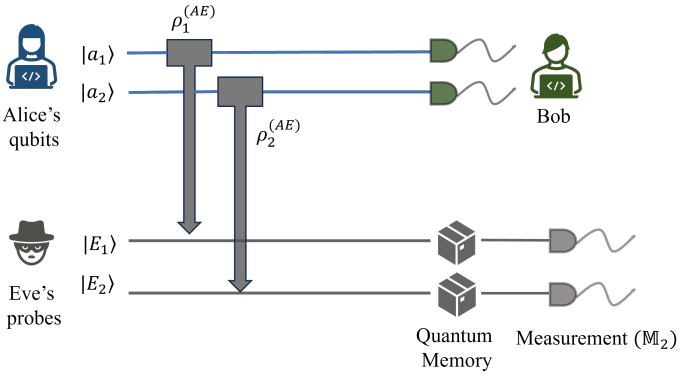
Figure 2.5: Intercept Resend Attack: Alice sends qubits, Eve randomly selects basis with 50% probability and sends the measured qubit to Bob. In such a case, Alice and Bob find 25% QBER, greater than the acceptable 11%. The protocol is discarded.

tum probe with each qubit independently and stores them until the measurement basis is announced.

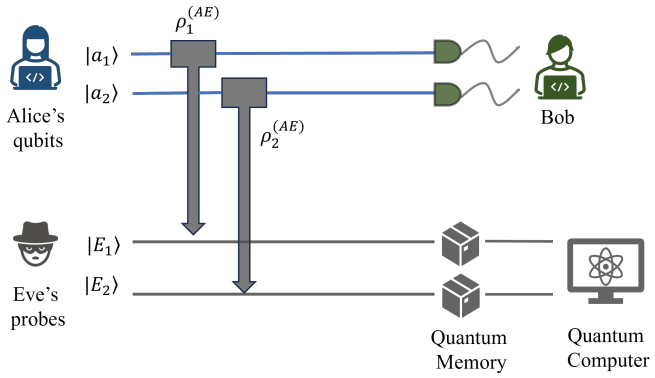
- Collective Attacks: Collective attacks (Fig. 2.6(b)) are similar to individual attacks but permit Eve to perform a global generalized measurement on all probes as a single quantum system using a quantum computer.

- Coherent Attacks: Coherent attacks (Fig. 2.6(c)) consider the entire quantum transmission as one system entangled with a probe of large dimensionality.

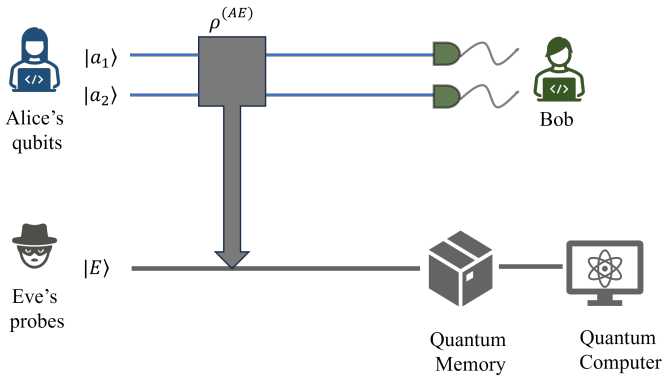
This study will concentrate on practical quantum communication systems, acknowledging that current and foreseeable technology cannot perform coordinated or coherent attacks. Since future eavesdropping methods cannot break present quantum transmissions, we will address individual attacks in our thesis.



(a) Individual Attack



(b) Collective Attack



(c) Coherent Attack

Figure 2.6: Attacks on Quantum Key Distribution: (a) individual, (b) collective and (c) coherent attack strategies of an adversary.

2.4.3 BB84 Protocol

Stephen Wiesner first proposed the concept of quantum cryptography in 1983 [74], and it gained renewed attention when Charles H. Bennett and Gilles Brassard introduced the first quantum key distribution (QKD) protocol in 1984, famously known as the BB84 protocol [20]. In our implementation of the BB84 protocol, Alice generates qubit states by encoding single photons in a polarisation degree of freedom and sends them to Bob. Fig. 2.7 represents a schematic diagram of the protocol.

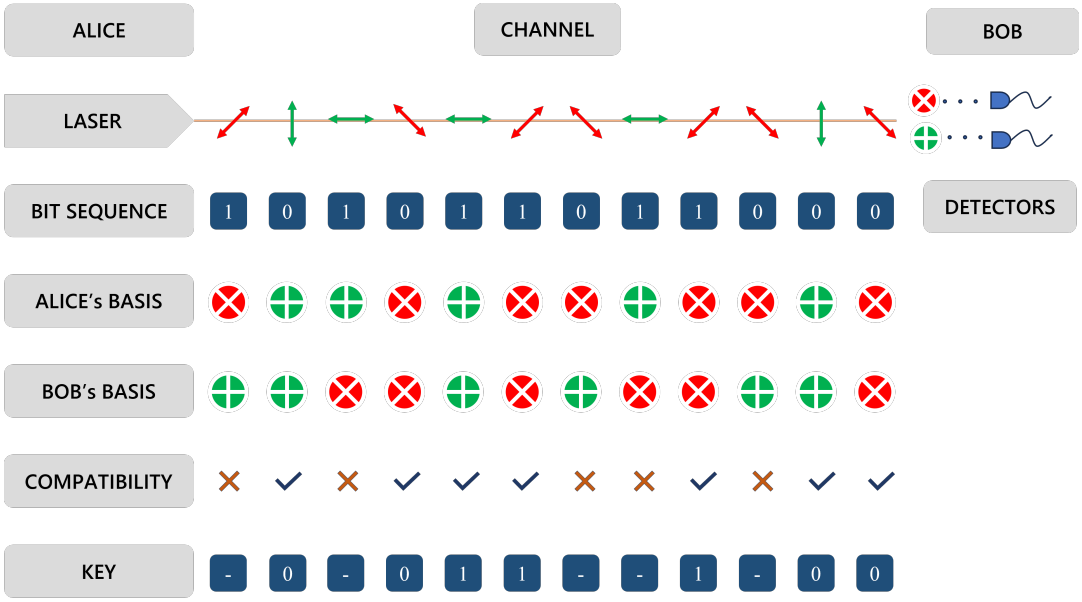


Figure 2.7: Schematics for Standard BB84 Protocol depicting the basis choice of Alice and Bob, the encoded bit and the check for compatibility of basis choice. Only the bits of compatible basis form the sifted key.

Protocol. *The systematic steps of the BB84 Protocol are listed below:*

1. *Set* $i = 0$. *Here, i is a variable that tracks the current round number.*
2. ***State Preparation (Alice's Lab):*** *Alice generates random numbers* $\mathcal{X}_i \in \{0, 1\}$, $\mathcal{A}_i \in \{0, 1\}$. *She first decides between the two Mutually Unbiased*

basis (MUBs) depending on the outcome of $\mathcal{X}_i$, and then she encodes her photon in any one degree of polarization as the qubit $\mathcal{A}_i$.:

(a) When, $\mathcal{X}_i = 0$, then she prepares her state in the Standard basis (H/V or 0/1).

i. $\mathcal{A}_i = 0$, she encodes in H polarisation.

ii. $\mathcal{A}_i = 1$, she encodes in V polarisation.

(b) When, $\mathcal{X}_i = 1$, then she prepares her state in the Hamadard basis (D/A or +/-).

i. $\mathcal{A}_i = 0$, she encodes in D polarisation.

ii. $\mathcal{A}_i = 1$, she encodes in A polarisation.

3. ***State transmission:*** *Alice sends the prepared state to Bob through the quantum channel.*

4. ***State measurement (Bob's lab):*** *Bob generates a random bit $\mathcal{Y}_i$, which decides the measurement basis.*

(a) If, $\mathcal{Y}_i = 0$, then he measures the qubit in the Standard basis (H/V or 0/1).

(b) If $\mathcal{Y}_i = 1$, then he measures the qubit in the Hadamard Basis.

After the measurement, Bob gets a bit $\mathcal{B}_i$

5. *Proceed to step 1 unless i equals n, and set $i = i + 1$. Proceed to the next step otherwise. Here, n represents the total number of rounds for the protocol.*

6. *Alice and Bob publicly disclose the value of the bits $(\mathcal{X}_1, \mathcal{X}_2, \cdots, \mathcal{X}_n)$ and $(\mathcal{Y}_1, \mathcal{Y}_2, \cdots \mathcal{Y}_n)$ respectively. They discard the rounds in which $\mathcal{X}_i \neq \mathcal{Y}_i$ - i.e. they only focus on the rounds from the set $\mathfrak{h} := \{i \in \{1, 2, \cdots n\} : \mathcal{X}_i = \mathcal{Y}_i\}$.*

7. *From any randomly chosen subset* $\mathfrak{g} \subset \mathfrak{h}$*, with* $|\mathfrak{g}| \ll |\mathfrak{h}|$ *they estimate QBER (the probability that* $\mathcal{A}_i \neq \mathcal{B}_i$ *whenever* $\mathcal{X}_i = \mathcal{Y}_i$ *):*

$$E \;:=\; \frac{|\{i \in \mathfrak{g} : \mathcal{A}_i \neq \mathcal{B}_i\}|}{|\{i \in \mathfrak{g}\}|} \tag{2.126}$$

8. *If* $E \geq 11\%$*, they discard the protocol. Otherwise, they proceed to the classical post-processing and perform error correction and privacy amplification.*

2.4.4 Encoding Photons with Polarization

The above-mentioned QKD protocol is typically implemented using the polarization of single photons as the qubits. Such an implementation is made possible using a combination of waveplates and polarizers. In our QKD scheme, utilizing four lasers (Fig. 2.8), we encode our quantum states using the states $|H\rangle$, $|V\rangle$, $|D\rangle$, and $|A\rangle$. Here, $|D\rangle$ and $|A\rangle$ are defined as superpositions of $|H\rangle$ and $|V\rangle$, where,

$$\begin{aligned} |D\rangle &= \frac{(|H\rangle + |V\rangle)}{\sqrt{2}}, \\ |A\rangle &= \frac{(|H\rangle - |V\rangle)}{\sqrt{2}}. \end{aligned} \tag{2.127}$$

Each laser emits pulses randomly at a rate of 1.25 MHz. Polarizing beam splitters (PBS) are utilized in our setup to transmit $|H\rangle$ states and reflect $|V\rangle$ states. Additionally, half-wave plates (HWP) set at 22.5 degrees serve to transform $|H\rangle$ states into $|D\rangle$ states and $|V\rangle$ states into $|A\rangle$ states. This configuration enables us to efficiently encode and manipulate quantum information for secure communication protocols.

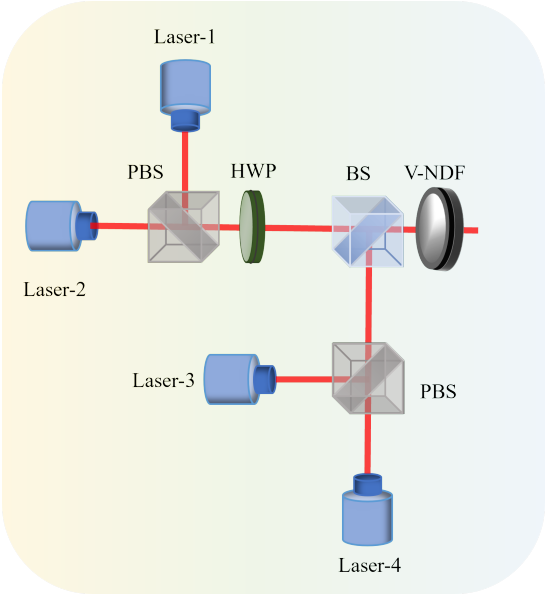
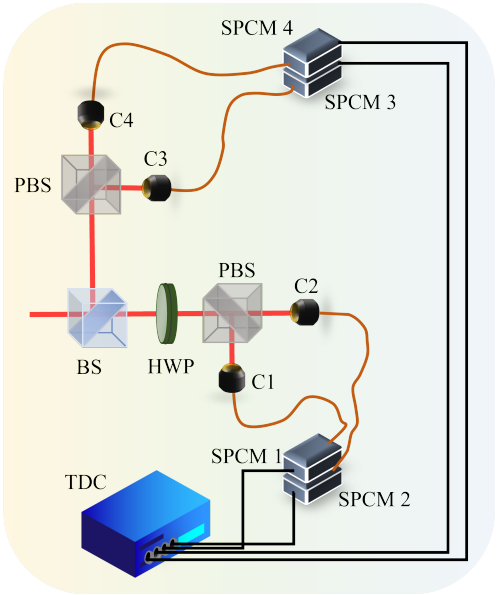


Figure 2.8: Polarisation Encoding Setup: Laser 1,2,3,& 4; PBS: polarising beam splitter; HWP: half wave plate, BS: beam splitter; V-NDF: variable neutral density filter.



SPCM	State
1	$\|A\rangle$
2	$\|D\rangle$
3	$\|V\rangle$
4	$\|H\rangle$

Figure 2.9: Polarisation Decoding: BS: beam splitter; HWP: half-wave plate; PBS: polarising beam splitter; C: coupler; SPCM: single photon counting module; TDC: time to digital converter.

2.4.5 Decoding Polarisation of Photons

In our QKD decoding scheme (Fig. 2.9), a beam splitter (BS) randomly selects the basis for measurement. We decode our quantum states in two different basis: $\{|H\rangle, |V\rangle\}$ and $\{|D\rangle, |A\rangle\}$. A polarizing beam splitter (PBS) is employed to transmit $|H\rangle$ states and reflect $|V\rangle$ states. Furthermore, half-wave plates (HWP) set at 22.5 degrees transform $|H\rangle$ states into $|D\rangle$ states and $|V\rangle$ states into $|A\rangle$ states. Photons from the quantum channel are coupled to single-photon counting modules (SPCMs) via couplers C_1, C_2, C_3, and C_4. Finally, the time-to-digital converter (TDC) records the timing information of photon detections.

2.4.6 BB84 Protocol with Weak Coherent Pulses

Weak coherent pulses are generally used in the practical implementation of the BB84 protocol. When these coherent pulses are encoded in polarisation degree of freedom, we represent them as $|\alpha, \mathbf{e_k}\rangle$, where $\mathbf{e_k}$ is the polarisation degree of freedom.

Source

Alice sends phase-randomized weak coherent pulses. The state ρ emitted by Alice can be represented as a mixture of coherent states $|\alpha e^{i\theta}, \mathbf{e_k}\rangle$, with θ phase as,

$$\rho = \frac{1}{2\pi}\int_0^{2\pi} |\alpha e^{i\theta}, \mathbf{e_k}\rangle \langle \alpha e^{i\theta}, \mathbf{e_k}| \, d\theta \tag{2.128}$$

The coherent state $|\alpha e^{i\theta}, \mathbf{e_k}\rangle$ can be expressed in terms of number states $|n, \mathbf{e_k}\rangle$ as follows:

$$|\alpha e^{i\theta}, \mathbf{e_k}\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{(\alpha e^{i\theta})^n}{\sqrt{n!}} |n, \mathbf{e_k}\rangle$$

$$= e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n e^{in\theta}}{\sqrt{n!}} |n, \mathbf{e_k}\rangle \tag{2.129}$$

Substituting this expression into the density matrix ρ, we get,

$$\begin{aligned} \rho &= e^{-|\alpha|^2} \sum_{n=0}^{\infty} \frac{|\alpha|^{2n}}{n!} |n, \mathbf{e_k}\rangle\langle n, \mathbf{e_k}| \\ &= \sum_{n=0}^{\infty} P(n) |n, \mathbf{e_k}\rangle\langle n, \mathbf{e_k}| \end{aligned} \tag{2.130}$$

where $P(n) = e^{-|\alpha|^2} \frac{|\alpha|^{2n}}{n!}$ represents the probability of finding the system in the n-th number state. Using (2.96) and (2.97) we get,

$$P(n) = \frac{\mu^n}{n!} \mathrm{e}^{-\mu}. \tag{2.131}$$

where μ is the mean photon number.

Channel

The encoded qubits can be transmitted from Alice to Bob either using a free space channel or an optical fibre-based channel. The losses in the free space quantum channel are mainly due to the geometrical loss due to beam divergence and the different transmitter and receiver aperture sizes. The other cause in the free space is atmospheric loss due to absorption and scattering. The transmittance in free space t_{FS} is thus given as:

$$t_{FS} = \eta_{GL} \cdot \eta_{AL} \tag{2.132}$$

where, η_{GL} is geometric loss factor and η_{AL} is atmospheric loss factor.

The loss in the fiber-based channel is characterised by the loss coefficient α' measured in dB/km, channel length l and the channel transmittance t_{FB} is given as,

$$t_{FB} = 10^{-\alpha' l/10} \tag{2.133}$$

We adopt identical notations and formalism as presented in [73] for congruence. Depending on the type of channel used we get the channel transmittance between Alice and Bob as t_{AB}

Detector

We define the efficiency at Bob as η_{Bob}, which includes the transmittance of the optical components as well as the detection efficiency. Then the overall efficiency η for detection by Bob of a single photon sent by Alice is,

$$\eta = t_{AB} \cdot \eta_{Bob} \tag{2.134}$$

We use threshold detectors that can only detect the presence and absence of a pulse. The probably of detection of an n photon state emitted by Alice is given as:

$$\eta_n = 1 - (1 - \eta)^n. \tag{2.135}$$

Yield

Yield Y_n is the conditional probability of a detection event at Bob's side when Alice sends an n photon pulse. The yield Y_n includes the probability of detection of n photon pulse, η_n and the background events Y_0. We assume that the background counts and the signal are independent of each other. Then yield Y_n is given as,

$$Y_n = Y_0 + \eta_n - Y_0\eta_n. \tag{2.136}$$

Gain

Gain Q_μ is the probability with which Bob detects a signal sent by Alice. It depends on the characteristics of the source, channel and detectors, and hence is a function of mean photon number μ and the yield Y_n. The overall gain for any protocol (not necessarily ideal protocol) is given in terms of yields by:

$$Q_\mu = \sum_{i=0}^{\infty} Y_n \frac{\mu^n}{n!} e^{-\mu} = \sum_{n=0}^{\infty} Q_n, \tag{2.137}$$

where,

$$Q_n = Y_n \frac{\mu^n}{n!} e^{-\mu}. \tag{2.138}$$

Here, Q_n is the conditional gain when a pulse containing n number of photons is emitted by Alice and Q_μ is the overall gain.

Quantum Bit Error Rate (QBER)

Quantum Bit error rate (QBER) E_μ is the rate with which Bob makes a wrong detection when his basis is compatible with Alice's. The error rate of a *n*-photon state e_n for an ideal protocol is given as,

$$e_n = \frac{e_0 Y_0 + e_d \eta_n}{Y_n}, \tag{2.139}$$

where e_d is the detection error. For any protocol (not necessarily an ideal protocol), QBER is related to mean photon number μ, yields Y_n and error rates e_n as

$$E_\mu Q_\mu = \sum_{n=0}^{\infty} e_n Y_n \frac{\mu^n}{n!} e^{-\mu}. \tag{2.140}$$

2.5 Summary

In this chapter, we tried to map theoretical concepts from information theory with their practical applications. Initially we examined the key tools such as Shannon entropy and mutual information, establishing a relation between the two. Then, we explored qubits, their representation on the Bloch sphere, methods of manipulation, and techniques for measurement. Additionally, we introduced the density matrix formalism and discussed von Neumann entropy. Furthermore, we covered QKD algorithms, emphasizing their security aspects alongside error correction and privacy amplification. By leveraging the polarization degree of freedom, we explored practical implementations. Specifically, we discussed the BB84 protocol employing weak coherent pulses, accompanied by essential mathematical frameworks defining concepts such as yield, gain, and Quantum Bit Error Rate (QBER). Looking ahead, our subsequent chapters will gradually introduce additional concepts and techniques relevant to our ongoing study.

Chapter 3

Vulnerability due to detection coupling mismatch

3.1 Introduction

QKD facilitates the secure distribution of keys, which is ensured by a limit on the estimated QBER. Nevertheless, device imperfections in practical implementations can introduce vulnerabilities. Exploiting these imperfections, adversaries may acquire key information without alerting authenticated parties.

In a QKD protocol, information is typically encoded using a single degree of freedom, such as polarization, in our case. Side-channel attacks leverage the leakage of information through additional characteristics of the transmitted signal, such as spectral properties, spatial modes, or timing. Several studies, including [75, 76], explored potential side channels arising from Alice's state preparation in free-space BB84 QKD with polarization-encoded, attenuated pulses. Free-space quantum key

distribution (QKD) involves an additional spatial mode of photons compared to fiber-based QKD. Consequently, it is essential to carefully examine the potential leakage of side channels in free-space setups due to spatial mode discrepancies to gauge the extent of information accessible to eavesdroppers. In the BB84 protocol, combining different lasers to generate the four polarizations can introduce spatial mismatches, potentially resulting in information leakage. Ensuring that photons share the same spatial profile is crucial; they must be indistinguishable in terms of their spatial modes.

Moreover, imperfections at the detection end can also create vulnerabilities, as highlighted in [77]. Discrepancies in the coupling among the four detectors receiving the encoded polarization state introduce an extra degree of freedom at Bob's end, which adversaries could exploit. Side-channel attacks resulting from mismatches in detection efficiency due to spatial mode variations of incoming photons have been investigated in prior studies such as [78] and [79]. Characterizing all components of the QKD system is crucial to addressing information leakage stemming from side channels.

Our present investigation [80] focuses on information leakage at the detector end, stemming from coupling mismatches among the four detectors. This occurs when there is misalignment at the receiver's end, causing the couplers to deviate from the transverse plane of the incoming beam and be at relative angles from each other. Our characterization is specifically targeted at the detection setup. Even when all four states share the same spatial mode, detection coupling mismatch can occur due to misalignment at the receiver's end, where the couplers are not aligned with the incoming beam's transverse plane and are positioned at relative angles. To ensure no information leakage due to different spatial modes of the signal, we employ a single laser with a half-wave plate to generate the four polarization states. Following

propagation through a free-space channel, we examine the distribution at all four detectors at the receiver's end.

Free-space quantum communication presents one of the various potential applications of orbital angular momentum (OAM) in light beams. Spatial multiplexing and de-multiplexing OAM beams alongside other states, such as polarization, offer additional independent data carriers [81]. However, free-space quantum key distribution (QKD) is vulnerable to atmospheric turbulence, causing beam broadening. Research by [82] indicates that in a random inhomogeneous medium, the beam broadening of an average vortex beam is less than that of a Gaussian beam. Therefore, we conducted experiments involving two signal modes: Gaussian and Laguerre-Gaussian (LG) with radial index 0 and azimuthal index 1 (LG01 mode). It is worth noting that information is encoded solely in the polarization degree of freedom, not in the orbital angular momentum (OAM) degree associated with the azimuthal index of LG mode. We included LG modes to illustrate that high coupling mismatch results in information leakage, and enhanced coupling helps mitigate information leakage.

