# Free Space Quantum Key Distribution: Experiments for Improving Security and Key Rate

A thesis submitted in partial fulfilment of

the requirements for the degree of

**Doctor of Philosophy**

*by*

**Ayan Biswas**

(Roll No. 16330008)

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

2021

**To**

***My Family and Friends***

# Declaration

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

Signature

Name: Ayan Biswas

(Roll No: 16330008)

Date:

# CERTIFICATE

It is certified that the work contained in the thesis titled **"Free Space Quantum Key Distribution: Experiments for Improving Security and Key Rate"** by Mr. Ayan Biswas (Roll No. 16330008), has been carried out under my supervision and that this work has not been submitted elsewhere for a degree.

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

(Thesis Supervisor)

Date:

# Acknowledgments

*My journey of Ph.D. at Physical Research Laboratory (PRL), Ahmedabad has now come to an end. Thanking is the most difficult task and writing this particular section of my thesis gives me immense pleasure. Though we know that it will never be enough to thank anyone in most of the cases, yet I would like to express my gratitude to the people who gave their support, and have directly or indirectly motivated me throughout.*

*First and foremost, I would like to express my deepest gratitude to my supervisor, Prof. R. P. Singh, for providing continuous support during my Ph.D. He gave me freedom to advance my curiosity towards newer fields of research and encouraged me to learn new things. He helped me choose a new research area for myself and has taught me not be hesitant to try something new at any point of life. Though there were many tough times, but he always believed in me and all his students. His positive attitude towards solving any scientific problems encourages me to probe deeper into the subject. He was always available for discussions and guidance, be it academic or personal. His valuable suggestions and critical comments have helped me to improve at all aspects of my life. His constant guidance, inspiration, encouragement, and motivation during this entire period helped me at the time of research and writing of this thesis.*

*Further, I express my sincere gratitude towards my Doctoral Scientific Committee (DSC) members, Dr. Goutham Kumar Samanta, Dr. Rajesh Kumar Kushawaha, and Dr. Sashikiran Ganesh. They have always guided me during my thesis progress and provided constructive remarks to my research work, which helped me grow academically. I am grateful to them for asking me the difficult questions during the seminars, which eventually helped me to understand my work better. I will always remain grateful to Dr. G. Samanta for giving me opportunities in being a part of the extra-curricular science outreach activities that he organized in and around PRL. I enjoyed accompanying him at all the forums and share my knowledge with young minds. I am thankful to all three of them for providing me with an unending support and their friendly behaviour, which always kept me motivated for my thesis work.*

*I am also thankful to all the Academic Committee members for their insightful comments and encouragement during my research period. I express my sincere gratitude to all the faculty members of PRL who had taught me during the course work and inspired me to pursue research. They provided an overall view of research works carried out in PRL, which helped*

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

*The inspiration, support, and cooperation that I have received from my group members are beyond the scope of any acknowledgement. They were always