In this study, we outline the mathematical framework for computing the mutual information between Eve and Bob based on the parameters outlined in Sec. 3.2. Subsequently, in Sec. 3.3, we delve into the experimental specifics, including the eavesdropper's strategy for acquiring key information. The experimental findings are detailed in Sec. 3.4, followed by the conclusion in Sec. 3.5, where we address the potential implications of this leakage and propose methods for reducing errors to enhance the key rate.

3.2 Theoretical Background

Here, we examine the security vulnerabilities inherent in our QKD system and explore a potential attack in Sec. 3.2.1. Adhering to the standard convention, we refer to the sender as Alice, the receiver as Bob, and the adversary as Eve. The information acquired by Eve can be quantified utilizing certain mathematical tools. The mathematical framework essential for quantifying the information leakage is discussed in Sec. 3.2.2.

3.2.1 Loopholes and attack

QKD is theoretically unconditionally secure under ideal conditions. However, when implemented in real-world scenarios with imperfect devices (such as source, detectors, and optics), security vulnerabilities arise. Various well-known attacks exploit imperfections in sources and detectors, including the photon number splitting attack [36], detector blinding or bright pulse attacks [44, 83], faked state attacks [84, 85], time shift attacks [86], spatial mismatch [79], among others. Any deviation in source parameters, such as laser pulse width, wavelength, power, and beam profile, can provide information to Eve [75, 76]. Similarly, discrepancies at the detection end may also result in information leakage. In this study, we analyze the impact of misalignment or coupling mismatch at the detection setup on information leakage to Eve. Here, "coupling" refers to the amount of signal coupled to the fiber with the assistance of collimators.

From an attacker's perspective, Eve aims to gather information stealthily without raising suspicion, and the imperfections of the devices in the practical system can assist her in this endeavour. In our attack model, Eve intercepts the signal and mea-

sures its polarization. Subsequently, she manipulates Bob into making a measurement in a basis compatible with hers by directing the beam at an angle where the detector corresponding to her measurement has the highest probability of detection. For example, if Eve measures the H/V basis and obtains an H polarization result, she directs the beam to a position where the probability of H detection is highest among Bob's detectors. This manipulation relies on exploiting the detectors' varying detection probabilities at different angles stemming from significant coupling mismatches. Eve can gain advanced knowledge of which position yields the maximum detection probability for a specific detector, enabling her to characterize and exploit these vulnerabilities. Experimental details are in Sec. 3.3.2.

3.2.2 Information Leakage

There are multiple methods for quantifying the information leakage to Eve. Here, we quantify it in terms of the mutual information between Bob and Eve. The objective is to examine potential side-channel attacks at the receiver's end. Let B and E represent two discrete random variables with alphabets $\mathscr{B}$ and $\mathscr{E}$, respectively. The mutual information between B and E is defined as follows:

$$I(E:B) = H(B) - H(B|E), \tag{3.1}$$

where $H(B)$ denotes the Shannon entropy, which is calculated as follows:

$$H(B) = -\sum_{b\in\mathscr{B}} p(b)\log_2(p(b)), \tag{3.2}$$

$b \in \mathscr{B}$, $p(b)$ is the probability of obtaining b and $H(B|E)$ is the conditional Shannon entropy,

$$H(B|E) = -\sum_{e_v\in\mathscr{E}} p(e_v)\sum_{b\in\mathscr{B}} p(b|e_v)\log_2(p(b|e_v)) \tag{3.3}$$

$p(b|e)$ is the conditional probability of obtaining b given e.

Using Eq. (3.3) in Eq. (3.1), we get,

$$I(E:B) = H(B) + \sum_{e_v \in \mathscr{E}} p(e_v) \sum_{b \in \mathscr{B}} p(b|e_v) \log_2(p(b|e_v)) \tag{3.4}$$

Using Bayes theorem,

$$p(b|e_v) = \frac{p(b)}{p(e_v)} p(e_v|b), \tag{3.5}$$

we get,

$$I(E:B) = 1 + \sum_{e_v \in \mathscr{E}} \sum_{b \in \mathscr{B}} \frac{p(e_v|b)}{2} \log_2 \left(\frac{p(e_v|b)}{2p(e_v)} \right). \tag{3.6}$$

Here, we assume a binary symmetric channel. We have $H(B) = 1$ and $p(b) = 1/2$ due to the uniformly distributed bits and considering the basis selection to be a completely random process.

In Eqs. (3.3) - (3.6), e_v represents the parameter that Eve can utilize to acquire information. These parameters in QKD are an extra degree of freedom that an adversary can exploit to gain some information. Here, we want to explore the information detection leakage due to a detection coupling mismatch. We employ the approach proposed in [76] to estimate information leakage in terms of cross-correlation. Here, we briefly introduce the concept of cross-correlation.

Cross-correlation measures the similarity between two different functions. This is determined by shifting one function $g(s)$ relative to another function $f(s)$ by a certain interval (Δs). At each step of the shift, the values of both functions are evaluated, and the cross-correlation is computed. For discrete systems, the cross-correlation between two functions is given by:

$$R(\Delta s) = \sum_{i=0}^{\infty} f^*(s_i) g(s_i + \Delta s) \tag{3.7}$$

where $R(\Delta s)$ represents the cross-correlation between $f(s)$ and $g(s)$ when their origins are shifted by Δs (Figure 4.1). For continuous functions, the cross-correlation is expressed as:

$$R(\Delta s) = \int_0^\infty f^*(s)g(s + \Delta s)ds. \tag{3.8}$$

The correlation function R provided by Equation (3.8) indicates the similarity between f and g concerning Δs, where Δs represents the shift between the two functions and R ranges from 0 to 1.

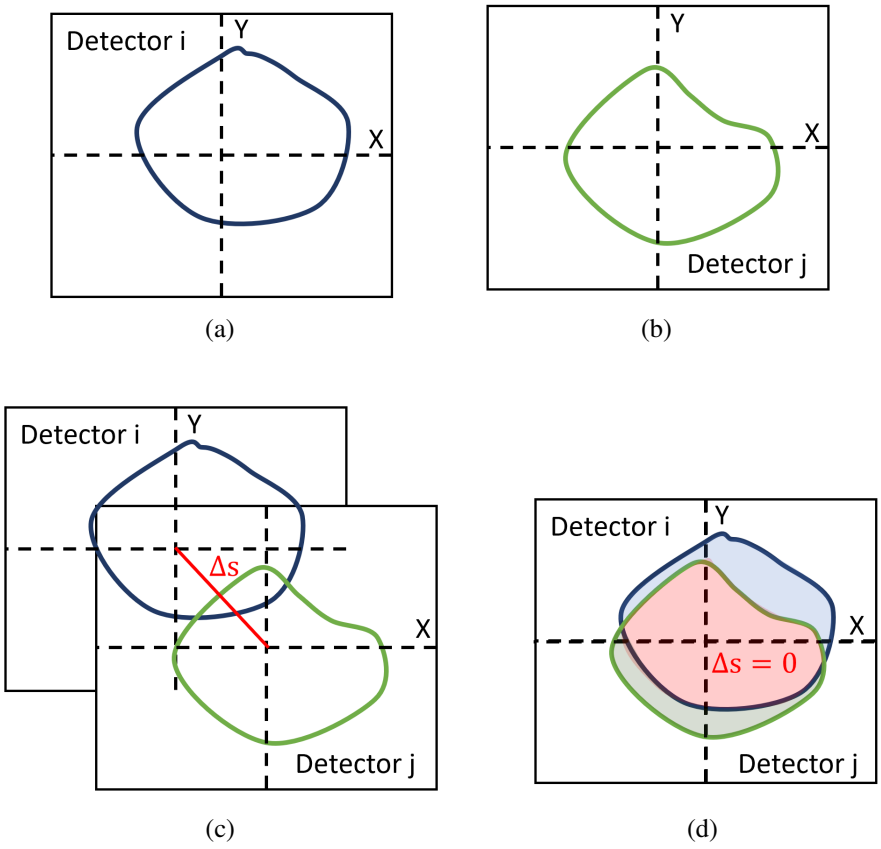


Figure 3.1: (a) and (b) are the distributions for detectors i and j, respectively, at each position X and Y of the lens L2. (c) shows how one distribution is scanned over the other for different Δs to measure the cross-correlation $R_ij(\Delta s)$. (d) shows the overlap of two distributions at $\Delta s = 0$

In subsequent discussions, detections in the four detectors are plotted against the

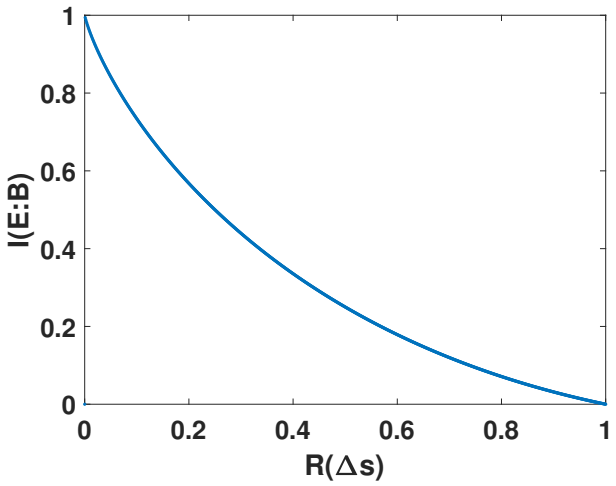


Figure 3.2: Relation between coupling quality in terms of $R(\Delta s)$ and information leakage in terms of I(E:B).

lens L2's X and Y positions (See Section. 3.3.2). We want to calculate the cross-correlation between the two detectors; hence, f and g correspond to the detection matrix. Fig. 3.1(a) and Fig. 3.1(b) depict the distributions of the two detectors i and j, respectively. Fig. 3.1(c) shows the scan of one matrix over another at Δs to calculate the cross-correlation $R(\Delta s)$ and Fig. 3.1(d) shows the overlap of two distributions at $\Delta s = 0$. The indistinguishability between the detection matrix can be known from $R(\Delta s = 0)$. When they are exactly similar, the cross-correlation $R(\Delta s = 0) = 1 = R(0)$. $R(0)$ measures the detection mismatch between the detectors, and $p(e_v|b)$ is the probability of Eve gaining the information exploiting such mismatch hence by argument, we can compare $R(0) \times \frac{1}{2}$ with Eve's guessing probability $p(e_v|b)$. Consequently, mutual information can be computed in terms of cross-correlation.

$$I(E:B) = 1 + \sum_{\substack{i,j \\ i \neq j}} \frac{R_{ij}(0)}{4} \log_2 \left(\frac{R_{ij}(0)}{4} \right). \tag{3.9}$$

We denote the cross-correlation between detectors i and j as R_{ij}. The summation

includes the cross-correlation values for the respective detectors. We can expand (3.9) as:

$$I(E:B) = 1 + \frac{R_{ij}(0)}{4}\log_2\left(\frac{R_{ij}(0)}{4}\right) + \frac{R_{ji}(0)}{4}\log_2\left(\frac{R_{ji}(0)}{4}\right). \tag{3.10}$$

We can verify from (3.10) that in case of the same detection matrices, $R(0) = 1$ and $I(E:B)$ will be zero. Evaluating cross-correlation provides an estimate of information leakage. The relationship between coupling quality and information leakage is illustrated in Fig. 3.2. We have calculated the cross-correlation numerically.

3.3 Experimental Setup

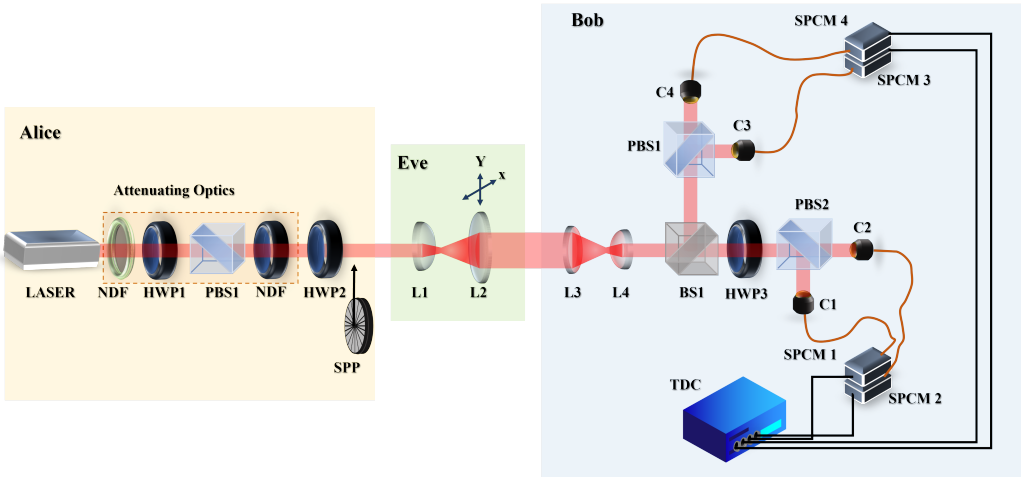


Figure 3.3: Experimental setup for characterizing coupling mismatch in detection: NDF: Neutral Density Filter; HWP: Half Wave Plate; BS : Beam Splitter; PBS : Polarizing Beam Splitter; M1 and M2 : Mirrors; L1, L2, L3 and L4: Lens of 2.5 cm, 30 cm, 20 cm and 5cm respectively; C1, C2, C3 and C4: Couplers; SPCM: Single Photon Counting Module; TDC: ID-900 Time Controller; SPP: spiral phase plate which is introduced to generate LG mode.

The experimental setup schematic for investigating the detection coupling mismatch is depicted in Fig. 3.3. This setup comprises three main sections: Alice, Bob, and Eve. Alice's section encompasses the source and encoding optics responsible for generating weak coherent laser pulses with the desired polarization. Further de-

tails regarding Alice's setup are provided in Sec. 3.3.1. Eve's section, detailed in Sec. 3.3.2, allows us to explore potential attacks stemming from detection coupling mismatch. Bob's section involves decoding optics and a single-photon counting module (SPCM) utilized for detecting photons originating from Alice, discussed comprehensively in Sec. 3.3.3.

3.3.1 Sender: Alice

For this experiment, a laser diode operating at $808nm$ (L808P010 Thorlabs) serves as the source. We have developed a custom laser driver circuit (LDC) capable of driving laser diodes in pulsed mode. The parameters of the laser diode, including repetition rate, power, and pulse width, can be adjusted according to the experimental requirements using the LDC. In this setup, the laser diode operates at a repetition rate of $5MHz$, with an optical pulse width of $1ns$. The laser beam is attenuated using a neutral density filter (NDF), followed by a combination of a half-wave plate (HWP1) and a polarizing beam splitter (PBS) for additional attenuation of the pulse. The transmitted beam from the PBS is horizontally polarized (H), and it undergoes further encoding of the signal pulse in the desired polarization degree of freedom by passing through another half-wave plate (HWP2).

The diode laser inherently produces a Gaussian beam, with which the experiment was performed. Subsequently, the experiment was repeated using the LG_{01} mode, generated by introducing a spiral phase plate (SPP) into the beam path (Fig. 3.3).

3.3.2 Adversary: Eve

We consider the adversary (Eve) positioned within the channel to manipulate the signal. Our objective is to investigate the impact of the detection probability of the

signal at various incident angles on the receiver's optics. To minimize beam divergence during propagation, the beam transmitted by Alice undergoes magnification through a combination of lenses L1 and L2, with focal lengths of 2.5 cm and 30 cm, respectively, kept at a distance of 32.5 cm from each other. Each lens has an aperture size of 1 inch. Lens L2 is integrated into Eve's setup, allowing her to utilize it in her attack. It is mounted on the motorized X and Y translation stage (Thorlabs - KMTS50E/M). Through this configuration, we analyze the effect on the detection probability across the four detectors.

Modifying the positions of the stage will induce changes in the incident angle of the incoming signal. Manual recording of data by adjusting the XY position and noting down counts on the time-to-digital converter (TDC) each time is laborious and time-consuming. To streamline our experimental procedures, we have automated our data acquisition process by interfacing the motorized stage and TDC with the computer using LabVIEW. This automation involves moving the stage in increments of 40μm while simultaneously recording the single detection counts from four detectors using the TDC. Lens L2 is oriented perpendicular to the direction of beam propagation, ensuring that the translation stage alters only the transverse coordinates of the lens. This translation of lens L2 in two transverse directions enables the beam to be projected at different positions onto the receiver's optics.

3.3.3 Receiver: Bob

At the receiver end, the collecting optics consist of a combination of lenses L3 and L4, with focal lengths of 20 cm and 5 cm, respectively, kept 25 cm from each other. After collecting optics at Bob, the beam radius is 1.8 mm and 1.7 mm for Gaussian and vortex beams, respectively. The beam is then directed towards Bob's decoding optics, which include a combination of beam splitter (BS), polarizing beam splitter

(PBS), and half-wave plates. The beam splitter (BS1) randomly selects between the two measurement bases. The four beams passing through PBS2 and PBS3 are further coupled to the single-photon detectors (Excelitas SPCM-800-14-FC) (D1-D4) using a multi-mode fibre (MMF) aided by an adjustable fibre collimator. The collimator used is the CFC5-B from Thorlabs of focal length 4.6mm, and the multi-mode fiber is the M42L01 from Thorlabs with core diameter 50μm and numerical aperture 0.22. The MMF is employed to enhance collection efficiency without favouring any specific modes. Subsequently, the detectors are connected to a four-channel time-to-digital converter (TDC, IDQuantique ID900), which records the detection events and their timing information.

3.3.4 Experiment Steps

Initially, the beam and all optical components are aligned using apertures, and the coupling is fine-tuned to achieve maximum counts in the detector. Lens L2 is secured on the XY translation stage to ensure the transmitted beam is well-collimated and aligned. Counts are then recorded for the four detectors at various X and Y positions, and the normalized counts are plotted against the X and Y values.

We investigate the detection coupling mismatch by determining the correlation between two 2D matrices. We obtain a 2D matrix containing the counts in each detector at every position X and Y of the lens. Subsequently, we numerically solve Eq. (3.8) to estimate the correlation between the two matrices, and Eq. (3.9) is utilized to calculate the corresponding information leakage.

To achieve a perfect alignment, couplers should be perpendicular to the incoming beam, with the transverse plane defined by the XY plane and the direction of beam propagation along the Z axis. Suppose the coupler of one detector is at an angle

θ with the X axis. If all other detectors are also at this θ angle, there will be no coupling mismatch due to alignment despite the overall alignment being off by θ. Therefore, relative alignment is crucial. Coupling involves four degrees of freedom: transverse movement in the X and Y directions and tip-tilt about the X and Y axes. The ideal method for alignment is to keep all couplers perpendicular to the incoming beam, ensuring no relative alignment mismatch. In the case of high coupling mismatch conditions, we maximized the detectors' counts without considering the couplers' orientation. However, we aligned the couplers perpendicular to the incoming beam for low coupling mismatch while maximizing the counts, ensuring optimal alignment and minimal mismatch.

During optical alignment, it is crucial to position the components within the transverse plane of the propagating beam. To enhance coupling, we manipulate the orientation of the small coupling lens, which is mounted on the tip-tilt mounts and two translation stages. The tip-tilt mounts assist in adjusting the angle, while the translation stages facilitate movement within the transverse plane.

3.4 Results and discussion

The counts recorded in all four detectors at various positions of the incident signal beam were plotted and analyzed. Fig. 3.4-left illustrates the normalized plots of detector counts for high coupling mismatch (left), while Fig. 3.4-right depicts the normalized plots of detector counts for low coupling mismatch (right), corresponding to the X and Y positions of lens L2 for an incident Gaussian beam. The range of X and Y scales remains consistent across all plots. The colour bar displayed on the right side scales the colour to values. As the plots are normalized, the intensities can be interpreted as the probability of detection at a specific position.

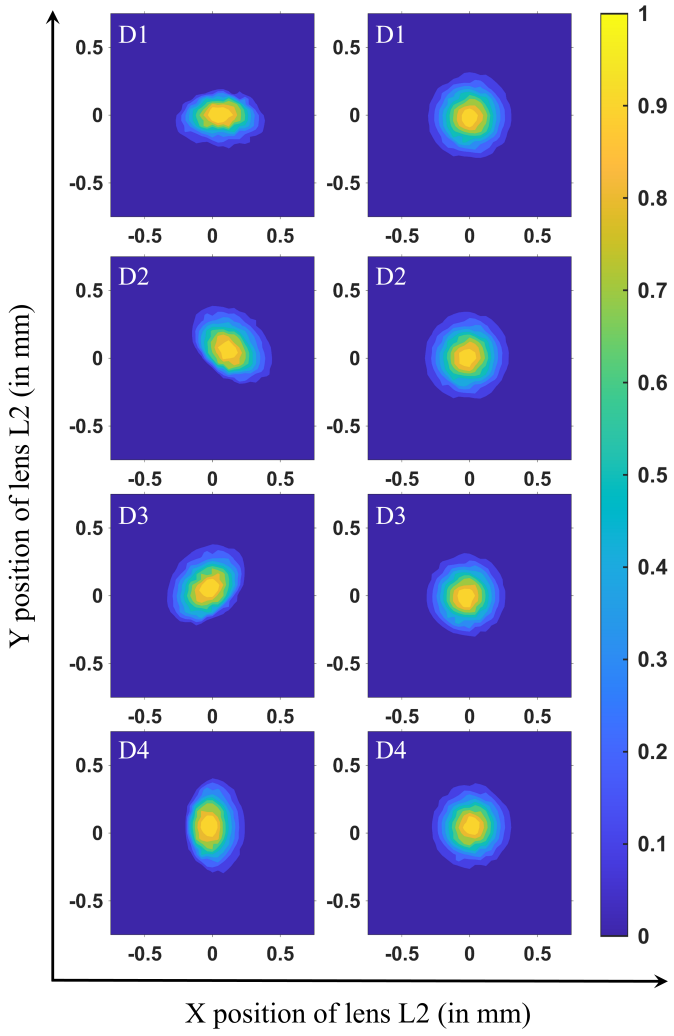


Figure 3.4: Normalized plots of detector counts for high coupling mismatch (left) and low coupling mismatch (right) with X and Y position of lens L2 (mm) for a incident Gaussian beam. The range of X and Y scales are same for all plots. The colorbar shown on right scales the color to values.

The experiment conducted with the Gaussian mode in the laboratory environment aimed to yield similar plots in all four detectors. However, the plots for high coupling mismatch, as depicted in Fig. 3.4-left, are not identical across the four detectors, indicating a varying probability of detection when the beam falls at specific positions at the coupler. Certain positions of X and Y exhibit a higher probability of detection in one detector compared to others. Eve can exploit this by selecting the positions of X and Y to induce detection in a particular detector with a high probability, thus exerting control over Bob's detection and gaining partial information without disclosing her presence. Conversely, for low coupling mismatch, as illustrated in Fig. 3.4-right, the plots are nearly identical for all four detectors. These similar plots offer no additional information to Eve regarding the polarization or basis used for encoding the signal.

The correlation between two detectors is determined using Eq. (3.8). Counts recorded for the X and Y positions of the lens create a two-dimensional matrix for each detector. For a given $n \times n$ matrix for the two detectors, the $(2n+1) \times (2n+1)$ cross-correlation matrix is computed numerically. The value of R at $\Delta s = 0$ provides insight into the distinguishability of the functions. These results can also be interpreted in terms of the cross-correlation R of plots among all four detectors, as illustrated in Table 3.1 and Fig. 3.6. For low coupling mismatch, the value of R is nearly 1, whereas for high coupling mismatch, it is lower. Table 3.1 also displays the information leakage to Eve in terms of mutual information. Fig. 3.7 compares the information leakage to Eve between low and high coupling mismatch scenarios. For low coupling mismatch, $I(E : B)$ is approximately 10^{-2}, while for high coupling mismatch, it is around 10^{-1}, which is an order of magnitude higher. These values are influenced by the amount of detection coupling mismatch between the detectors, thereby helping quantify the mismatch. If the coupling deteriorates further, this value will increase. The findings suggest that a high correlation in the

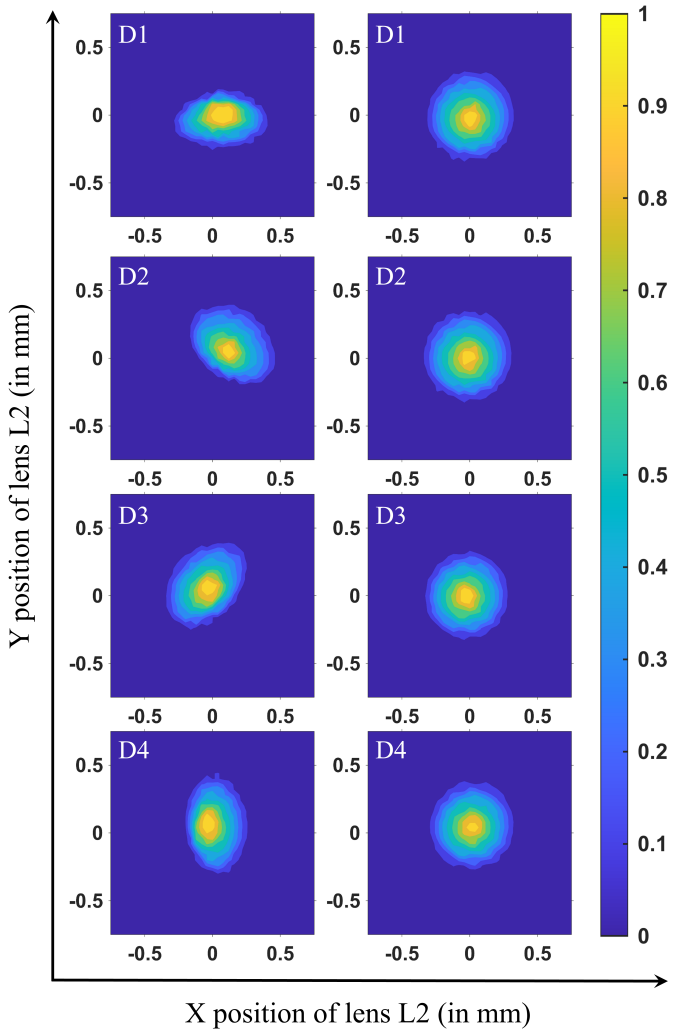


Figure 3.5: Normalized plots of detector counts for high coupling mismatch (left) and low coupling mismatch (right) with X and Y position of lens L2 (mm) for a incident order-1 vortex beam. The range of X and Y scales are same for all plots. The colorbar shown on right scales the color to values.

spatial profiles observed by the four detectors implies less information leakage.

Detectors	Gaussian Beam			
	High coupling mismatch		Low coupling mismatch	
	R	I(E:B)	R	I(E:B)
D1 & D2	0.7423	0.0981	0.9868	0.0038
D1 & D3	0.7307	0.1039	0.9816	0.0052
D1 & D4	0.7723	0.0838	0.9450	0.0164
D2 & D3	0.6239	0.1638	0.9902	0.0028
D2 & D4	0.6565	0.1442	0.9661	0.0099
D3 & D4	0.9227	0.0237	0.9451	0.0164

Table 3.1: Cross-Correlation between the detectors and Mutual information between Bob and Eve (in bits) for low and high coupling mismatch of Gaussian beam.

Detectors	Vortex order 1			
	High coupling mismatch		Low coupling mismatch	
	R	I(E:B)	R	I(E:B)
D1 & D2	0.7196	0.1096	0.9880	0.0034
D1 & D3	0.6641	0.1398	0.9797	0.0058
D1 & D4	0.7539	0.0925	0.9446	0.0166
D2 & D3	0.6158	0.1689	0.9904	0.0027
D2 & D4	0.7163	0.1442	0.9671	0.0096
D3 & D4	0.8944	0.0237	0.9499	0.0149

Table 3.2: Cross-Correlation between the detectors and Mutual information between Bob and Eve (in bits) for low and high coupling mismatch of vortex beam of order 1.

The experiment was subsequently conducted using a vortex signal beam, and the counts were graphed against the corresponding X and Y positions. Fig. 3.5 displays the normalized plots of detector counts for high coupling mismatch (left) and low coupling mismatch (right), depicting the X and Y positions of lens L2 (in mm) for an incident order-1 vortex beam. Notably, no significant difference is observed in the plots between Gaussian and vortex beams. Table 3.2 reveals that the values of cross-correlation and information leakage for the Laguerre Gaussian mode are approximately equivalent to those for the Gaussian mode. This suggests that the symmetric spatial mode for low coupling mismatch minimizes information leakage.

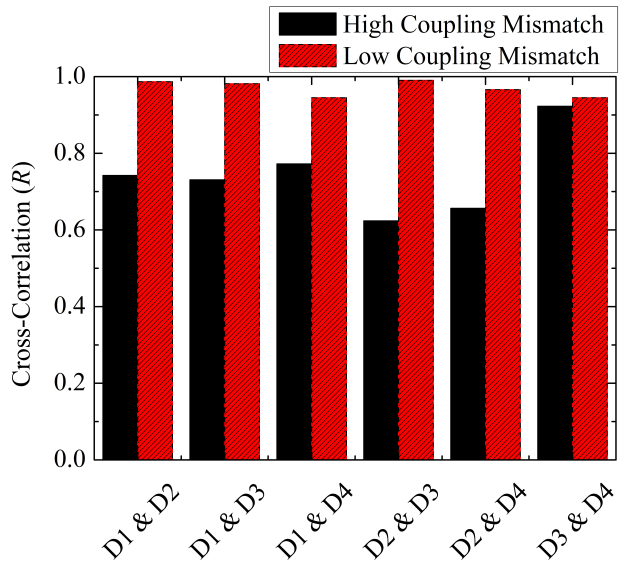


Figure 3.6: Cross-correlation for the high and low coupling mismatch between the detectors for Gaussian beam.

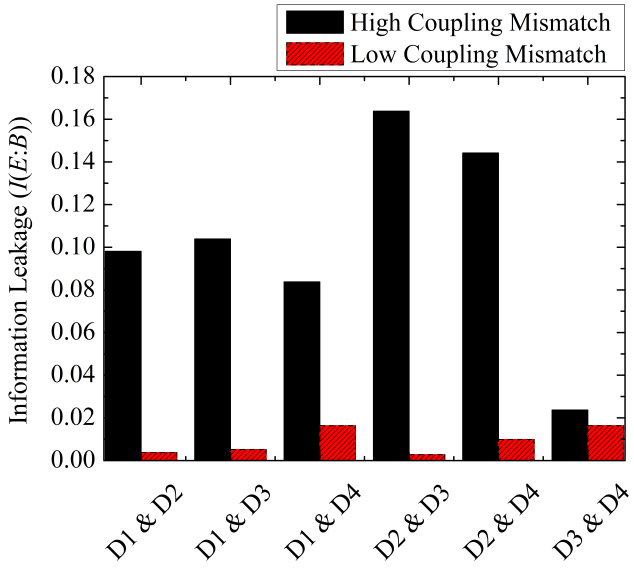
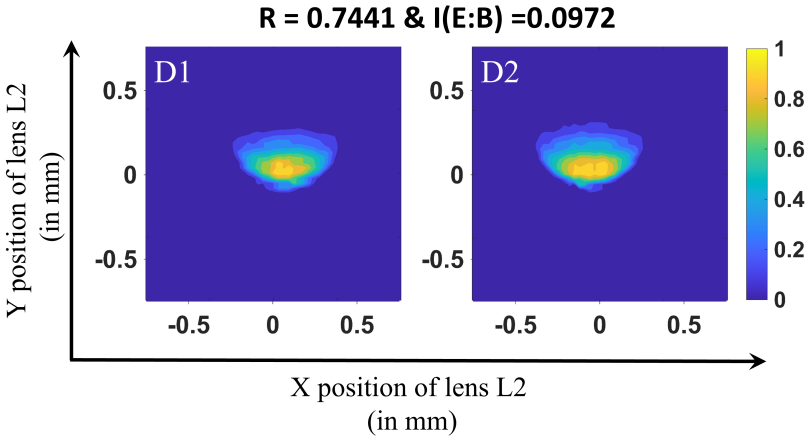
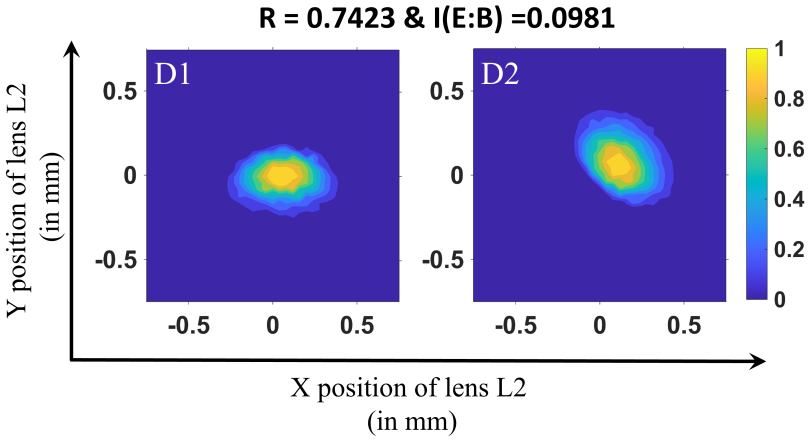


Figure 3.7: Information leakage for the high and low coupling mismatch between the detectors for Gaussian beam.



(a)



(b)

Figure 3.8: Two cases (a) and (b) where we observe similar cross-correlation values for different detection matrices corresponding to coupling mismatch.

The cross-correlation between two detection matrices can be similar for two different configurations of mismatches. Fig. 3.8 showcases two cases where similar cross-correlation values are observed for different detection matrices corresponding to coupling mismatch. The figures are accompanied by their respective values of cross-correlation and mutual information. However, the pivotal aspect is to characterize the device for any potential information leakage and minimize it while integrating it into the estimation of the secure key rate. The focus of this experiment is to assess the extent of leakage caused by misalignment (coupling mismatch), which impacts not only the key rate but also the security. Quantifying this leakage aids in monitoring the amount of side-channel leakage at Bob's end.

3.5 Summary and Conclusion

We have investigated how a high coupling mismatch at the detectors' end results in information leakage to Eve, even for symmetrical modes. We compared cases of low and high coupling mismatch in terms of cross-correlation and mutual information. Ideally, mutual information, which estimates information leakage, should be zero. In our case, information leakage improves by an order of magnitude with improved coupling. The values of information leakage serve as a metric for quantifying the degree of mismatch between the two detectors. The experiment was conducted for both Gaussian and Laguerre Gaussian beams, considering two types of symmetrical modes. The results indicate that with proper coupling of the beam to the detectors and a symmetric profile of the incoming beam, information leakage is minimized. Mutual information between Eve and Bob due to mismatch is calculated and can be considered in privacy amplification. This experiment not only enhances system security but also determines the amount of secure keys that can be extracted from it, which is significant for standardizing any QKD system for

deployment.

Chapter 4

Mitigating the source-side channel vulnerability

4.1 Introduction

Properly characterising the devices employed in implementing QKD protocols is essential to ensure security. This concern has been addressed in various studies [35–38, 40, 44, 87]. A critical aspect of optical quantum cryptography involves using single-photon Fock states. Though realizing true single-photon sources experimentally remains challenging, several practical options are employed. These include weak coherent pulses (WCPs), heralded single-photon sources, and entangled photon sources [31].

Numerous QKD implementations utilize weak coherent pulses (WCPs) as an approximation for single-photon Fock states. These pulses are generated by significantly attenuating a pulsed laser source via calibrated attenuators. It is widely ac-

cepted that laser sources operating significantly above the threshold produce coherent states. Consequently, the resulting weak laser pulses display Poissonian statistics. The mean photon number serves as the distinctive characteristic of Poissonian statistics. Ensuring accurate measurement of the average photon count is imperative for the successful implementation of secure QKD with WCPs.

There is a non-zero probability of obtaining more than a single photon per pulse due to the Poisson statistics of WCPs. This exposes our QKD system to adversarial attacks such as the photon number splitting attack [36]. To mitigate the risk of information leakage, the decoy state protocol [70–73] has been proposed. Decoy pulses with slightly different mean photon numbers are sent along with the signal pulses. Since Decoy pulses are also characterized by Poisson statistics, accurate estimation and characterization of photon statistics become desirable.

Implementing QKD protocols relies on the widespread use of single-photon avalanche photodiodes (SPADs) [88]. It is important to consider various factors such as dead time, spectral range, dark count rate, timing jitter, detection efficiency, and the photon number resolution [89] when assessing the capabilities of a single-photon detector. SPADs are threshold detectors which are non-photon resolving. They are often referred to as on-off detectors since they can only detect the presence or absence of a pulse containing photons. Therefore, utilizing a single SPAD for characterizing the source may yield inaccurate estimates. Previous studies [90–93] discuss various approaches to photon characterization using multiple on-off detectors.

In this work, we focus on characterizing the photon statistics of WCPs for QKD applications. We first estimate the mean photon number utilizing a single detector. Thereafter, we employ four detectors for source characterisation to achieve higher accuracy. Previously in [93], authors suggest the utilization of four detectors

to compute limits on probabilities for lower photon numbers $(n \leq 3)$. We have extended this approach to obtain highly accurate estimations of the mean photon numbers. We gave a comparison of new results with previous estimates. Thereafter, we investigated the deviation of the mean photon number (μ) and analyze the resulting information leakage caused by this miscalculation.

Many studies have explored various state preparation flaws, providing security proofs that establish protective measures even in the presence of these loopholes [94–100]. Lasers inherently exhibit statistical fluctuations since they follow Poisson statistics. However, in practical experiments, additional variability can arise from factors such as power supply instabilities, temperature variations, laser driver noise, mechanical vibrations, etc. Ideally, all sources with the same mean photon number (μ) should exhibit the same variance. However, experimental fluctuations can cause these variances to differ. We aim to study the mismatch between the fluctuations of these sources and understand its impact on the security of our Quantum Key Distribution (QKD) process.

The chapter's organization is as follows: In Sec. 4.2, we discuss the theoretical background for estimating the mean photon number per pulse and the fluctuations of a weak coherent pulse (WCP) source. Next, in Sec. 4.3, we detail the experimental setup and procedures. Sec. 4.4 presents the results of our source characterization of intensity and fluctuations. Finally, in Sec. 4.5, we conclude and summarize our findings.

4.2 Theoretical Background

In this section, we present the theoretical prerequisites for our study.

4.2.1 Weak Coherent Pulses (WCPs)

A pulsed laser with a repetition rate ν_{rep} and wavelength λ is attenuated to produce weak coherent pulses (WCPs). As lasers are coherent sources, even a faint laser emits coherent states. The number of photons per pulse is not deterministic but follows a Poisson distribution. Here, we elaborate on the method we use to generate WCPs with a desired distribution.

It is imperative for QKD sources to maintain a mean photon number of less than one to adhere to the security requirements of QKD protocols. We begin by measuring the average power P_{avg} of the source, from which we calculate the energy per pulse E_{pulse} as:

$$E_{pulse} = \frac{P_{avg}}{\nu_{rep}}. \tag{4.1}$$

The average number of photons per pulse n_{avg} is given by,

$$n_{avg} = \frac{E_{pulse}\lambda}{hc}. \tag{4.2}$$

To achieve the desired mean photon number, we employ a neutral density filter with a specified optical density (OD). The OD determines the level of attenuation applied to the laser beam. By selecting a suitable filter and adjusting the attenuation, we can generate weak coherent pulses (WCPs) with the desired Poisson statistics characterized by a mean photon number denoted as μ_{desired}, which is suitable for QKD applications.

$$\mu_{desired} = \frac{E_{pulse}\lambda}{hc} * 10^{-OD}. \tag{4.3}$$

We now elaborate on methods to estimate the mean photon number (μ) of the source

utilized in QKD implementations.

4.2.2 Method-I : Using single detection

Single-photon detectors based on avalanche photodiodes are employed to detect the number of detections per second.

$$N = \mu \times \nu_{rep} \times \eta. \tag{4.4}$$

Where N represents the number of detections per second, ν_{rep} is the repetition rate of the laser, and η denotes the detection efficiency. We can estimate the value of μ as:

$$\mu = \frac{N}{\nu_{rep} \times \eta}. \tag{4.5}$$

Single photon avalanche photodiodes are the predominant choice for detecting quantum signals, capable of discerning the presence or absence of photons within a pulse. However, relying solely on a single on-off detector may result in underestimating photon statistics. Hence, employing photon-resolving detectors or a more comprehensive methodology becomes crucial in characterizing the Quantum Key Distribution (QKD) source. Accurately estimating μ holds paramount significance for accurate key rate calculations.

4.2.3 Method-II Rigorous Characterisation

For source characterization, it is essential to split the pulse using a sufficient number of beam splitters and threshold detectors. Since the mean photon number in Quantum Key Distribution (QKD) is typically low, we assume that the multi-photon probability is minimal. This assumption allows us to thoroughly characterize the

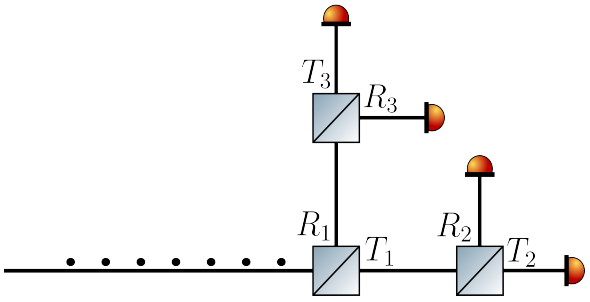


Figure 4.1: The branching efficiencies are defined as the probability for a photon to reach a particular detector. In the setup shown above the four branching efficiencies can be given as $\{T_1T_2, T_1R_2, R_1T_3, R_1R_3\}$.

source using multiple detectors, such as four detectors ($D = 4$). Fig. 4.1 illustrates an example of the setup required for conducting such characterization. The branching efficiencies define the probability of a photon reaching a specific detector. Let $\eta_{b,i}$ denote the branching efficiency, $\eta_{c,i}$ represent the coupling efficiency, and $\eta_{d,i}$ indicate the quantum efficiency of the detectors.

Overall efficiency is given as,

$$\eta_i = \eta_{b,i} * \eta_{c,i} * \eta_{d,i}, \tag{4.6}$$

where $i = 1, 2, 3, 4$ represents all four arms and respective detectors. The average efficiency is given by,

$$\eta := \frac{1}{4} \sum_{i=1}^{D} \eta_i. \tag{4.7}$$

We define $Z_D := \{1, 2, 3, 4\}$ as the set of all the detectors. We aim to record the r-fold coincidences ($r = 2, 3, 4$), where $r = 1$ refers to the counts in a single detector. Let us denote the observed r-fold coincidence probability as: $c_{obs,r}$ [93].

$$c_{obs,r} = \binom{D}{r}^{-1} \sum_{W \subset I_r} c_{obs,W}, \tag{4.8}$$

where $I_r := \{W \subset Z_D \mid |W| = r\}$ represents all possible subsets W of Z_D with

cardinality $|W|= r$. $c_{\text{obs},W}$ denotes the total coincidence probability of the set W, where all detectors in W detect irrespective of the detection events in the remaining detectors. The averaged r-fold coincidences, given that the pulse has n photons, is defined as:

$$c_{obs,r} = c_{n,r} := \sum_{j=0}^{r} (-1)^j \omega_{r,j} \sum_{W \in I_j} \left(1 - \sum_{i \in W} \eta_i\right)^n, \tag{4.9}$$

where,

$$\omega_{r,j} := \frac{\binom{D-j}{r-j}}{\binom{D}{r}}. \tag{4.10}$$

For a Poisson distribution with mean photon number μ, the averaged r-fold coincidences $(r = 1, 2, 3, 4)$ should satisfy:

$$c_{obs,r} = \sum_{n=0}^{\infty} p_n c_{n,r}, \tag{4.11}$$

where,

$$p_n = \frac{e^{-\mu}\mu^n}{n!}. \tag{4.12}$$

To evaluate the coincidences from experimental data, we will utilize Eq. (4.8) as referenced in our work. Furthermore, we will employ the bounds specified in the article [93] to experimentally verify the Poissonian statistics of the WCPs used in QKD implementations and accurately estimate the mean photon number for the distribution.

4.2.4 Information Leakage

An adversary could potentially acquire complete information regarding the bit value encoded within a multi-photon pulse. Privacy amplification diminishes the information accessible to an adversary concerning the shared key between the authenticated parties. It is crucial to ascertain the optimal number of bits for subtraction in privacy

amplification to prevent underestimation. Given that Eve's attack strategy cannot be predicted in advance, we consider an attack scenario wherein Eve can access all information within the multi-photon pulses. Absolute security could be ensured by employing adequate privacy amplification, whereby all bit values associated with the multi-photon pulses are discarded.

Misestimation of information leakage

If a WCP source follows a Poisson distribution with μ representing the mean photon count per pulse, then the probability of multi-photons per pulse is expressed as:

$$p_{multi} = \sum_{p_n \geq 2} p_n \tag{4.13}$$

When estimating the secure key rate, we account for this worst-case scenario by discarding the coincidences between Bob's detectors and only considering the single detections with a basis compatible with Eve. We estimate the subtraction terms as the multi-photon pulses contributing to the single detections to address the information leakage. Therefore, we consider:

$$I(A:E) = \sum_{p_n \geq 2} \left(p_n * \frac{1}{2^n} \right) \tag{4.14}$$

Here, p_n is the probability of Alice emitting a pulse containing n photons and $p_n = e^{-\mu}\mu^n/n!$. The factor of $1/2^n$ is the probability of Bob receiving the detection in the correct basis for a n photon pulse. Since only the detections in the correct basis contribute to the key we have considered the contributions from the multi-photon pulses as the information leakage. We have considered the case where Eve mimics the photon statistics and sends the same no. of photons to Bob as she received from Alice.

To estimate the information leakage accurately, we must estimate the multiphoton pulses, which eventually reduces to estimating the mean photon number per pulse (μ) accurately. We will see in the results how miscalculation of mean photon number (see Fig. 4.3) leads to misestimation of information leakage (see Fig. 4.4).

Here, we have considered the WCP BB84 QKD protocol. However, in the decoy state protocol, the estimation of single-photon and vacuum yields also depends on the mean photon number of the signal and decoy states. Therefore, this rigorous characterization study is valid for decoy and non-decoy cases. While the information leakage discussed here is case-specific, the methodology and insights gained can also be extended to other scenarios. An incorrect calculation of the mean photon number will inevitably lead to an inaccurate estimation of information leakage.

Information leakage due to fluctuations

We use polarisation degree of freedom for encoding the photons. Any additional degree of freedom inherent in our states could be exploited and poses a potential risk of a side-channel attack. The weak coherent source has intrinsic intensity fluctuations with time. Our aim is to explore the disparities in the fluctuations manifested by the sources. Assuming N_s signal states are emitted with an intensity of μ, we propose that accurately $N_s\mu e^{-\mu}$ out of the N_s signal states correspond to single photons. It is crucial to ensure that these fluctuations are not a parameter that Eve can exploit to gain information. Ideally, weak coherent sources should follow Poissonian statistics, where the variance is equal to the mean photon number. However, experimentally, they deviate from the mean and differ from each other (see Fig.4.4). By studying the cross-correlation among these sources, we can estimate the side-channel leakage and ensure the robustness of our system against such vulnerabilities.

To quantitatively evaluate the level of information leakage to Eve, we employ the methodology introduced in [76]. The similarity between the sources is characterised by the correlation function R. By comparing R with Eve's guessing probability $p(e|b)$, we can compute the mutual information in terms of cross-correlation.

$$I'(A:E) = 1 + \sum_{\substack{i,j \\ i \neq j}} \frac{R_{ij}}{4} \log_2 \left(\frac{R_{ij}}{4} \right). \tag{4.15}$$

In this context, R_{ij} represents the cross-correlation between sources i and j. When the functions are perfectly identical, $I'(A:E)$ reduces to zero, as indicated by Eq. (4.15). The assessment of cross-correlation provides an approximation of the degree of information leakage. In order to distinguish between information leakages caused by multi-photon pulses and those from side channels, we denote them as $I(A:E)$ and $I'(A:E)$, respectively.

4.3 Experimental Method

The experimental setup has four diode lasers operating at 808 nm (L808P010 Thorlabs). Utilizing the standard BB84 transmitter configuration, these lasers contribute to generating the four polarization states essential for QKD. To ensure consistency, we meticulously selected diodes with closely matched characteristics. Additionally, a custom-designed laser driver circuit was employed to drive these diodes effectively. Subsequent to this, we conducted a thorough characterization of the diodes, focusing on parameters like wavelength, pulse width, and spatial profile to optimize their indistinguishability. Any discernibility in other degrees of freedom, such as spatial mode, temporal profile, or spectral profile, poses a risk of potential side-channel attacks, which have been addressed in prior research [75, 76]. The source setup encompasses the laser diodes along with the attenuating optics.

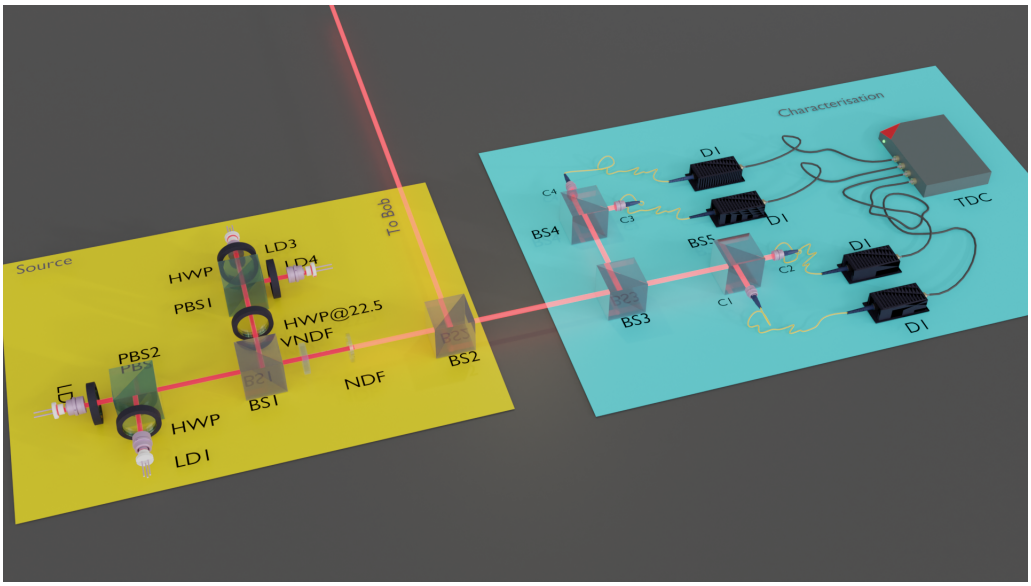


Figure 4.2: Experimental setup for characterising photon statistics of the source: V-NDF: Variable Neutral Density Filter; NDF: Neutral Density Filter; HWP: Half Wave Plate; BS: Beam Splitter; PBS: Polarizing Beam Splitter; M: Mirror; C: Coupler; D: Single Photon Counting Module; TDC: ID-900 Time Controller.

Each laser diode is triggered by voltage pulses with a repetition rate of 1.25 MHz. Employing a half-wave plate and a polarizing beam splitter (PBS), the emitted beam from the diodes undergoes polarization and attenuation adjustments. The PBS allows horizontally polarized light to transmit while reflecting vertically polarized light. Adjusting the half-wave plate's rotation controls each beam's intensity. Up to this point, the setup remains identical for both bases. To transition to the diagonal basis, we introduce another half-wave plate rotated by $22.5°$. This rotation aligns the beam's polarization with the diagonal basis. The beams merge at a beam splitter (BS1), with only one arm's output considered while the other is discarded. The beam intensity is halved due to the combination of the four beams at this beam splitter.

Subsequently, all four beams traverse through a variable neutral density filter (NDF) with a maximum optical density (OD) of 4, accompanied by a fixed NDF with an

optical density of 6. These filters attenuate the beam intensity accordingly. We intend to examine the photon statistics of the resultant beam from this final NDF, which constitutes the signal. To analyze the photon statistics of each source independently, we block the other sources and analyze them individually, one by one.

Parameter	Value
Coincidence window	2 ns
Pulse width	1 ns
Detection jitter	350 ps
Dark counts	100 cps
Background counts (bg)	
bg in detector-1	425 cps
bg in detector-2	1049 cps
bg in detector-3	1119 cps
bg in detector-4	1904 cps

Table 4.1: Coincidence window, pulse width, detection jitter, dark counts, and background counts. Counts are recorded for an integration window of 1s, i.e. counts per second (cps). Background counts of the detectors are the averaged values for 1s. The dark count is the maximum dark count of the detector.

We collect timestamps for detections from each source, including two-fold, three-fold, and four-fold coincidences. We also measure the background counts by blocking the source, noting that each detector experiences varying background levels due to differing background light exposures (see table 4.1). To ensure accuracy, these detections are subtracted from the total counts during source characterization. Since background counts for each detector are treated separately, they do not affect our analysis. The coincidence window is kept as 2ns, keeping in mind the pulse width and the detection jitter (see table 4.1). The detectors have a dead time, i.e. a period after detection for which the detector is not responsive to any incoming photons. This period is crucial since it might lead to underestimating detection count rates. However, the dead time of our detectors is very low, specifically 22 ns, and our laser emits pulses at an interval of 800 ns. Hence, there will not be any significant effect.

Beam Splitter	T^2	R^2
BS3	0.494	0.453
BS4	0.474	0.446
BS5	0.461	0.456

Table 4.2: Transmittance and reflectance of beam-splitters used in characterisation setup

We adjust the variable NDF to obtain different μ values. The estimation of μ is approximately calculated using Eq. (4.16).

$$N = \mu\nu_{rep}\eta \tag{4.16}$$

Where N represents the count rate in the detector per second, μ stands for the mean photon number, ν_{rep} denotes the repetition rate, which is 1.25 MHz, and η signifies the overall efficiency. The overall efficiency, described by Eq. (4.6), encompasses the quantum efficiency of the detector ($\eta_{d1} = \eta_{d2} = \eta_{d3} = \eta_{d4} = 65\%$), fiber-coupling efficiencies ($\eta_{c1} = 85\%$, $\eta_{c2} = 0.91\%$, $\eta_{c3} = 0.87\%$, and $\eta_{c4} = 0.88\%$), and branching efficiency (η_{bi}). While acknowledging the potential discrepancies in detector efficiencies, for which we rely on the data sheets of the instruments. Given the reciprocal nature of characterizing a detector with a source and vice versa, we conduct the characterization one at a time. The beam splitters do not exhibit a 50-50 splitting ratio; therefore, we also incorporate these experimental efficiencies into our calculations. We characterized the beam splitters, and Table 4.2 contains the transmittance and reflectance values.

Hence, with Eq. (4.16), we can approximately determine whether we have reached the intended value of μ by examining the count numbers in a single detector, as elaborated in Sec. 4.2.2, given that these counts solely indicate the presence or absence of a pulse containing photons. Subsequently, we characterize the source by analyzing the r-fold coincidences recorded to estimate μ using Sec. 4.2.3. We will utilize Eq. (4.8) to evaluate the coincidences from experimental data ([101]).

Furthermore, we employ the probability bounds specified in the article [93] (see Appendix A.1) to experimentally verify the Poissonian statistics of the WCPs used in QKD implementations and accurately estimate the mean photon number for the distribution. This procedure is iterated for all four laser diodes emitting various polarizations. The steps to data analysis are presented in Appendix A.2

We employ a single detector for each source to investigate the intensity fluctuations of all four sources. Additionally, we adjust the variable attenuator by rotating it to achieve the desired count rate while the detectors capture individual signals. This data is recorded over multiple cycles to analyze the source fluctuations. The experiment is repeated for different source intensities to observe fluctuations as a function of intensity.

4.4 Results and Discussion

We recorded both single and coincidental detections and confirmed that the photon statistics adhere to a Poisson distribution, as elaborated in Sec. 4.2.3. Comparing the computed values obtained through Method-I (Sec. 4.2.2) and Method-II (Sec. 4.2.3), we illustrated the disparity as a function of the mean photon number (μ) in Fig. 4.3. As expected, the difference in the estimated values grows with an increase in the mean photon number. This trend is foreseeable since a single detector lacks the precision to make accurate measurements, especially in the presence of multi-photon pulses. Coincidences obtained through multiple on-off detectors offer higher accuracy.

We compute the mutual information for each scenario using Eq. (4.14) using the mean photon numbers from method 1(4.2.2) and method 2(4.2.3). We then find the difference between these estimated leakages to find the miscalculation in informa-

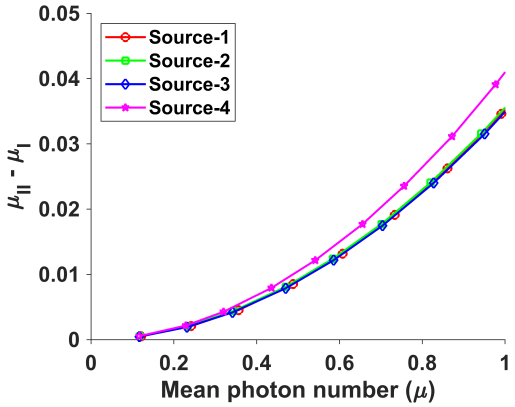


Figure 4.3: Difference between the mean photon number (μ) calculated using Method-I and Method-II of mean photon number (μ).

tion leakage. We must emphasize that we are examining the worst-case scenario, where Eve can exploit information from all multi-photon pulses within the BB84 protocol. This study can be expanded to cover other prepare-and-measure protocols employing weak coherent pulses as the source. Accurate assessment of potential information leakage is essential, achievable only through a well-characterized understanding of photon statistics. Errors in estimating the mean photon number result in an incorrect estimation of $I(A:E)$. An adversary can exploit the undisclosed portion of information. The corresponding variation in information leakage $I(A:E)$ with respect to the mean photon number (μ) is illustrated in Fig. 4.4.

Fig. 4.5 depicts the fluctuations in intensity relative to the average photon count for all four sources. These fluctuations were derived using a single consistent detector based on multiple iterations of single-count data obtained from each source. The error bars represent the deviation between data points and the fitted linear curve. As expected, increasing the mean photon count results in higher intensity fluctuations.

The differences observed among the four laser diodes stem from inherent variations, as no two diodes are perfectly identical. Moreover, slight discrepancies in the components of the laser diode driver circuit can also impact the outcomes. These chal-

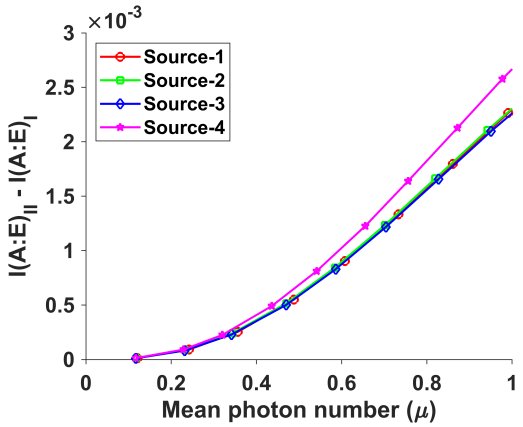


Figure 4.4: Information leakage due to miscalculated mean photon number (μ) as a function of mean photon number (μ)

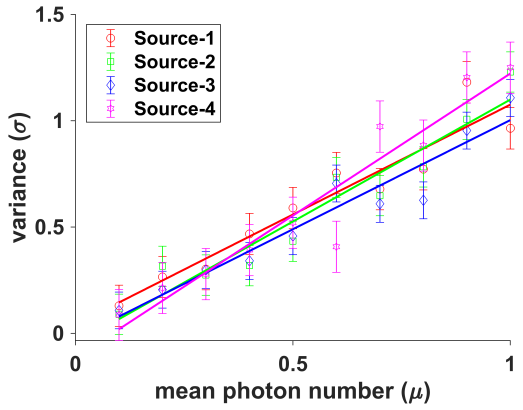


Figure 4.5: The variation in intensity fluctuations for all four sources vs the average photon count (μ).

lenges are common in practical scenarios involving multiple lasers. The ongoing approach involves improving the quality of the devices and meticulously characterizing them to identify any imperfections.

Fig. 4.6 displays the distribution of all four sources with an average value of 0.5 photons per pulse. weak coherent sources ideally follow Poissonian statistics, where the intensity fluctuations match the mean photon number. In our case, with a mean of 0.5, the variances for sources 1, 2, 3, and 4 are 0.5678, 0.5272, 0.5000, and 0.5566, respectively. Since Poissonian statistics are determined solely by the mean photon number, plotting the experimental data against a Poissonian distribution would not provide significant insights. We used a large sample set, and it's known that any distribution tends to approximate a Gaussian distribution with large samples. However, we do not claim that the sources follow a Gaussian distribution. Instead, using a Gaussian distribution is a mathematical aid to experimentally calculate the cross-correlation since it is characterized by both mean and variance. These plots, based on fitted data, compare the fluctuations of all four sources at a specific μ value. The shaded region's area represents the probability of no detection, as counts cannot be negative.

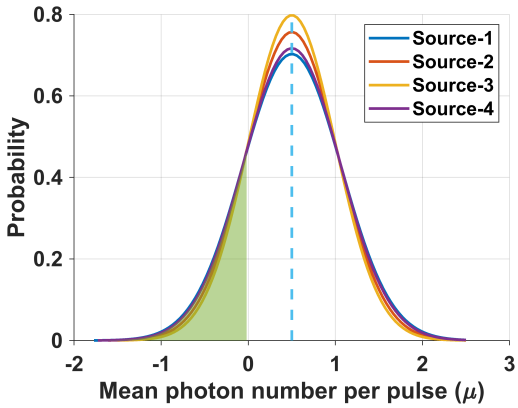


Figure 4.6: The distribution of all four sources at an average value of 0.5 photons per pulse

The correlations and possible information leakage are presented in Table 4.3. Main-

taining consistency and uniformity among the sources is vital to prevent disparities. Diverse intensity fluctuations among the sources might enable Eve to extract information, potentially leading to a side-channel attack. By examining the pairwise correlations among all the sources, we aim to circumvent Eve's attempts to gather information between bits or across basis. Therefore, accurately estimating the extent of information leakage is crucial for ensuring secure quantum communication.

Sources	R	I(A:E)
S1 & S2	0.9904	0.0027
S1 & S3	0.9715	0.0082
S1 & S4	0.9993	0.0002
S2 & S3	0.9949	0.0014
S2 & S4	0.9948	0.0014
S3 & S4	0.9796	0.0058

Table 4.3: The correlations R and the potential information leakage $I(A : E)$ among different sources.

4.5 Summary and Conclusion

The WCPs utilized in QKD implementations adhere to a Poisson distribution. Accurately characterizing this source is crucial to accurately estimate potential information leakage arising from multi-photon pulses. Since the SPADs employed are not photon-resolving, employing multiple on-off detectors offers enhanced resolution. For QKD applications, four SPADs are sufficient, given that the average photon number per pulse remains well below one. Inaccurate determination of the mean photon number could result in undetected information leakage, leaving the system vulnerable to adversarial attacks. Thus, comprehensive characterization of mean photon numbers in practical QKD systems employing weak coherent pulses is imperative. Discrepancies between the mean photon number and the resulting in-

formation leakage are assessed, with values escalating as the mean photon number increases. While the one-detector method suffices for smaller μ values ($\mu \leq 0.3$), beyond this threshold, the approximation deviates significantly from rigorous characterization.

The variations observed among the four sources differ, leading to a maximum information leakage of around 10^{-2} bits per pulse. These fluctuations become more pronounced as the intensity rises, highlighting the importance of assessing the intensity gap between the decoy and signal states. Significant differences could potentially open avenues for side-channel attacks by Eve. Calibrating commercial devices, including the QKD system, is crucial to comprehend their limitations. The study indicates that the information leakage grows as the mean photon number ($\mu \leq 1$) increases. Hence, for higher μ values, employing four detectors yields more accurate outcomes. Alternatively, utilizing number-resolving single-photon detectors is possible, but they are expensive and bulky.

Chapter 5

Entrapped Pulse Coincidence Detection Protocol

5.1 Introduction

We have consistently emphasized the significance of acknowledging device imperfections and loopholes in the security of QKD protocols. The presence of imperfect sources constitutes one such vulnerability. In many instances of prepare and measure protocols, weak coherent pulses (WCPs) are utilized instead of a single photon source (SPS). These WCPs adhere to Poissonian statistics, meaning there is a chance of multi-photon pulses. An attacker could exploit the occurrence of multiple photons in a pulse to execute a photon number splitting (PNS) attack and extract information from the shared key.

To mitigate the vulnerabilities exposed in the practical application of QKD protocols, we have two options: transition to a more resilient protocol or apply security

patches to counter known attacks. Security patching involves careful monitoring of various system parameters to identify and rectify potential information leaks. By considering imperfections in the source, we can gauge the information leakage stemming from pulses containing multiple photons. The introduction of security proofs accommodating device imperfections can be found in the literature [17, 19, 51]. Furthermore, researchers in [70] suggested using decoy states as a defence against the PNS attack. The integration of ideas from [19] and [70] laid the groundwork for the decoy state protocol [71–73], which stands as one of the most widely employed QKD protocols.

Monitoring coincidences serves as an alternative strategy to counter PNS attacks. It involves comparing the anticipated and observed coincidences at the recipient's end when a source emits weak coherent pulses with known photon statistics through a well-defined channel. Previous investigations [102–104] have proposed this method to restrict the eavesdropper's access to the key information, with some proposing its utilization to augment the key rate. However, [105] warns about the potential for an eavesdropper to execute a sophisticated PNS attack by replicating detector statistics.

In this study, we suggest merging the decoy state protocol with coincidence detection as a countermeasure against a wide range of advanced PNS attacks. Following convention, we designate the sender as Alice, the receiver as Bob, and the adversary as Eve. We monitor coincidences not only for the signal but also for the decoy states. Since Eve lacks information regarding the transmission of a signal or decoy, it becomes impractical for her to replicate the receiver's statistics accurately. This augmentation complements the standard decoy state protocol, thus bolstering security measures. Consequently, even if Eve succeeds in replicating statistics on average at Bob's end through various strategies, disparities between the yield of signal and decoy pulses emerge. By incorporating two-fold coincidences, we can

attain heightened key rates while fortifying security against sophisticated PNS attacks employing decoy states. To avoid confusion with the decoy state protocol, we will refer to these extra pulses as entrapped pulses. We will call this the entrapped pulse coincidence detection (EPCD) protocol. This integration of entrapped pulses and coincidence detections allows us to strategically exploit their functionalities.

If the observed coincidences suggest that a PNS attack has not been executed, we include the effects of two-photon gain (Q_2) and error (e_2) in the asymptotic key rate, as outlined in [104]. Additionally, if security against the unambiguous state discrimination (USD) attack is desired, it becomes impossible to integrate contributions from three or higher photon gains and error terms. Given the added considerations from the statistics of two-photon events, it becomes essential to devise a method for establishing stringent bounds on the achievable key rates within the protocol.

It is challenging to compute the key rates of a general QKD protocol. It is difficult to obtain tight lower bounds using analytical techniques since key rate estimation involves solving a nonlinear optimization problem with many variables. Computing lower bounds on key rates by making approximations as in [73] often leads to pessimistically underestimated key rates.

Many studies [106–112] propose novel techniques to obtain good lower bounds on the secure key rate. Obtaining tight bounds on the key rates based on the generalized decoy state protocol has been of interest, and several novel techniques [106–112] have been proposed that successfully compute good lower bounds on the rates. A common approach involves recasting the decoy state protocol into an entanglement-based protocol, followed by conducting a security analysis of this revised protocol. These techniques leverage advanced results in convex optimization and serve as

highly effective tools for computing key rates of any general QKD protocols.

In this work, we introduce a simple-to-implement method to derive tight bounds on the key rates. Our method differs from the previous approaches. Our approach relies on formulating the optimization problem for computing the key rate as a series of converging polynomial optimization problems, each of which can be efficiently solved using well-established numerical techniques. Implementing our method is straightforward and can be easily coded.

Although, in principle, it is feasible to compute arbitrarily tight bounds on the key rate, doing so requires increased computational time and resources. In practice, our method yields reasonably tight key rates within just a few minutes when executed on a personal computer with a standard configuration. Subsequently, we utilize the suggested protocol and key rate calculation method in a free-space QKD implementation. Through our method, we illustrate that our proposed protocol outperforms the decoy state protocol when coincidence monitoring certifies the absence of the PNS attack [36].

Our protocol employs entrapped pulses and monitors coincidences, necessitating proper source and channel characterization. The channel transmittance must be known and trusted, as this is crucial for defending against photon-number-splitting (PNS) attacks through coincidence monitoring. We assume the asymptotic limit in our analysis, with finite key analysis planned for future research. Our protocol is designed to be secure against passive and active attacks; any interference by an eavesdropper (Eve) would be detected due to the disturbance introduced in the quantum states. Thus, our protocol provides a robust security framework, even under an active attack, ensuring reliable QKD implementation.

This chapter is structured as follows. In Sec. 5.2.4, we present the protocol, while

Sec. 5.3 outlines our approach for calculating the secret key rate associated with the protocol. Sec. 5.4 provides details regarding the experimental setup and the method utilized for data analysis. Our experimental findings and the implementation of Semi-Definite Programming (SDP) for key rate computation are discussed in Sec. 5.5, followed by concluding remarks in Sec. 5.6.

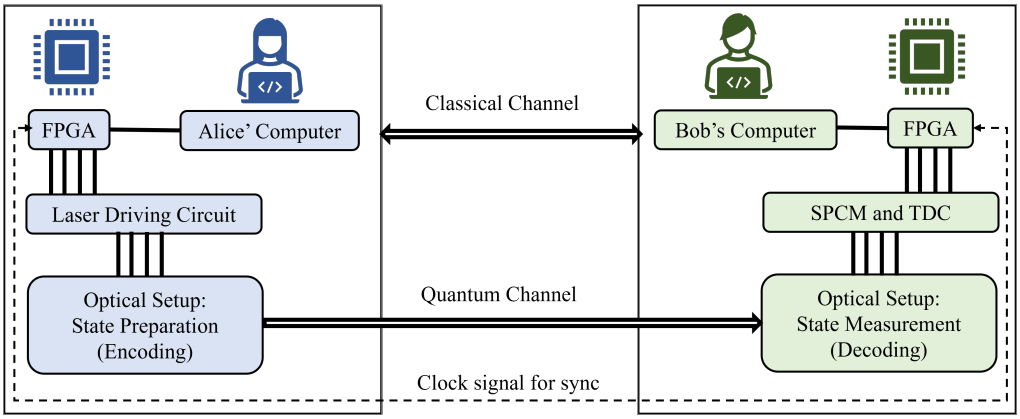


Figure 5.1: Standard Scheme for Quantum Communication in free space with existing classical systems

5.2 Theoretical background

The BB84 protocol's implementation with weak coherent pulses is vulnerable to PNS attacks, wherein Eve exploits the multi-photon pulses sent by Alice. Traditional mitigation against PNS attacks, such as the decoy state protocol, involves sending occasional decoy pulses along with signal pulses. An alternative strategy, proposed by [104] and [103], suggests monitoring coincidences at Bob's end to detect PNS attacks. The protocol proposed in this work involves implementing modifications at both Alice's and Bob's ends. Specifically, entrapped pulses are transmitted from Alice's end, and Bob's end is equipped to monitor coincidence detections. This approach effectively mitigates PNS attacks and leads to a notable enhancement in key rates. In this section we first discuss the secure key rates for

decoy and CD protocol, and then define our EPCD protocol, along with the methods to compute key rates.

5.2.1 Secure key rate: Decoy state Protocol

We employ weak coherent pulses in practical implementations of the BB84 protocol hence, there is a non-zero probability of multiphoton pulses. However, we only consider the contributions from the single-photon pulses in the key rate. The asymptotic secure key rate [73] is given as:

$$R \geq \frac{1}{2}\left\{-Q_\mu H_{\text{bin}}(E_\mu) f(E_\mu) + Q_1\left(1 - H_{\text{bin}}(e_1)\right)\right\}. \tag{5.1}$$

Here, μ is the mean photon number of the signal pulses, Q_μ is the overall gain of signal states, E_μ is the overall quantum bit error (QBER), Q_1 is the gain of single-photon states, e_1 is the error rate of single photon states and $H_{\text{bin}}(e)$ is the binary entropy.

Q_μ and E_μ are the experimental parameters, however Q_1 and e_1 needs estimation. For the case with only one decoy, traditional analytical methods in [73] compute lower bounds on the key rate by establishing bounds on Q_1 and e_1.

5.2.2 Secure key rate: Coincidence Detection Protocol

We can detect a PNS attack by monitoring the coincidences, given a well-characterized source and channel. This monitoring allows us to determine whether the photon statistics have been altered or remain unchanged [103]. If the statistics are unchanged, we are assured that no PNS attack has been performed. However, Eve can still perform the collective and unambiguous state discrimination (USD) attack [113].

Let us consider the collective attacks without the USD attack. The attack results in the maximum mutual information between Alice and Eve, $I(A;E)_i$, which can be expressed as [104]:

$$I(A;E)_i = H_{\text{bin}}\left(\frac{1+\cos^i c}{2}\right), \tag{5.2}$$

where $\cos c = 1 - 2e_i$. The key rate is given as;

$$R \geq \frac{1}{2}\left\{-Q_\mu f(E_\mu) H_{\text{bin}}(E_\mu) + Q_1\left[1 - H_{\text{bin}}(e_1)\right] + \sum_{i=2}^{\infty} Q_i\left(1 - I(A;E)_i\right)\right\}, \tag{5.3}$$

Here, i represents the state containing i number of photons. Q_i and e_i are the gain and error rate of this i-photon state, respectively. $H_{\text{bin}}(e)$ is the binary entropy.

Now, we consider when Eve performs collective and USD attacks. If Eve employs the USD attack, it will certainly fail on two-photon pulses but might have a non-zero success probability with three or more photon pulses [113]. Hence, we consider the contributions due to just single and two-photon states.

$$\begin{aligned} R \;\geq\; & \frac{1}{2}\{-Q_\mu H_{\text{bin}}(E_\mu) f(E_\mu) + Q_1\left(1 - \Phi(2e_1 - 1)\right) \\ & + Q_2\left(1 - \Phi((2e_2-1)^2)\right)\}. \end{aligned} \tag{5.4}$$

Where $\phi(x)$ is defined as follows:

$$\Phi(x) \;:=\; H_{\text{bin}}\left(\frac{1}{2} + \frac{x}{2}\right). \tag{5.5}$$

Here, Q_2 and e_2 denote the two-photon gains and error rates, respectively. When calculating the secure key rates for the protocol, the values of gains Q_1, Q_2, and the error rates e_1,e_2, are unknown. In a typical decoy state protocol employing an infinite number of decoy states, accurate estimation of values is achievable. Nevertheless, this method demands significant resources and is practically unattainable. Study [73] suggested utilizing approximations with a single decoy state, but these

approximations tend to underestimate the key rates. Here, we propose leveraging the current setup by utilizing coincidences alongside optimization techniques to establish tighter bounds on the key rates. In Sec. 5.3, we elaborate on our methodology for computing key rates.

5.2.3 Monitoring Coincidences

We monitor the coincidences to examine if the photon statistics have been altered or if they remain unchanged[103]. If altered, we can compute rates using Eq. (5.1). Conversely, if the detected coincidences match the expected statistics, we can conclude that no PNS attack has occurred, and the key rate can be calculated using Eq.(5.4). Now, we discuss the estimation of coincidences for a characterised source and channel. The coincidences depend on both the statistics of the source as well as the overall transmittance.

The probability that Alice emits an n photon pulse is given by $P(n)$,

$$P(n) = \frac{e^{-\mu}\mu^n}{n!} \tag{5.6}$$

Then the overall efficiency η for detection by Bob of a single photon sent by Alice is (See 2.4.6),

$$\eta = t_{AB} \cdot \eta_{Bob} \tag{5.7}$$

where t_{AB} is channel transmissivity and η_{Bob} is the detection efficiencies at Bob's end, including optical and detector efficiency. We can replace all the losses in the channel, Bob's optics and the detection efficiencies by a beam splitter of transmittance η. If we consider each photon in a pulse independent of each other, then the probability of detection of each photon is η. Thus, We can monitor the coincidences by comparing the expected coincidences to the observed ones as presented in [103].

We consider the case when a pulse containing n photons ($|n\rangle$) falls on the $50:50$ beam splitter.

$$|n\rangle \rightarrow \sum_{k=0}^{n} \binom{n}{k} |n-k\rangle_R |k\rangle_T \tag{5.8}$$

We now discuss the case of our interest, when two photons pulse emitted by Alice. The probability of getting two-fold coincidence only occurs when both the photons exit from different parts of the beam splitter, i.e. case II in Table. 5.2.3 which has the probability $1/2$.

Cases	Transmitted Photons	Reflected Photons	Probability
I	2	0	1/4
II	1	1	1/2
III	0	2	1/4

Table 5.1: Cases and probabilities when two photons are incident on Bob's beam splitter.

The probability that Alice emits a two-photon pulse is $e^{-\mu}\mu^2/2$. The overall probability that these two photons reach Bob's detection setup after passing the quantum channel and get detected as a two-fold coincidence is $e^{-\eta\mu}\mu^2\eta^2/4$. Since this probability is directly related to η^2, the coincidence rates will be suppressed quadratically with losses in the channel. We characterize the source and the channel well and can estimate the expected number of coincidences and check for a PNS attack [103].

5.2.4 EPCD Protocol

We now define our protocol of using entrapped pulses along with the two-photon coincidences, i.e. entrapped pulse coincidence detection (EPCD) protocol.

Protocol (Entrapped Pulse Coincidence Detection Protocol (EPCD))**.** *In this protocol, we present a comprehensive approach to utilizing entrapped pulses, along with monitoring coincidences. Alice sends a signal characterized by an average photon*

number ν_0, along with K entrapped pulses characterized by average photon numbers $\nu_1, \nu_2, \cdots, \nu_K$. For a sequence of n pulses, each identified by an index i, the subsequent actions are iterated for each pulse.

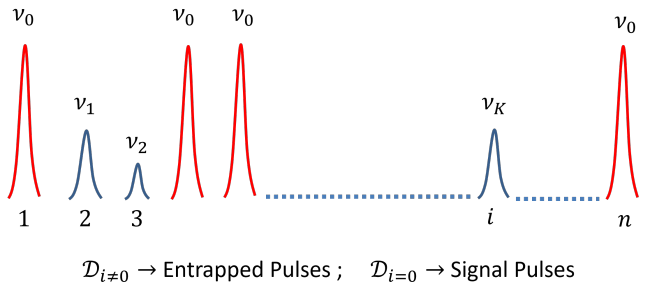


Figure 5.2: Graphical representation of signal and entrapped pulses randomly transmitted by Alice

1. ***State preparation (Alice's lab):*** *Alice generates random numbers $\mathcal{D}_i \in \{0, 1, \cdots K\}$, $\mathcal{X}_i \in \{0, 1\}$ and $\mathcal{A}_i \in \{0, 1\}$. Where,*

   (a) *$\mathcal{D}_i$ determines whether a signal (ν_0) or an entrapped pulse ($\nu_1, \nu_2, \cdots \nu_K$) is transmitted. If $\mathcal{D} = d$ then mean photon number is ν_d*

   (b) *$\mathcal{X}_i$ determines the basis in which pulse i is encoded. If $\mathcal{X}_i = 0(1)$, she encodes in Standard (Hadamard) basis.*

   (c) *$\mathcal{A}_i$ is the bit value encoded for pulse i.*

2. ***State transmission:*** *Alice sends the prepared state to Bob through a quantum channel.*

3. ***State measurement (Bob's lab):*** *Bob lets the pulse pass through a beam splitter, having two ports $\mathfrak{B}^{(0)}$ and $\mathfrak{B}^{(1)}$. At wing, $\mathfrak{B}^{(0)}$ ($\mathfrak{B}^{(1)}$) Bob performs measurement in the Standard (Hadamard) basis. Let $\mathcal{B}_i^{(j)}$ denote the measured bit value for the pulse i in port j.*

4. *Alice and Bob continue to prepare and measure, incrementing the value of* i *to* $i+1$ *until* $i = n$*. Once* $i = n$*, they proceed to the next step.*

5. *Alice publicly discloses the value of her basis* $(\mathcal{X}_1, \mathcal{X}_2, \cdots, \mathcal{X}_n)$.

6. *Let* $\mathcal{Y}_i$ *denote Bob's basis choice and* $\mathcal{B}_i$ *is the measured bit value. No measurement outcome is denoted as* $\perp$.

   (a) *If* $\mathcal{B}_i^{(j\oplus 1)} = \perp$ *and* $\mathcal{B}_i^{(j)} \in \{0,1\}$*:* $\mathcal{Y}_i = j$ *,* $\mathcal{B}_i = \mathcal{B}_i^{(j)}$.

   (b) *If* $\mathcal{B}_i^{(0)}, \mathcal{B}_i^{(1)} \in \{0,1\}$*, then Bob sets* $\mathcal{Y}_i = x$ *and* $\mathcal{B}_i = \mathcal{B}_i^{(x)}$ *if* $\mathcal{X}_i = x$.

   (c) *Else Bob sets* $\mathcal{Y}_i$ *randomly and* $\mathcal{B}_i = \perp$.

7. *Bob publicly discloses the values of the basis* $(\mathcal{Y}_1, \mathcal{Y}_2, \ldots, \mathcal{Y}_n)$*. Alice and Bob then discard the rounds in which* $\mathcal{X}_i \neq \mathcal{Y}_i$*, i.e., they only focus on the rounds from the set* $\mathfrak{h} := \{i \in \{1, 2, \ldots, n\} : \mathcal{X}_i = \mathcal{Y}_i\}$.

8. *Alice also discloses the entrapped pulses used in each round* $(\mathcal{D}_1, \mathcal{D}_2, \cdots, \mathcal{D}_n)$.

9. *Alice and Bob perform error correction and privacy amplification as in standard BB84 protocol. From any randomly chosen subset* $\mathfrak{g} \subset \mathfrak{h}$*, with* $|\mathfrak{g}| \ll |\mathfrak{h}|$ *they estimate Gains (probability that a signal sent by Alice is received by Bob):*

$$Q_{\nu_d} := \frac{|\{i \in \mathfrak{g} : \mathcal{D}_i = d, \mathcal{B}_i \neq \perp\}|}{|\{i \in \mathfrak{g} : \mathcal{D}_i = d\}|} \tag{5.9}$$

   and QBER (E_{ν_d}) *i.e. the probability that Alice's bit value does not match with Bob's bit value* $(\mathcal{A}_i \neq \mathcal{B}_i)$ *whenever they both prepared and measured in same basis* $(\mathcal{X}_i = \mathcal{Y}_i)$*):*

$$E_{\nu_d} := \frac{|\{i \in \mathfrak{g} : \mathcal{D}_i = d, \mathcal{A}_i \neq \mathcal{B}_i\}|}{|\{i \in \mathfrak{g} : \mathcal{D}_i = d\}|} \tag{5.10}$$

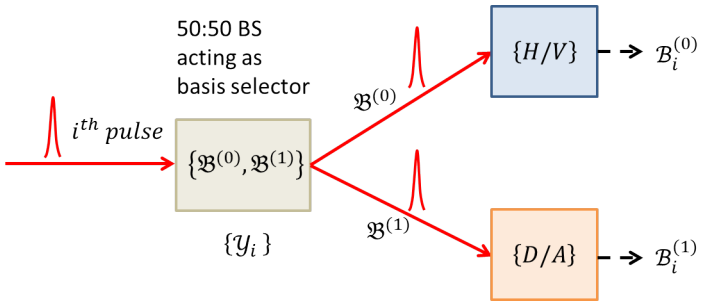


Figure 5.3: Graphical representation of basis selection and recorded measurements at Bob's end for i^{th} pulse

The above is a generalised description of the protocol; for consistency, we will use $\nu_0 = \mu$ to represent the mean photon number of the signal state. The implementation of the standard decoy state protocol closely follows the procedure outlined in the above protocol, involving one beam splitter and two branches denoted as $\mathfrak{D}^{(0)}$ and $\mathfrak{D}^{(1)}$. While measurements in the standard basis are performed by $\mathfrak{D}^{(0)}$, $\mathfrak{D}^{(1)}$ conducts measurements in the Hadamard basis. The primary distinction lies in the coincidence monitoring, with no significant impact on the experimental feasibility of the protocol. The experimental demonstration of this protocol is discussed in Sec. 5.4.

As noted in [102–104], it has been observed that the PNS attack can be detected by simply measuring the coincidences, even without the presence of entrapped pulses. However, Eve can mimic the photon statistics at Bob's end [105] if we only send the signal without the entrapped pulses. Nevertheless, this type of attack can be effectively countered by employing entrapped pulses. Since the adversary is uncertain whether the transmitted state is an entrapped pulse, she cannot replicate the photon statistics for both the signal and the entrapped pulses.

5.3 Computing Key-rate

We first discuss the computation of the key rate for coincidence detection given by Eq.(5.4). Recalling discussion in Sec. 2.4.6, and using Eq.(2.138) in Eq.(5.4) we get,

$$\begin{aligned} R \;\geq\; & \frac{1}{2}\Big\{ - Q_\mu H_{\text{bin}}(E_\mu) f(E_\mu) + Y_1 \mu e^{-\mu} \left(1 - \Phi(2e_1 - 1)\right) \\ & + Y_2 \frac{\mu^2}{2} e^{-\mu} \left(1 - \Phi((2e_2 - 1)^2)\right) \Big\}. \end{aligned} \tag{5.11}$$

where we have substituted, $Q_1 = Y_1 \mu e^{-\mu}$ and $Q_2 = Y_2 \frac{\mu^2}{2} e^{-\mu}$, using Eq.(2.138). Here, Y_1 and Y_2 are single and two-photon yields, respectively.

We know that Q_μ and E_μ are experimental parameters hence, the optimisation problem reduces to the last two terms of Eq.(5.11). We take out the common factor of $e^{-\mu}$. Hence, the key rate can be obtained by solving the following optimization problem:

$$\begin{aligned} r := \min & \left(Y_1 \mu \left(1 - \Phi\left(2e_1 - 1\right)\right) + Y_2 \frac{\mu^2}{2} \left(1 - \Phi\left((2e_2 - 1)^2\right)\right) \right) \\ \text{s.t.} \forall k: \quad & Y_k, e_k \in [0, 1] \\ \forall d: \quad & Q_{\nu_d} e^{\nu_d} = \sum_{k=0}^{\infty} Y_k \frac{\nu_d^k}{k!} \\ \forall d: \quad & E_{\nu_d} Q_{\nu_d} e^{\nu_d} = \sum_{k=0}^{\infty} e_k Y_k \frac{\nu_d^k}{k!} \end{aligned} \tag{5.12}$$

The reason for performing such an optimization is straightforward to understand. The objective function of the optimization problem concerns the key rate R (refer to Eq. (5.4)). This key rate relies on the k photon yields Y_k and k photon error rates e_k, which are not directly known from experimental statistics. However, what is known are the overall gain Q_μ and the QBER (E_μ). When we consider just the coincidence

detection protocol, the constraints of the optimization problem are related just to the Gain and QBER of the signal. However, when we include the entrapped states, we get an extra set of constraints on the optimization problem from the Gain and QBER of the signal and the decoy states. The more decoy states, the better; however, for practical reasons, we have constrained ourselves to just a single decoy state.

Now we consider the cases when coincidences are not considered, i.e. the cases of BB84 and decoy state protocol. The key rate to be estimated is given by,

$$R \;\geq\; \frac{1}{2}\left\{-Q_\mu H_{\text{bin}}(E_\mu) f(E_\mu) + Y_1 \mu e^{-\mu}\left(1 - \Phi(2e_1 - 1)\right)\right\}. \tag{5.13}$$

In this case, the optimization problem for computing the key rate differs from Eq. (5.12) only in the objective function. Specifically, it does not include contributions from the two-photon terms Y_2 and e_2. Hence, the optimisation problem is:

$$\begin{aligned} r := \min &\left(Y_1 \mu \left(1 - \Phi\left(2e_1 - 1\right)\right)\right) \\ \text{s.t.}\forall k: &\quad Y_k, e_k \in [0,1] \\ \forall d: &\quad Q_{\nu_d} e^{\nu_d} = \sum_{k=0}^{\infty} Y_k \frac{\nu_d^k}{k!} \\ \forall d: &\quad E_{\nu_d} Q_{\nu_d} e^{\nu_d} = \sum_{k=0}^{\infty} e_k Y_k \frac{\nu_d^k}{k!} \end{aligned} \tag{5.14}$$

It is to be noted that for the non-decoy case $d = 0$, there is just a single intensity, $\nu_0 = \mu$. For the decoy state, the number of constraints depends on the number of decoy states employed.

Given that no assumptions can be made about the Yields $Y_k \in [0,1]$ and error rates $e_k \in [0,1]$, we acknowledge the possibility of a potential adversary to manipulate them freely. The adversary is, in principle, unrestricted in choosing any values for these parameters, provided that the chosen values align with the observed experimental statistics. This fact is captured using the constraints in the optimization

problem, limiting the choice available to the adversary. To account for the strategy that is most advantageous to the adversary within these constraints, we minimize the rate.

In the literature, Ma et al. [73] conducted the first comprehensive exploration of lower bounds on the asymptotic key rates for the decoy state protocol. For the case with only one decoy, traditional analytical methods compute lower bounds on the key rate by first establishing bounds on Y_1 and e_1:

$$Y_0 \leq Y_0^U := \frac{E_\nu Q_\nu e^\nu}{e_0}, \tag{5.15}$$

$$Y_1 \geq Y_1^L := \frac{\mu}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \left(\frac{\nu^2}{\mu^2}\right) - Y_0^U \left(\frac{\mu^2 - \nu^2}{\mu^2}\right)\right), \tag{5.16}$$

$$e_1 \leq e_1^U := \frac{E_\nu Q_\nu e^\nu}{Y_1^L \nu} \tag{5.17}$$

Exploiting the monotonicity properties of binary entropy, specifically that $H_{\text{bin}}(x)$ is increasing for all $x \in [0, 1/2]$, and the fact that $(1 - H_{\text{bin}}(x)) > 0$, a lower bound on the secure key rate (5.13) is given by:

$$R \geq \frac{1}{2}\Big\{ - Q_\mu f(E_\mu) H_{\text{bin}}(E_\mu) + Y_1^L \mu e^{-\mu} \left(1 - H_{\text{bin}}(e_1^U)\right) \Big\}. \tag{5.18}$$

An immediate approach to computing lower bounds on the key rate for the protocol with coincidence detection involves employing similar analytic techniques to establish upper and lower bounds, denoted as Y_2^L and e_2^U, on Y_2 and e_2 respectively, that are compatible with the constraints. However, this process is tedious, and tight bounds may not be easily found. The next section introduces a simple-to-implement method to iteratively derive bounds on the key rate that converge to the asymptotic key rate from below.

5.3.1 Solving the optimization problem

Two primary challenges emerge when addressing optimization problem Eq. (5.12). First, the problem is non-convex due to the non-convex nature of both the constraints and the objective function in Eq. (5.12). General optimization problems are notoriously difficult to solve due to their abstract nature unless they fit specific classes of convex optimization problems. As a result, the optimization problem cannot be solved directly using conventional techniques. Second, the optimization problem involves infinitely many free parameters, namely, Y_k and e_k. The presence of these infinitely many parameters adds further complexity to the problem.

The challenge of dealing with infinitely many variables can be addressed straightforwardly by recognizing that the contribution of Y_k and e_k when $k \gg 1$ is negligible to the sums $\sum_k (\nu_d^k/k!\,)Y_k$ and $\sum_k (\nu_d^k/k!\,)Y_k e_k$. Consequently, we relax the constraints of Eq. (5.12) by truncating the infinite sums $\sum_k (\nu_d^k/k!\,)Y_k$ to involve sums over a finite number of variables. This comes, however, with a small penalty that depends on the number of terms kept in the sum. We formally implement this truncation in the Appendix. B.1.

We begin by discussing our general technique for addressing certain simple non-polynomial optimization problems, drawing inspiration from [114, 115]. This method involves deriving lower bounds for optimization problems through the partitioning of the parameter space into smaller sub-spaces. Formally, this partition (or grid), denoted as $\mathcal{P}$, divides the space into multiple sub-domains $\{\mathcal{C}_i\}_i$. For each sub-domain $\mathcal{C}_i$, we formulate a new optimization problem (or sub-problem) by constraining the parameters to that sub-domain. Each sub-problem can be lower-bounded by a polynomial optimization problem using simple methods, such as Taylor's theo-

rem, with only a minimal loss of tightness. Obtaining lower bounds on the resulting sub-problems is achieved by computing the Semi-definite Programming (SDP) relaxations of the polynomial optimization problem (in practice, this is done using software tools like NCPOL2SDPA [116]). Detailed information on partitioning and lower-bounding the sub-problems generated by any given partition is formally done in Appendix-C.3 of [117].

The solutions to the optimization problems can be improved by refining the partition so that the sub-domains have smaller dimensions. Typically, if the partitioning is done over the parameter space of P independent parameters, then enhancing tightness by a factor of β would require computing β^P times more sub-problems. Consequently, this technique is particularly applicable and effective when partitioning is applied to a relatively smaller number of parameters.

Now let us return to the optimization problem at hand. There are only two non-polynomial terms $\Phi(2e_1 - 1)$ and $\Phi((2e_2 - 1)^2)$ in the optimization problem. Furthermore, only two parameters, e_1 and e_2, contribute to the non-polynomial terms in the problem. As e_1 and e_2 are both constrained within the range of $[0, 1]$, we construct a partition $\mathcal{P}$ of the set $[0, 1] \times [0, 1]$, generating rectangular sub-domains $\mathcal{C}_i$. Leveraging the properties of the function $\Phi(x)$, we find the constants $\xi_{1,i}^{\max}$ and $\xi_{2,i}^{\max}$ that (tightly) lower bound the functions $\Phi(2e_1 - 1)$ and $\Phi((2e_2 - 1)^2)$ respectively in the sub-domain $\mathcal{C}_i$[1](See Lemma 3, Appendix-C.3 of [117]). We then use these tight bounds to lower-bound the objective function as follows

$$\sum_{k\in\{1,2\}} Y_k \frac{\mu^k}{k!} \left(1 - \Phi\left((2e_k - 1)^k\right)\right) \geq \sum_{k\in\{1,2\}} Y_k \frac{\mu^k}{k!} \cdot \left(1 - \xi_{k,i}^{\max}\right). \tag{5.19}$$

The loss in tightness when bounding the objective functions by such constants $\xi_{1,i}^{\max}$

[1]To minimize the objective function, a lower-bound on $-\Phi((2e_k - 1)^k)$ is needed.

and $\xi_{2,i}^{\max}$ depend upon the dimensions of the domain $\mathcal{C}_i$. Thus, the loss of tightness can be made arbitrarily small by refining the partition. However, making a finer partition comes at the expense of higher computation time, as more and more sub-problems need to be numerically solved.

All the results lead to the following final result, which forms the basis of the algorithm for computing key rate r (as defined in equation Eq. (5.12)).

Theorem 1(Informal): *Consider a partition $\mathcal{P} = \{\mathcal{C}_i\}_i$ of the interval $[0,1] \times [0,1]$. The minimum achievable value $r \geq \min_i \{r_n(\mathcal{C}_i)\}_i$, where each $r_n(\mathcal{C}_i)$ corresponds to the solution of a polynomial optimization problem over $2n$ number of variables (given by equation C.12, [117]). Moreover, for any given (arbitrarily small) margin of error $\epsilon > 0$, there exists (a sufficiently large) n and a (sufficiently fine) partition $\mathcal{P}$ such that the difference $|r - \min_i \{r_n(\mathcal{C}_i)\}_i|$ is at-most ϵ.*

In essence, this result implies that the lower bounds can be determined with arbitrarily high precision by solving multiple polynomial optimization problems and then computing the minimum of all the results obtained.

Assuming a random background with errors occurring equally likely, we explicitly set the background error rate as $e_0 = 1/2$. To account for the impact of finite statistics on the experimental values Q_μ, Q_ν, E_μ, and E_ν, it is imperative to consider uncertainties in their measurement. In Appendix E, Theorem-1 of [117]is modified to accommodate these statistical uncertainties in the computation of rates. It is important to note that the key rates reported here are in the asymptotic limit. However, this analysis only serves to acknowledge the uncertainty associated with experimentally observed values, and the computed rates are still asymptotic key rates compatible with experimentally obtained statistics with relevant uncertainties in observed values. The computation of finite-round statistics can, in principle, be

performed using theoretical tools such as the Generalized Entropy Accumulation Theorem [118, 119]. Such analysis would require a more sophisticated analysis and is reserved for future work.

5.4 Experimental Method

This section outlines the experimental procedures involved in implementing our secure QKD protocol. The experimental setup consists of three main stages: state preparation, transmission, and state measurement.

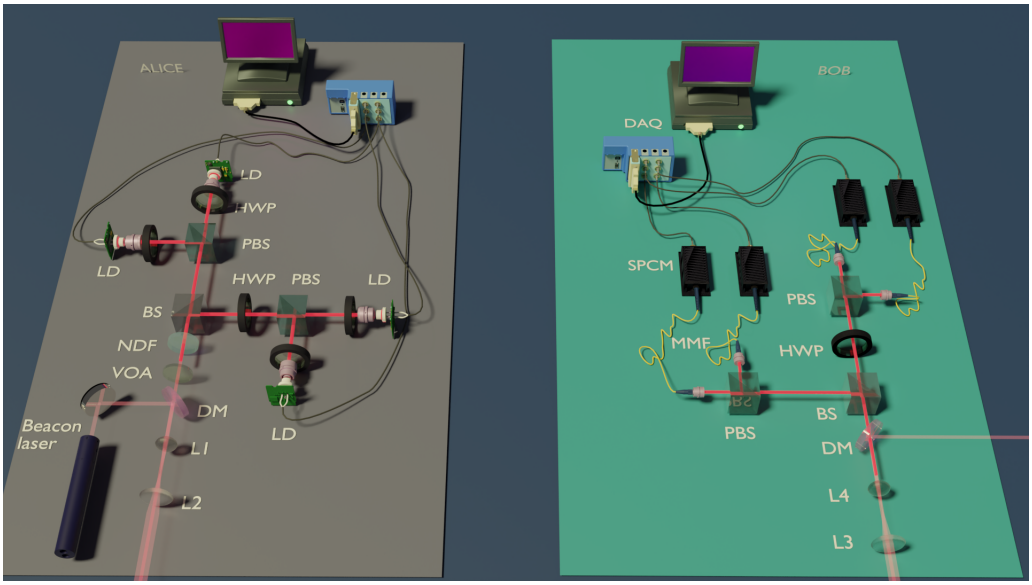


Figure 5.4: Schematic of the experimental setup. It includes both the optics and electronic components. LD: Laser Diodes, HWP, Half Wave Plate, BS: Beam Splitter, PBS: Polarising Beam Splitter, NDF: Neutral Density Filter, VOA: Variable optical Attenuator, DM: Dichroic Mirror, L: lens, MMF: Multi-Mode Fibre, SPCM: Single Photon Counting Module, DAQ: Data Acquisition system

5.4.1 State Preparation: Alice

Alice utilizes the polarization state of weak coherent pulses to encode the quantum information for transmission. Weak coherent pulses are generated by attenuating the laser pulses using neutral density filters. Our experimental setup (see Fig. 5.4) includes four laser diodes operating at a wavelength of 808 nm (Thorlabs $L808P010$). An in-house designed laser driving circuit, controlled by a Field Programmable Gate Array (FPGA), activates the laser diodes. This setup generates pulses at a frequency of 5 MHz, with each pulse having an optical width of 1 ns. These pulses are then optically engineered to create four polarizations—horizontal (H), vertical (V), diagonal (D), and anti-diagonal (A)—using polarizing beam splitters (PBS) and half-wave plates (HWP). The combination of PBS and HWP acts as a polarizer and assists in pulse attenuation. The FPGA ensures the lasers are randomly triggered to produce the four polarization states. We have analyzed all four sources to address potential issues like pulse width, wavelength variations, and power discrepancies [76]. After combining all pulses on a beam splitter (BS), the signal passes through a fixed and variable neutral density filter (NDF), reducing the intensity further. The variable NDF is adjusted to modify signal intensity, quantified in terms of mean photon number, as described in [120]. The decoy pulses are generated using this variable NDF by changing the intensity of the pulses. This enables us to conduct a proof of principle decoy state QKD, using the pulses at two different intensities for generating the signal and the decoy pulses. Thereafter, Alice sends the encoded signal and decoy pulses to Bob via the free space channel.

5.4.2 Transmission: The Channel

The communication signal is sent to Bob via a free-space channel. At the Thaltej campus of the Physical Research Laboratory (PRL) in Ahmedabad, Gujarat, India, two adjacent buildings are involved in the communication setup. Both the sending and receiving stations are located in rooms on the rooftop of the first building. A reflector positioned on the second building aids in directing the signal towards Bob. The channel is then characterized for the losses, where we have included the losses due to launching and collecting optics in the channel loss itself. The channel was characterized using the beacon laser of 633 nm, giving the transmittance of 86%. The experimental parameters and their values are specified in Table. 5.2. We have conducted our experiment in a natural environment rather than a controlled laboratory setting, deliberately incorporating atmospheric interference and night lighting variables. This approach ensures a more comprehensive and realistic assessment, enhancing the credibility and applicability of our findings.

Parameter	Value
Channel Transmission	0.86
Pulse width	1 ns
Detection jitter	350 ps
Coincidence window	2 ns
Detection Efficiency	0.62
Coupling Efficiency	0.87
Dark counts	100 cps
Background counts	3000 cps

Table 5.2: The values for channel transmission, pulse width, detection jitter, coincidence window, detector efficiency and coupling efficiency, dark and background counts. The unit cps is for counts per second. The background and dark counts are the worst cases considered.

5.4.3 State Measurement: Bob

Upon reaching Bob, the signal is decoded through projective measurements onto four polarization states. The measurement basis is determined using a beam splitter (BS), with an HWP at 22.5 degrees in one path for diagonal basis and the other path for rectilinear basis. Signals are detected using single photon counting modules (Excelitas-SPCM-AQRH-14), and a high-performance data acquisition card records detection timestamps across various polarizations. The detection efficiency, coupling efficiency, dark counts and background counts were recorded and are reported in Table. 5.2. Due to the nature of our source as a WCP, coincidences can occur during detection. The coincidence window is kept as 2 ns. After sufficient quantum state exchange, Alice and Bob move on to post-processing.

5.4.4 Data Analysis and Postprocessing

We recorded the timestamps when each pulse of Alice was emitted in all four polarisations. Bob's recorded data comprises the timestamps for detection clicks in all four detectors. From Bob's time stamps, we estimated the singles and the coincidences. If only one detector clicks for a given time stamp, it is a single detection; otherwise, we record two, three and fourfold coincidences depending on the number of detectors giving a simultaneous click. Alice reveals her chosen basis publicly. For single detections, Bob retains those where his basis is compatible with Alice's basis. In the case of coincidence detection, Bob is only interested in two-fold coincidences, specifically those occurring in opposite basis. In such instances, Bob selects measurements aligned with Alice's basis choice. These steps correspond to Steps 5-8 outlined in the protocol detailed in Sec. 5.2.4. The refined bits from this process form the sifted key, a portion of which is used to assess the gain and quan-

tum bit error rate (QBER). This gain and QBER are then further used to estimate the bounds on the key rates of different protocols. The algorithm 2 of Appendix B.2

5.5 Results and discussion

Increasing the key rate in practical scenarios continues to be challenging, given that other approaches typically necessitate additional hardware or sophisticated optimization techniques for key extraction. To address this, we devised a middle-ground solution that demands minimal resources from both software and hardware perspectives. We conducted a comparative analysis of key rates across various protocols and evaluated the effectiveness of our key rate optimization method against several existing approaches.

We conducted a comparison between the traditional decoy-state method and the proposed SDP-based method to calculate lower bounds on secure key rates, as defined in Eq. (5.18). This comparison was carried out across various values of the mean photon number, illustrated in Fig. 5.5, by simulating the decoy-based BB84 protocol under different mean photon numbers. Throughout the simulation, the mean photon number of the decoy was held constant at $\nu = 0.1$. Our findings show that our proposed method yields tighter lower bounds compared to the traditional analytic method, achieving a 27% improvement at the optimal mean photon number ($\mu = 0.8$). This improvement indicates reduced key wastage in terms of resource utilization.

We utilized our SDP-based method to analyze key rates across four protocols: BB84, decoy state protocol, CD protocol, and EPCD protocol. Employing the SDP technique, we determined bounds on yields and errors to compute key rate bounds using Eq. (5.18) and Eq. (5.4). The respective key rates were plotted against

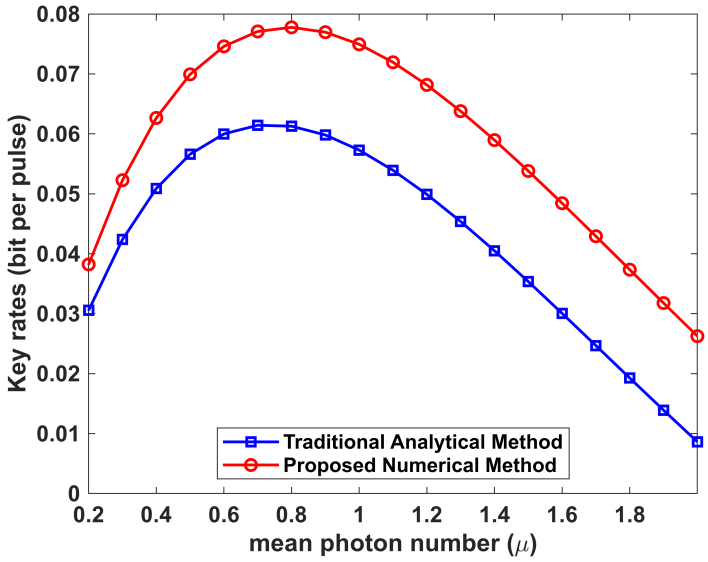


Figure 5.5: Key rates (bits per pulse) as a function of mean photon number (μ) for two cases: (i) traditional analytical technique and (ii) proposed numerical technique using simulated results

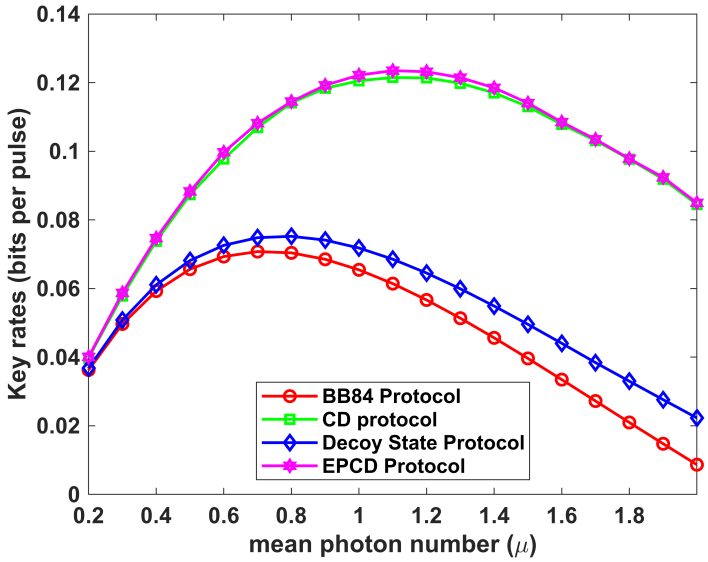


Figure 5.6: Simulated key rates (bits per pulse) as a function of mean photon number (μ) for four protocols: (i) BB84 Protocol, (ii) CD protocol, (iii) Decoy state protocol and (iv) EPCD protocol.

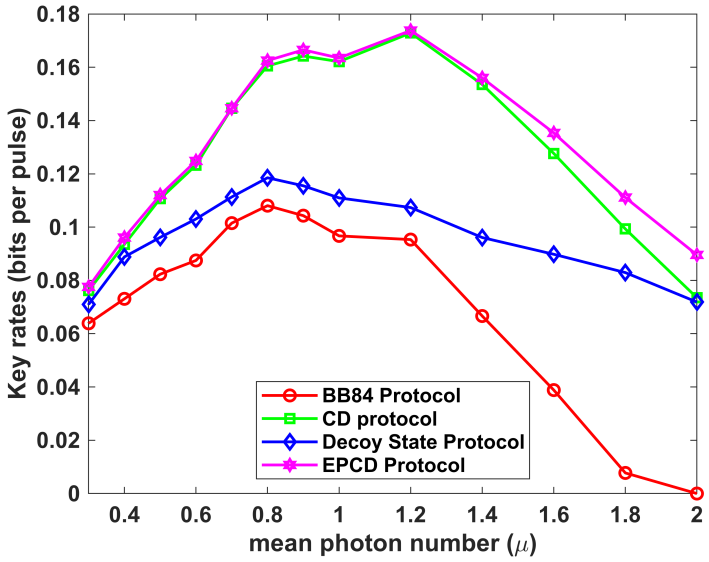


Figure 5.7: Experimental secure key rates (bits per pulse) as a function of mean photon number (μ) for four protocols: (i) BB84 Protocol, (ii) CD protocol, (iii) Decoy state protocol and (iv) EPCD protocol. Lines drawn are for the aid of the eye.

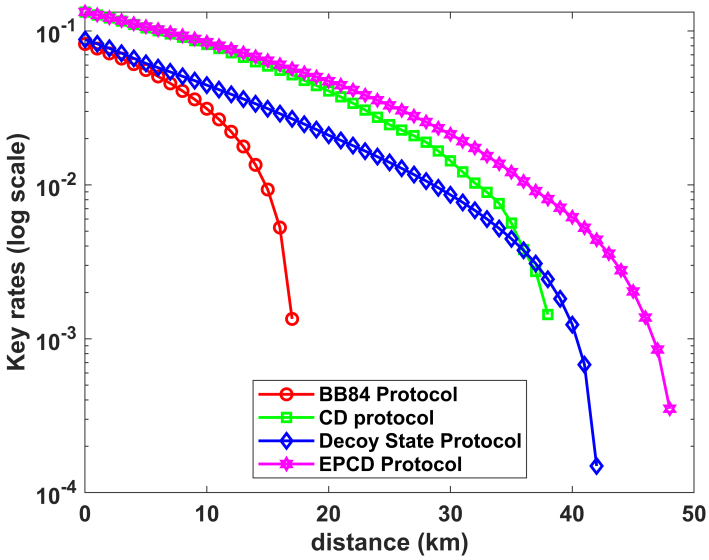


Figure 5.8: Key rates (bits per pulse) as a function of distance (in km) for four protocols: (i) BB84 Protocol, (ii) CD protocol, (iii) Decoy state protocol and (iv) EPCD protocol. The plots are in log scale

the mean photon number (μ) in Fig. 5.6. Our analysis demonstrates a significant enhancement in key rate when coincidences are considered. Specifically, the coincidence detection (CD) protocol allows for a higher optimal mean photon number ($\mu = 1.1$) compared to using the traditional decoy-state method without coincidences ($\mu = 0.8$). Furthermore, comparing the optimal key rates of the decoy state protocol and the EPCD protocol, we observe an improvement of approximately 64%.

Using the experimental setup described in the previous Section, we executed protocols systematically across various signal intensities, each corresponding to distinct mean photon numbers. The experimentally obtained gain (Q_μ) and quantum bit error rate (QBER) (E_μ) were then utilized to estimate optimal bounds on the secure key rate as discussed in Sec. 5.3. We incorporated timestamps to record both coincidences and single detections during data collection at different source intensities. This approach allowed us to investigate four variants of our quantum key distribution (QKD) protocol: Standard BB84, BB84 with decoy states, BB84 with coincidence monitoring, and BB84 with entrapped pulses and coincidence monitoring. Optimal key rates were computed for all four protocols across different mean photon number values (μ), as depicted in Fig. 5.7. Additionally, our experimental results align well with theoretical predictions regarding improvements in secure key rates. Notably, we achieved a maximum key rate of 0.17 bits per pulse using the EPCD protocol.

We have simulated the expected secure key rate for the four protocols as a function of distance over fiber with a loss of 0.2 dB/km. The simulated key rates are plotted in Fig. 5.8. In this simulation, we have considered the mean photon number of the signal and decoy to be $\mu = 0.8$ and $\nu = 0.1$, respectively. It is evident that the EPCD protocol consistently gives higher key rates than other protocols across

varying distances, showcasing its effectiveness in extending communication ranges. This consistent performance highlights the EPCD protocol's reliability and strength in addressing challenges related to communication distance.

5.6 Summary and Conclusion

In this work, we have proposed the entrapped pulse coincidence detection (EPCD) protocol, where we have integrated two approaches to harness their collective strength. Monitoring coincidences of the signal as well as entrapped pulses allows us to detect the most practical, sophisticated PNS attacks. With an assurance of no PNS attack, we showed that by including contributions from two-photon statistics, we could achieve higher key rates.

A novel method for optimizing key rates using Semi-Definite Programming (SDP) is introduced, providing tight bounds on asymptotic key rates for the protocols discussed in this chapter. In practical terms, this method yields reasonable bounds on key rates within a few minutes when executed on a personal computer. Moreover, the method is readily parallelizable, ensuring adaptability for scenarios where computed bounds may need further tightening, although we have not encountered such a situation in our experience thus far. This method has been used to compute the asymptotic key rates for the field implementation of our protocol. The obtained results illustrate that employing the proposed protocol substantially enhances the asymptotic key rates. We plan to conduct a future study on the finite-size analysis of our proposed protocol.

Chapter 6

Summary

Unlike conventional cryptography, which depends on the difficulty of breaking the code, QKD guarantees security based on the fundamental laws of physics. However, practical implementations of QKD can introduce vulnerabilities that attackers could exploit. This thesis explores some of these potential security gaps at the source and detection stages and proposes solutions to address these limitations while improving key generation rates.

The first chapter emphasizes the importance of establishing secure keys for enabling secure communication. It discusses two main branches of cryptology: cryptography, the art of securing information, and cryptanalysis, the art of breaking such codes. Further, we discussed cryptographic techniques, including symmetric and asymmetric key distribution methods, along with their limitations. It highlights the weaknesses of classical cryptography, especially its vulnerability to future advancements like powerful algorithms and quantum computers. Following the introduction of the one-time pad (OTP), the issue of security essentially boils down to a key distribution problem. It then discusses how QKD has enabled secure key exchange

by utilizing the laws of quantum mechanics to guarantee security without needing to guess an eavesdropper's limitations. However, potential vulnerabilities due to imperfect devices highlight the need for further research in this area. Finally, it presents the objective, overview and structure of the thesis.

The second chapter introduces the theoretical concepts of information theory and the practical realization of QKD protocols. Initially, it examines the key tools, such as Shannon entropy and mutual information, and establishes a relationship between the two. Then, it explores qubits, their Bloch sphere representation, manipulation techniques, and measurement methods. Moreover, we introduced the density matrix formalism and delved into von Neumann entropy. Additionally, we explored Quantum Key Distribution (QKD) algorithms, highlighting their security aspects, including error correction and privacy amplification techniques. Leveraging the polarization degree of freedom, it discusses practical implementations and establishes direct correspondences between theory and application. It then discusses the BB84 protocol using weak coherent pulses, along with the essential mathematical framework defining yield, gain, and QBER. In the following chapters, we gradually introduced additional concepts and techniques relevant to the subsequent study.

The third chapter focuses on detector coupling mismatch and explores how imperfections at the detector end can lead to information leakage. We investigate scenarios with low and high coupling mismatch, comparing them using cross-correlation and mutual information. Our work demonstrates that improved coupling significantly reduces information leakage by an order of magnitude. These leakage values quantify the mismatch between detectors. Experiments are conducted using both Gaussian and Laguerre-Gaussian beams for two types of symmetrical modes. We calculate the mutual information between an eavesdropper and the legitimate receiver due to this mismatch. By addressing the information leakage, this research

not only enhances system security but also helps determine the amount of secure key that can be extracted.

The fourth chapter discusses the implementation of QKD using a weak coherent source following Poissonian distribution. Accurate characterization of mean photon number per pulse for weak coherent sources is crucial for secure QKD to minimize information leakage from unintended multi-photon pulses. This chapter addresses the limitations of SPADs and proposes using four detectors for better resolution in low-photon scenarios employed in QKD. The chapter emphasizes the importance of proper characterization to avoid security vulnerabilities and recommends using four detectors for high mean photon number settings. The difference in the mean photon number calculated using one and four SPADs is estimated. The values increase with an increase in the mean photon number. Inaccurate mean photon number estimation can cause undetected information leaks, hence compromising security.

The fifth chapter introduces the Entrapped Pulse Coincidence Detection (EPCD) protocol, which combines two existing approaches for improved security in Quantum Key Distribution (QKD). EPCD leverages the strengths of both decoy state detection and coincidence counting to effectively address Photon Number Splitting (PNS) attacks, a sophisticated eavesdropping technique. Additionally, the chapter presents a novel method using Semi-Definite Programming (SDP) to calculate tighter bounds on achievable key rates for various QKD protocols. It provides tighter bounds on key rates compared to traditional methods and is parallelizable, allowing for further refinement of bounds if needed. Simulations further confirm the effectiveness of the EPCD protocol across different communication distances. The EPCD protocol consistently outperforms others, demonstrating its potential to extend secure communication distance.

6.1 Scope For Future Work

In this thesis, we have studied the potential information leakage to the eavesdropper due to imperfections at the source and detector end. We explored the ways for rigorous characterisation of statistics of weak coherent pulses employed as a source in QKD protocols. We discussed the vulnerabilities due to the use of these WCPs instead of single photon sources. Finally, we proposed the entrapped pulse coincidence detection (EPCD) protocol to enhance the security as well as the key rates of protocols employing WCPs.

Expanding on the foundation established in this thesis, we want to conduct a rigorous finite-key analysis to quantify the achievable secure key rate. By comparing this achievable key rate and security level with traditional QKD protocols utilizing Weak Coherent Pulses (WCPs), we can quantify the enhancements provided by EPCD in terms of security and efficiency for the practical case of finite key distribution.

In long-distance communication, loss is a critical factor affecting achievable key rates. For the EPCD protocol, the two-photon yield depends quadratically on channel transmittance, necessitating thorough protocol analysis under loss conditions in future studies. In free-space communication, atmospheric turbulence is inevitable, making it essential to investigate its impact on EPCD protocol performance. Atmospheric turbulence introduces distortions and losses in the communication channel, directly affecting achievable key rates and Quantum Bit Error Rate (QBER). Developing simulation models and conducting controlled experiments will help quantify the impact of various turbulence parameters. Comparing the EPCD protocol's performance under turbulent conditions with existing protocols will provide valuable insights into their relative resilience against real-world channel imperfections.

Studying turbulence effects on polarization, phase, and mode will be crucial, especially for satellite-to-ground QKD, where turbulence can significantly impact performance and reliability.

Finally, exploring Measurement Device-Independent Quantum Key Distribution (MDI-QKD) offers a path towards even stronger communication security. MDI-QKD protocol enables the removal of side-channel attacks at the detector's end. While MDI-QKD requires nearly perfect state preparation by Alice and Bob, this is a manageable condition since they can use attenuated laser pulses and verify their states in a secure environment. Future research can refine the protocol to address imperfections in state preparation, making MDI-QKD an even more practical and secure solution. The potential future scope includes optimizing performance and developing advanced protocols to support long-distance communication.

By pursuing these exciting avenues of future research, we can significantly contribute to developing secure and practical QKD protocols that can be implemented in real-world applications.

Appendix A

Supplementary Material for Chapter 4

A.1 Upper and lower limits of probability

The weak coherent pulses follow poisonnian photon statistics and to characterise such a source its essential to give the rigourous bounds on p_n. Such bounds were formulated in [93] and the explicit formulas for the bounds calculated with $D = 4$ are given below. Where, they defined $\tilde{c}_{\mathrm{obs},r} := c_{\mathrm{obs},r}/c_{r,r}$, which reduces to $\tilde{c}_{\mathrm{obs},r} = c_{\mathrm{obs},r}/(r!\,\eta^r)$ for the uniform cases of $\eta = \eta_1 = \eta_2 = \eta_3 = \eta_4$. They are of $O(1)$ in the limit of $\eta \to 0$. To simplify the notations, they also defined $s_j := \sum_{W \in I_j} \prod_{i \in W} \eta_i / \begin{pmatrix} D \\ j \end{pmatrix}$ $(j = 2, \ldots, D)$, and $\xi_{i,j} := s_i/\left(s_j \eta^{i-j}\right) - 1 (i, j = 2, \ldots, D)$.

The formula for the uniform case is simply given by setting $\xi_{i,j} = 0$ for all i, j.

$$\begin{aligned} p_0^L &= 1 - \tilde{c}_{\text{obs},1} + \left[1 - (1 - 3\xi_{2,1})\,\eta\right] \tilde{c}_{\text{obs},2} \\ &- \left[1 - (3 - 3\xi_{3,2})\,\eta + (2 - 12\xi_{3,2} + 6\xi_{3,1})\,\eta^2\right] \tilde{c}_{\text{obs},3} \\ &+ 4\,(1 + \xi_{4,3})\,\eta\left[1 - 6\eta + (11 + 3\xi_{3,1})\,\eta^2\right. \\ &\left. -6\,(1 + \xi_{3,1})\,\eta^3\right] \tilde{c}_{\text{obs},4}, \end{aligned} \tag{A.1}$$

$$\begin{aligned} p_0^U &= 1 - \tilde{c}_{\text{obs},1} + \left[1 - (1 - 3\xi_{2,1})\,\eta\right] \tilde{c}_{\text{obs},2} \\ &- \left[1 - (3 - 3\xi_{3,2})\,\eta + (2 - 12\xi_{3,2} + 6\xi_{3,1})\,\eta^2\right] \tilde{c}_{\text{obs, }3} \\ &+ [1 - (6 - 2\xi_{4,3})\,\eta + (11 + 6\xi_{2,1} - 8\xi_{3,2}/3 \\ &-12\xi_{4,3} + 11\xi_{4,2}/3)\,\eta^2 - (6 + 24\xi_{2,1} - 32\xi_{3,2}/3 \\ &\left. -16\xi_{4,3} + 44\xi_{4,2}/3 - 6\xi_{4,1})\,\eta^3\right] \tilde{c}_{\text{obs ,}4}, \end{aligned} \tag{A.2}$$

$$\begin{aligned} p_1^L &= \tilde{c}_{\text{obs},1} - \left[2 - (1 - 3\xi_{2,1})\,\eta\right] \tilde{c}_{\text{obs},2} \\ &+ \left[3 - (6 - 6\xi_{3,2})\,\eta + (2 - 12\xi_{3,2} + 6\xi_{3,1})\,\eta^2\right] \tilde{c}_{\text{obs ,}3} \\ &- [4 - (18 - 6\xi_{4,3})\,\eta + (22 + 12\xi_{2,1} \\ &-16\xi_{3,2}/3 - 24\xi_{4,3} + 22\xi_{4,2}/3)\,\eta^2 \\ &- (6 + 24\xi_{2,1} - 32\xi_{3,2}/3 \\ &\left. -16\xi_{4,3} + 44\xi_{4,2}/3 - 6\xi_{4,1})\,\eta^3\right] \tilde{c}_{\text{obs }4,}, \end{aligned} \tag{A.3}$$

$$\begin{aligned} p_1^U &= \tilde{c}_{\text{obs, }1} - \left[2 - (1 - 3\xi_{2,1})\,\eta\right] \tilde{c}_{\text{obs, }2} \\ &+ \left[3 - (6 - 6\xi_{3,2})\,\eta + (2 - 12\xi_{3,2} + 6\xi_{3,1})\,\eta^2\right] \tilde{c}_{\text{obs, }3} \\ &- 4\,(1 + \xi_{4,3})\,\eta\left[3 - 12\eta + (11 + 3\xi_{3,1})\,\eta^2\right] \tilde{c}_{\text{obs},4}, \end{aligned} \tag{A.4}$$

$$p_2^L = \tilde{c}_{\text{obs},2} - 3\left[1-(1-\xi_{3,2})\,\eta\right]\tilde{c}_{\text{obs},3} + 12\,(1+\xi_{4,3})\,\eta(1-2\eta)\tilde{c}_{\text{obs }4,}, \tag{A.5}$$

$$p_2^U = \tilde{c}_{\text{obs },2} - 3\left[1-(1-\xi_{3,2})\,\eta\right]\tilde{c}_{\text{obs },3} + \left[6-(18-6\xi_{4,3})\,\eta+(11+6\xi_{2,1} -8\xi_{3,2}/3-12\xi_{4,3}+11\xi_{4,2}/3)\,\eta^2\right]\tilde{c}_{\text{obs },4}, \tag{A.6}$$

$$p_3^L = \tilde{c}_{\text{obs},3} - \left[4-2\,(3-\xi_{4,3})\,\eta\right]\tilde{c}_{\text{obs},4}, \tag{A.7}$$

$$p_3^U = \tilde{c}_{\text{obs },3} - 4\,(1+\xi_{4,3})\,\eta\tilde{c}_{\text{obs },4}, \tag{A.8}$$

$$p_{\geq 4}^L = 4!\,(1+\xi_{4,1})\,\eta^4\tilde{c}_{\text{obs },4}, \tag{A.9}$$

$$p_{\geq 4}^U = \tilde{c}_{\text{obs }4.}. \tag{A.10}$$

A.2 Data Analysis of Chapter 4

Algorithm 1 Source Characterization

1: **Data Preparation and Initialisation**

- Read the data file containing 100 sets.
- Separate the columns into singles, two-fold coincidences, three-fold coincidences, and four-fold coincidences.

2: **Method 1 (4.2.2)**

- Use the equation (4.5) in Method 1 to calculate the mean photon number for each row.
- Compute the average mean photon number and variance over the 100 repetitions for each intensity level.

3: **Method 2 (4.2.3)**

- Use Method 2 to calculate the mean photon number.
- For each row, calculate the upper and lower limits on probabilities for the number of photons per pulse (see appendix A.1).
- Perform a Poissonian fit to these probabilities to determine the mean photon number.
- Compute the average mean photon number and variance over the 100 repetitions for each intensity level.

4: **Repeat for Different Intensities**

- Repeat the analysis for different intensities of the same source.
- Record the mean photon numbers for each intensity level using Method 1 and Method 2.

5: **Repeat for Different Sources**

- Repeat the analysis (Steps 1 to 4) for all four sources.
- Record the mean photon numbers for each source at each intensity level.

6: end =0

Appendix B

Supplementary Material for Chapter 5

B.1 Converting to a finite optimisation problem

As the objective function of problem (5.12) only consists of 2 terms with 4 variables, removing infinite parameters from constraints suffices. Consider the following lower bound on the constraint for Q_{ν_d} in the optimization problem:

$$\begin{aligned} Q_{\nu_d} e^{\nu_d} &= \sum_{k=0}^{n} Y_k \frac{\nu_d^k}{k!} + \sum_{k=n+1}^{\infty} Y_k \frac{\nu_d^k}{k!} \\ &\leq \sum_{k=0}^{n} Y_k \frac{\nu_d^k}{k!} + \sum_{k=n+1}^{\infty} \frac{\nu_d^k}{k!} \end{aligned} \tag{B.1}$$

where the above inequality holds because $Y_k \in [0, 1]$. Therefore, defining $\Theta_n(\nu_d)$ by the sum

$$\Theta_n(\nu_d) := \sum_{k=n+1}^{\infty} \frac{\nu_d^k}{k!} = e^{\nu_d} - \sum_{k=0}^{n} \frac{\nu_d^k}{k!} \tag{B.2}$$

allows us to obtain a relaxation corresponding to the constraint $Q_{\nu_d} e^{\nu_d} = \sum_{k=0}^{\infty} Y_k \nu_d^k / k!$ in optimization problem (5.12):

$$Q_{\nu_d} e^{\nu_d} - \Theta_n(\nu_d) \leq \sum_{k=0}^{n} Y_k \frac{\nu_d^k}{k!} \leq Q_{\nu_d} e^{\nu_d}. \tag{B.3}$$

In other words, we have formed a relaxation of the constraint given by an infinite sum of infinitely many variables through a constraint that involves a finite sum of finitely many variables. We use similar arguments to derive the following relaxations of the constraints for $E_{\nu_d} Q_{\nu_d} e^{\nu_d}$ in optimization problem (5.12):

$$E_{\nu_d} Q_{\nu_d} e^{\nu_d} - \Theta_n(\nu_d) \leq \sum_{k=0}^{n} e_k Y_k \frac{\nu_d^k}{k!} \leq E_{\nu_d} Q_{\nu_d} e^{\nu_d} \tag{B.4}$$

The above relaxations allow us to prove the following lemma:

Lemma 1. *Let us consider the optimization problem*

$$\begin{aligned}
r_n := \inf \Big(& Y_1 \mu \left(1 - \Phi\left(2e_1 - 1\right)\right) \\
& + Y_2 \frac{\mu^2}{2} \left(1 - \Phi\left((2e_2 - 1)^2\right)\right) \Big) \\
\textit{s.t. } \forall k: \quad & Y_k, e_k \in [0,1] \\
& \forall d: Q_{\nu_d} e^{\nu_d} - \Theta_n(\nu_d) \leq \sum_{k=0}^{n} Y_k \frac{\mu^k}{k!} \\
& \forall d: \sum_{k=0}^{n} Y_k \frac{\mu^k}{k!} \leq Q_{\nu_d} e^{\nu_d} \\
& \forall d: E_{\nu_d} Q_{\nu_d} e^{\nu_d} - \Theta_n(\nu_d) \leq \sum_{k=0}^{n} e_k Y_k \frac{\mu^k}{k!} \\
& \forall d: \sum_{k=0}^{n} e_k Y_k \frac{\mu^k}{k!} \leq E_{\nu_d} Q_{\nu_d} e^{\nu_d}
\end{aligned} \tag{B.5}$$

Then $r_n \leq r$. *Furthermore,*

$$\lim_{n\to\infty} |r_n - r| = 0$$

Proof. Consider the optimization problems for r_n and r. From the preceding discussion, it is evident that the constraints in problem (B.5) serve as relaxations for the constraints in problem (5.12). Consequently, the feasible set of optimization problem (5.12) is a subset of that of optimization problem (B.5). Moreover, the optimization problems designed to compute both r and r_n share identical objective functions. Thus, $r_n \leq r$ holds for all $n \in \mathbb{R}$.

Additionally, it is straightforward to recognize that when $n < m$, the constraints of the optimization problem for r_n are relaxations of those for r_m. This immediately implies that $r_n \leq r_m$. As we continue this process, the feasible set for the optimization problem for r_n approaches that of the optimization problem for r. Consequently, the non-decreasing sequence $\{r_n\}_n$ will converge to r. □

B.2 Data Analysis of Chapter 5

Algorithm 2 Computing the Key Rate

Input:

Gain and QBER for signal (Q_μ, E_μ)

Gain and QBER for decoy (Q_ν, E_ν)

Signal and decoy intensities (μ, ν)

Step 1: Define Function to Calculate Key Rate for BB84

function calculate_key_rate_BB84(Q_μ, E_μ, μ):

    Formulate the objective function (5.14)

    Define constraints based on Q_μ, E_μ, μ

    Solve the optimization problem using the SDP solver

Compute the key rate K using Eq. (5.13)
return key rate K of BB84
Step 2: Define Function to Calculate Key Rate for CD
function calculate_key_rate_CD(Q_μ, E_μ, μ):
Formulate the objective function (5.12)
Define constraints based on Q_μ, E_μ, μ
Solve the optimization problem using the SDP solver
Compute the key rate K using Eq. (5.11)
return key rate K of CD
Step 3: Define Function to Calculate Key Rate for Decoy
function calculate_key_rate_Decoy(Q_μ, E_μ, Q_ν, E_ν, μ, ν):
Formulate the objective function (5.14)
Define constraints based on Q_μ, E_μ, Q_ν, E_ν, μ, ν
Solve the optimization problem using the SDP solver
Compute the key rate K using Eq. (5.13)
return key rate K of Decoy
Step 4: Define Function to Calculate Key Rate for EPCD
function calculate_key_rate_EPCD(Q_μ, E_μ, Q_ν, E_ν, μ, ν):
Formulate the objective function (5.12)
Define constraints based on Q_μ, E_μ, Q_ν, E_ν, μ, ν
Solve the optimization problem using the SDP solver
Compute the key rate K using Eq. (5.11)
return key rate K of EPCD
Step 5: Execute and Obtain Results
Obtain key rates for each protocol:
$K_{BB84} \leftarrow$ calculate_key_rate_BB84(Q_μ, E_μ, μ)
$K_{CD} \leftarrow$ calculate_key_rate_CD(Q_μ, E_μ, μ)

37: $K_{Decoy} \leftarrow$ calculate_key_rate_Decoy(Q_μ, E_μ, Q_ν, E_ν, μ, ν)

38: $K_{EPCD} \leftarrow$ calculate_key_rate_EPCD(Q_μ, E_μ, Q_ν, E_ν, μ, ν)

39: **Output:**

40: Key rates;K_{BB84}, K_{CD}, K_{Decoy}, and K_{EPCD}

41: end =0

Bibliography

[1] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[2] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, p. 120–126, feb 1978. [Online]. Available: https://doi.org/10.1145/359340.359342

[3] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997. [Online]. Available: https://doi.org/10.1137/S0097539795293172

[4] A. Calderbank, E. Rains, P. Shor, and N. Sloane, "Quantum error correction via codes over gf(4)," *IEEE Transactions on Information Theory*, vol. 44, no. 4, pp. 1369–1387, 1998.

[5] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, 10th ed. USA: Cambridge University Press, 2011.

[6] S. Aaronson, *Quantum computing since Democritus*. Cambridge University Press, 2013.

[7] A. Kerckhoffs, "La cryptographie militaire," *Journal des Sciences Militaires*, 1883. [Online]. Available: https://www.arcsi.fr/doc/cryptomilitaire.pdf

[8] D. R. Stinson, *Cryptography: Theory and Practice*, 1st ed. USA: CRC Press, Inc., 1995.

[9] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?" *IEEE Security and Privacy*, vol. 16, no. 5, pp. 38–41, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8490169

[10] G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," *Transactions of the American Institute of Electrical Engineers*, vol. XLV, pp. 295–301, 1926.

[11] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct. 1949. [Online]. Available: https://ieeexplore.ieee.org/document/6769090

[12] E. Biham and T. Mor, "Security of quantum cryptography against collective attacks," *Phys. Rev. Lett.*, vol. 78, pp. 2256–2259, Mar 1997. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.78.2256

[13] B. A. Slutsky, R. Rao, P.-C. Sun, and Y. Fainman, "Security of quantum cryptography against individual attacks," *Phys. Rev. A*, vol. 57, pp. 2383–2398, Apr 1998. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.57.2383

[14] H.-K. Lo and H. F. Chau, "Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances," *Science*, vol. 283, no. 5410, pp. 2050–2056, mar 1999. [Online]. Available: https://www.science.org/doi/10.1126/science.283.5410.2050

[15] N. Lütkenhaus, "Estimates for practical quantum cryptography," *Phys. Rev. A*, vol. 59, pp. 3301–3319, May 1999. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.59.3301

[16] P. W. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Physical Review Letters*, vol. 85, no. 2, pp. 441–444, jul 2000. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.85.441

[17] N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," *Phys. Rev. A*, vol. 61, p. 052304, Apr 2000. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.61.052304

[18] D. Mayers, "Unconditional security in quantum cryptography," *Journal of the ACM*, vol. 48, no. 3, pp. 351–406, 2001.

[19] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," *arXiv:quant-ph/0212066*, 2002. [Online]. Available: https://arxiv.org/abs/quant-ph/0212066

[20] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, p. 7–11, Dec. 2014. [Online]. Available: http://dx.doi.org/10.1016/j.tcs.2014.05.025

[21] Ekert, "Quantum cryptography based on Bell's theorem." *Physical review letters*, vol. 67 6, pp. 661–663, 1991. [Online]. Available: https://www.semanticscholar.org/paper/f8dcc3047eef8da135bca13b926b1e6cf50e7f3a

[22] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, pp. 3121–3124, May 1992. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.68.3121

[23] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bell's theorem," *Phys. Rev. Lett.*, vol. 68, pp. 557–559, Feb 1992. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.68.557

[24] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," *Phys. Rev. Lett.*, vol. 89, p. 037902, Jun 2002. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.89.037902

[25] 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.*, vol. 92, p. 057901, Feb 2004. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.92.057901

[26] D. Stucki, C. Barreiro, S. Fasel, J.-D. Gautier, O. Gay, N. Gisin, R. Thew, Y. Thoma, P. Trinkler, F. Vannel, and H. Zbinden, "Continuous high speed coherent one-way quantum key distribution," *Opt. Express*, vol. 17, no. 16, pp. 13 326–13 334, Aug 2009. [Online]. Available: https://opg.optica.org/oe/abstract.cfm?URI=oe-17-16-13326

[27] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of cryptology*, vol. 5, no. 1, pp. 3–28, 1992.

[28] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, Mar 2002. [Online]. Available: https://link.aps.org/doi/10.1103/RevModPhys.74.145

[29] H. P. Yuen, "Security of quantum key distribution," *IEEE Access*, vol. 4, pp. 724–749, 2016.

[30] M. Sasaki, "Quantum key distribution and its applications," *IEEE Security & Privacy*, vol. 16, no. 5, pp. 42–48, 2018.

[31] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Reviews of Modern Physics*, vol. 92, no. 2, mar 2019. [Online]. Available: http://dx.doi.org/10.1103/RevModPhys.92.025002

[32] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," *Adv. Opt. Photon.*, vol. 12, no. 4, pp. 1012–1236, Dec 2020. [Online]. Available: https://opg.optica.org/aop/abstract.cfm?URI=aop-12-4-1012

[33] P.-Y. Kong, "A review of quantum key distribution protocols in the perspective of smart grid communication security," *IEEE Systems Journal*, vol. 16, no. 1, pp. 41–54, 2022.

[34] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, Oct. 1982. [Online]. Available: https://www.nature.com/articles/299802a0

[35] B. Huttner and A. K. Ekert, "Information gain in quantum eavesdropping," *Journal of Modern Optics*, vol. 41, no. 12, pp. 2455–2466, 1994.

[36] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on Practical Quantum Cryptography," *Physical Review Letters*, vol. 85, no. 6, pp. 1330–1333, aug 2000. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.85.1330

[37] A. Vakhitov, V. Makarov, and D. R. Hjelme, "Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography," *Journal of*

Modern Optics, vol. 48, no. 13, pp. 2023–2038, nov 2001. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/09500340108240904

[38] V. Makarov and D. R. Hjelme, "Faked states attack on quantum cryptosystems," *Journal of Modern Optics*, vol. 52, no. 5, pp. 691–705, mar 2005. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/09500340410001730986

[39] M. Curty and N. Lütkenhaus, "Intercept-resend attacks in the Bennett-Brassard 1984 quantum-key-distribution protocol with weak coherent pulses," *Physical Review A*, vol. 71, no. 6, p. 062301, Jun. 2005. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.71.062301

[40] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-horse attacks on quantum-key-distribution systems," *Physical Review A*, vol. 73, no. 2, p. 022320, feb 2006. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.73.022320

[41] ——, "Trojan-horse attacks on quantum-key-distribution systems," *Physical Review A*, vol. 73, no. 2, p. 022320, Feb. 2006. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.73.022320

[42] V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," *Physical Review A*, vol. 74, no. 2, p. 022313, Aug. 2006. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.74.022313

[43] V. Makarov, "Controlling passively quenched single photon detectors by bright light," *New Journal of Physics*, vol. 11, no. 6, p. 065003, Jun. 2009. [Online]. Available: https://iopscience.iop.org/article/10.1088/1367-2630/11/6/065003

[44] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature Photonics*, vol. 4, no. 10, pp. 686–689, oct 2010. [Online]. Available: http://www.nature.com/articles/nphoton.2010.214

[45] R. Aggarwal, H. Sharma, and D. Gupta, "Analysis of Various Attacks over BB84 Quantum Key Distribution Protocol," *International Journal of Computer Applications*, vol. 20, no. 8, pp. 28–31, Apr. 2011. [Online]. Available: http://www.ijcaonline.org/volume20/number8/pxc3873313.pdf

[46] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, and G. Leuchs, "Attacks on practical quantum key distribution systems (and how to prevent them)," *Contemporary Physics*, vol. 57, no. 3, pp. 366–387, Jul. 2016. [Online]. Available: http://www.tandfonline.com/doi/full/10.1080/00107514.2016.1148333

[47] Y.-J. Qian, D.-Y. He, S. Wang, W. Chen, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, "Hacking the Quantum Key Distribution System by Exploiting the Avalanche-Transition Region of Single-Photon Detectors," *Physical Review Applied*, vol. 10, no. 6, p. 064062, Dec. 2018. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevApplied.10.064062

[48] A. Huang, A. Navarrete, S.-H. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov, "Laser-seeding attack in quantum key distribution," *Phys. Rev. Appl.*, vol. 12, p. 064043, Dec 2019. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevApplied.12.064043

[49] K. Wei, W. Zhang, Y.-L. Tang, L. You, and F. Xu, "Implementation security of quantum key distribution due to polarization-dependent efficiency

mismatch," *Physical Review A*, vol. 100, no. 2, p. 022325, Aug. 2019. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.100.022325

[50] P. Chaiwongkhot, K. B. Kuntz, Y. Zhang, A. Huang, J.-P. Bourgoin, S. Sajeed, N. Lütkenhaus, T. Jennewein, and V. Makarov, "Eavesdropper's ability to attack a free-space quantum-key-distribution receiver in atmospheric turbulence," *Physical Review A*, vol. 99, no. 6, p. 062315, Jun. 2019. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.99.062315

[51] H. Inamori, N. Lütkenhaus, and D. Mayers, "Unconditional security of practical quantum key distribution," *The European Physical Journal D*, vol. 41, no. 3, pp. 599–627, jan 2007. [Online]. Available: https://doi.org/10.1140%2Fepjd%2Fe2007-00010-4

[52] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," *Phys. Rev. Lett.*, vol. 98, p. 230501, Jun 2007. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.98.230501

[53] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, p. 130503, Mar 2012. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.108.130503

[54] K. Wei, W. Li, H. Tan, Y. Li, H. Min, W.-J. Zhang, H. Li, L. You, Z. Wang, X. Jiang, T.-Y. Chen, S.-K. Liao, C.-Z. Peng, F. Xu, and J.-W. Pan, "High-speed measurement-device-independent quantum key distribution with integrated silicon photonics," *Phys. Rev. X*, vol. 10, p. 031030, Aug 2020. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevX.10.031030

[55] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.

[56] R. R. Puri, *Basic Quantum Mechanics*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 1–36. [Online]. Available: https://doi.org/10.1007/978-3-540-44953-9_1

[57] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 2nd ed. Akademiai Kiado, 1997.

[58] E. Diamanti, "Security and implementation of differential phase shift quantum key distribution systems," *Stanford University*, 01 2006.

[59] C. Bennett, G. Brassard, C. Crepeau, and U. Maurer, "Generalized privacy amplification," *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1915–1923, 1995.

[60] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, pp. 1098–1105, Aug 1996. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.54.1098

[61] A. M. Steane, "Simple quantum error-correcting codes," *Phys. Rev. A*, vol. 54, pp. 4741–4751, Dec 1996. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.54.4741

[62] E. Biham, B. Huttner, and T. Mor, "Quantum cryptographic network based on quantum memories," *Phys. Rev. A*, vol. 54, pp. 2651–2658, Oct 1996. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.54.2651

[63] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," *Mathematical, Physical and Engineering Sciences*, vol. 461, pp. 207–235, Jan 2005. [Online]. Available: https://doi.org/10.1098/rspa.2004.1372

[64] K. M., "Simple security proof of quantum key distribution based on complementarity," *New Journal of Physics*, vol. 11, p. 045018, 2009. [Online]. Available: https://dx.doi.org/10.1088/1367-2630/11/4/045018

[65] B.-O. M., M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, "Simple security proof for quantum key distribution," *Proceedings of the Second International Conference on Theory of Cryptography*, 2005. [Online]. Available: https://www.slmath.org/workshops/204/schedules/1258.Ben-Or

[66] R. Renner and R. König, "Universally composable privacy amplification against quantum adversaries," in *Proceedings of the Second International Conference on Theory of Cryptography*, ser. TCC'05. Berlin, Heidelberg: Springer-Verlag, 2005, p. 407–425. [Online]. Available: https://doi.org/10.1007/978-3-540-30576-7_22

[67] R. RENNER, "Security of quantum key distribution," *International Journal of Quantum Information*, vol. 06, no. 01, pp. 1–127, 2008. [Online]. Available: https://doi.org/10.1142/S0219749908003256

[68] V. Scarani and R. Renner, "Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing," *Phys. Rev. Lett.*, vol. 100, p. 200501, May 2008. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.100.200501

[69] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," *Nature Communications*, vol. 3, no. 1, p. 634, Jan. 2012. [Online]. Available: https://doi.org/10.1038/ncomms1631

[70] W. Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication," *Physical Review Letters*, vol. 91, no. 5,

p. 057901, aug 2003. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.91.057901

[71] H.-K. Lo, X. Ma, and K. Chen, "Decoy State Quantum Key Distribution," *Physical Review Letters*, vol. 94, no. 23, p. 230504, jun 2005. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.94.230504

[72] X.-B. Wang, "Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography," *Physical Review Letters*, vol. 94, no. 23, p. 230503, jun 2005. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.94.230503

[73] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Physical Review A*, vol. 72, no. 1, p. 012326, jul 2005. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.72.012326

[74] S. Wiesner, "Conjugate coding," *ACM SIGACT News*, vol. 15, no. 1, pp. 78–88, Jan. 1983. [Online]. Available: https://dl.acm.org/doi/10.1145/1008908.1008920

[75] S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier, and H. Weinfurter, "Information leakage via side channels in freespace bb84 quantum cryptography," *New Journal of Physics*, vol. 11, no. 6, p. 065001, jun 2009. [Online]. Available: https://dx.doi.org/10.1088/1367-2630/11/6/065001

[76] 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*, vol. 57, no. 6, pp. 1–7, 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9531968

[77] K. Wei, W. Zhang, Y.-L. Tang, L. You, and F. Xu, "Implementation security of quantum key distribution due to polarization-dependent efficiency

mismatch," *Phys. Rev. A*, vol. 100, p. 022325, Aug 2019. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.100.022325

[78] M. Rau, T. Vogl, G. Corrielli, G. Vest, L. Fuchs, S. Nauerth, and H. Weinfurter, "Spatial mode side channels in free-space qkd implementations," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 187–191, 2015. [Online]. Available: https://ieeexplore.ieee.org/document/6963270

[79] S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, "Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch," *Phys. Rev. A*, vol. 91, p. 062301, Jun 2015. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.91.062301

[80] T. Sharma, A. Biswas, P. Chandravanshi, S. Prabhakar, and R. P. Singh, "Vulnerability in free space qkd due to detection coupling mismatch," *IEEE Journal of Quantum Electronics*, vol. 59, no. 6, pp. 1–7, 2023.

[81] A. E. Willner, H. Huang, Y. Yan, Y. Ren, N. Ahmed, G. Xie, C. Bao, L. Li, Y. Cao, Z. Zhao, J. Wang, M. P. J. Lavery, M. Tur, S. Ramachandran, A. F. Molisch, N. Ashrafi, and S. Ashrafi, "Optical communications using orbital angular momentum beams," *Adv. Opt. Photon.*, vol. 7, no. 1, pp. 66–106, Mar 2015. [Online]. Available: https://opg.optica.org/aop/abstract.cfm?URI=aop-7-1-66

[82] V. P. Lukin, P. A. Konyaev, and V. A. Sennikov, "Beam spreading of vortex beams propagating in turbulent atmosphere," *Appl. Opt.*, vol. 51, no. 10, pp. C84–C87, Apr 2012. [Online]. Available: https://opg.optica.org/ao/abstract.cfm?URI=ao-51-10-C84

[83] V. Makarov, "Controlling passively quenched single photon detectors by bright light," *New Journal of Physics*, vol. 11, no. 6, p. 065003, jun 2009. [Online]. Available: https://doi.org/10.1088/1367-2630/11/6/065003

[84] V. Makarov and D. R. Hjelme, "Faked states attack on quantum cryptosystems," *Journal of Modern Optics*, vol. 52, no. 5, pp. 691–705, 2005. [Online]. Available: https://doi.org/10.1080/09500340410001730986

[85] V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," *Phys. Rev. A*, vol. 74, p. 022313, Aug 2006. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.74.022313

[86] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," *Phys. Rev. A*, vol. 78, p. 042333, Oct 2008. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.78.042333

[87] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, "Device Calibration Impacts Security of Quantum Key Distribution," *Physical Review Letters*, vol. 107, no. 11, p. 110501, sep 2011. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.107.110501

[88] S. Cova, A. Longoni, and A. Andreoni, "Towards picosecond resolution with single-photon avalanche diodes," *Review of Scientific Instruments*, vol. 52, no. 3, pp. 408–412, mar 1981. [Online]. Available: https://pubs.aip.org/rsi/article/52/3/408/310043/Towards-picosecond-resolution-with-single-photon

[89] R. Cheng, Y. Zhou, S. Wang, M. Shen, T. Taher, and H. X. Tang, "A 100-pixel photon-number-resolving detector unveiling photon statistics," *Nature Photonics*, vol. 17, no. 1, pp. 112–119, jan 2023. [Online]. Available: https://www.nature.com/articles/s41566-022-01119-3

[90] J. Sperling, W. Vogel, and G. S. Agarwal, "True photocounting statistics of multiple on-off detectors," *Phys. Rev. A*, vol. 85, p. 023820, Feb 2012. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.85.023820

[91] ——, "Correlation measurements with on-off detectors," *Phys. Rev. A*, vol. 88, p. 043821, Oct 2013. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.88.043821

[92] J. F. Dynes, M. Lucamarini, K. A. Patel, A. W. Sharpe, M. B. Ward, Z. L. Yuan, and A. J. Shields, "Testing the photon-number statistics of a quantum key distribution light source," *Optics Express*, vol. 26, no. 18, p. 22733, sep 2018. [Online]. Available: https://opg.optica.org/abstract.cfm?URI=oe-26-18-22733

[93] M. Kumazawa, T. Sasaki, and M. Koashi, "Rigorous characterization method for photon-number statistics," *Opt. Express*, vol. 27, no. 4, pp. 5297–5313, Feb 2019. [Online]. Available: https://opg.optica.org/oe/abstract.cfm?URI=oe-27-4-5297

[94] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, "Loss-tolerant quantum cryptography with imperfect sources," *Physical Review A*, vol. 90, p. 052314, 11 2014. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.90.052314

[95] A. Mizutani, M. Curty, C. C. W. Lim, N. Imoto, and K. Tamaki, "Finite-key security analysis of quantum key distribution with imperfect light sources,"

New Journal of Physics, vol. 17, p. 093011, 9 2015. [Online]. Available: https://iopscience.iop.org/article/10.1088/1367-2630/17/9/093011

[96] K. Tamaki, M. Curty, and M. Lucamarini, "Decoy-state quantum key distribution with a leaky source," *New Journal of Physics*, vol. 18, no. 6, p. 065008, jun 2016. [Online]. Available: https://dx.doi.org/10.1088/1367-2630/18/6/065008

[97] Y. Nagamatsu, A. Mizutani, R. Ikuta, T. Yamamoto, N. Imoto, and K. Tamaki, "Security of quantum key distribution with light sources that are not independently and identically distributed," *Physical Review A*, vol. 93, p. 042325, 4 2016. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.93.042325

[98] Y. Wang, W.-S. Bao, C. Zhou, M.-S. Jiang, and H.-W. Li, "Tight finite-key analysis of a practical decoy-state quantum key distribution with unstable sources," *Physical Review A*, vol. 94, p. 032335, 9 2016. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.94.032335

[99] W. Wang, K. Tamaki, and M. Curty, "Finite-key security analysis for quantum key distribution with leaky sources," *New Journal of Physics*, vol. 20, p. 083027, 8 2018. [Online]. Available: https://iopscience.iop.org/article/10.1088/1367-2630/aad839

[100] M. Pereira, M. Curty, and K. Tamaki, "Quantum key distribution with flawed and leaky sources," *npj Quantum Information*, vol. 5, p. 62, 7 2019. [Online]. Available: https://www.nature.com/articles/s41534-019-0180-9

[101] T. Sharma, "Thesis- chapter 4 data," 2024. [Online]. Available: https://doi.org/10.5281/zenodo.14033507

[102] A. S. StÉPhane Félix, Nicolas Gisin and H. Zbinden, "Faint laser quantum key distribution: Eavesdropping exploiting multiphoton pulses," *Journal of Modern Optics*, vol. 48, no. 13, pp. 2009–2021, 2001. [Online]. Available: https://doi.org/10.1080/09500340108240903

[103] A. Biswas, A. Banerji, N. Lal, P. Chandravanshi, R. Kumar, and R. P. Singh, "Quantum key distribution with multiphoton pulses: an advantage," *Optics Continuum*, vol. 1, no. 1, p. 68, Jan. 2022. [Online]. Available: https://opg.optica.org/abstract.cfm?URI=optcon-1-1-68

[104] K. Lim, H. Ko, C. Suh, and J.-K. K. Rhee, "Security analysis of quantum key distribution on passive optical networks," *Opt. Express*, vol. 25, no. 10, pp. 11 894–11 909, May 2017. [Online]. Available: https://opg.optica.org/oe/abstract.cfm?URI=oe-25-10-11894

[105] N. Lütkenhaus and M. Jahma, "Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack," *New Journal of Physics*, vol. 4, no. 1, p. 44, jul 2002. [Online]. Available: https://dx.doi.org/10.1088/1367-2630/4/1/344

[106] S. Nahar, T. Upadhyaya, and N. Lütkenhaus, "Imperfect phase-randomisation and generalised decoy-state quantum key distribution," *arXiv preprint arXiv:2304.09401*, 2023.

[107] X. Sixto, V. Zapatero, and M. Curty, "Security of decoy-state quantum key distribution with correlated intensity fluctuations," *Physical Review Applied*, vol. 18, no. 4, p. 044069, 2022.

[108] V. Zapatero, Á. Navarrete, K. Tamaki, and M. Curty, "Security of quantum key distribution with intensity correlations," *Quantum*, vol. 5, p. 602, 2021.

[109] M. Araújo, M. Huber, M. Navascués, M. Pivoluska, and A. Tavakoli, "Quantum key distribution rates from semidefinite programming," *Quantum*, vol. 7, p. 1019, 2023.

[110] D. Bunandar, L. C. Govia, H. Krovi, and D. Englund, "Numerical finite-key analysis of quantum key distribution," *npj Quantum Information*, vol. 6, no. 1, p. 104, 2020.

[111] P. J. Coles, E. M. Metodiev, and N. Lütkenhaus, "Numerical approach for unstructured quantum key distribution," *Nature communications*, vol. 7, no. 1, p. 11712, 2016.

[112] I. George, J. Lin, and N. Lütkenhaus, "Numerical calculations of the finite key rate for general quantum key distribution protocols," *Physical Review Research*, vol. 3, no. 1, p. 013274, 2021.

[113] M. Dušek, M. Jahma, and N. Lütkenhaus, "Unambiguous state discrimination in quantum cryptography with weak coherent states," *Phys. Rev. A*, vol. 62, p. 022306, Jul 2000. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.62.022306

[114] R. Bhavsar, S. Ragy, and R. Colbeck, "Improved device-independent randomness expansion rates using two sided randomness," *New Journal of Physics*, 2023.

[115] R. Bhavsar, "Improvements on device independent and semi-device independent protocols of randomness expansion," *arXiv preprint arXiv:2311.13528*, 2023.

[116] P. Wittek, "Algorithm 950: Ncpol2sdpa—sparse semidefinite programming relaxations for polynomial optimization problems of noncommuting vari-

ables," *ACM Transactions on Mathematical Software (TOMS)*, vol. 41, no. 3, pp. 1–12, 2015.

[117] T. Sharma, R. Bhavsar, J. Ramakrishnan, P. Chandravanshi, S. Prabhakar, A. Biswas, and R. P. Singh, "Enhancing key rates of qkd protocol by coincidence detection," 2024.

[118] T. Metger, O. Fawzi, D. Sutter, and R. Renner, "Generalised entropy accumulation," in *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE, 2022, pp. 844–850.

[119] T. Metger and R. Renner, "Security of quantum key distribution from generalised entropy accumulation," *Nature Communications*, vol. 14, no. 1, p. 5272, 2023.

[120] T. Sharma, A. Biswas, J. Ramakrishnan, P. Chandravanshi, and R. P. Singh, "Mitigating the source-side channel vulnerability by characterisation of photon statistics," *Journal of Lightwave Technology*, pp. 1–7, 2024.

List of Publications

Thesis Related Publications

1. **Sharma, T.**, Biswas, A., Ramakrishnan, J., Chandravanshi, P., Singh, R.P., 2024. Mitigating the Source-side Channel Vulnerability by Characterisation of Photon Statistics. J. Lightwave Technol. 1–7. https://doi.org/10.1109/JLT.2024.3361079

2. **Sharma, T.**, Biswas, A., Chandravanshi, P., Prabhakar, S., Singh, R.P., 2023. Vulnerability in Free Space QKD Due to Detection Coupling Mismatch. IEEE J. Quantum Electron. 59, 1–7. https://doi.org/10.1109/JQE.2023.3318585

3. **Sharma, T.**, Bhavsar, R., Ramakrishnan, J., Chandravanshi, P., Prabhakar, S., Biswas, A., Singh, R.P., 2024. "Enhancing key rates of QKD protocol by Coincidence Detection." arXiv. http://arxiv.org/abs/2402.19049

Other Publications

4. **Sharma, T.**, Biswas, A., Chandravanshi, P., Prabhakar, S., Singh, R.P., 2022.

Information Leakage due to Detection Coupling Mismatch, in: Quantum 2.0 Conference and Exhibition. Presented at the Quantum 2.0, Optica Publishing Group, Boston, MA, p. QW2A.2.
https://doi.org/10.1364/QUANTUM.2022.QW2A.2

5. Rani, A., Ramakrishnan, J., **Sharma, T.**, Chandravanshi, P., Biswas, A., Singh, R.P., 2023b. Experimental Shot Noise Measurement Using the Imperfect Detection—A Special Case for Pulsed Laser. IEEE J. Quantum Electron. 59, 1–8.
https://doi.org/10.1109/JQE.2023.3308263

6. Mishra, S., Biswas, A., Patil, S., Chandravanshi, P., Mongia, V., **Sharma, T.**, Rani, A., Prabhakar, S., Ramachandran, S., Singh, R.P., 2022a. BBM92 quantum key distribution over a free space dusty channel of 200 meters. J. Opt. 24, 074002.
https://doi.org/10.1088/2040-8986/ac6f0b

7. Rani, A., Chandravanshi, P., Ramakrishnan, J., Vaity, P., Madhusudhan, P., **Sharma, T.**, Bhardwaj, P., Biswas, A., Singh, R.P., 2023a. Free space continuous variable Quantum Key Distribution with discrete phases. Physics Open 17, 100162.
https://doi.org/10.1016/j.physo.2023.100162

Conference Paper

8. Sharma, T., Biswas, A., Chandravanshi, P., Prabhakar, S., Singh, R.P., 2022. Information Leakage due to Detection Coupling Mismatch, in: Quantum 2.0 Conference and Exhibition.
https://doi.org/10.1364/QUANTUM.2022.QW2A.2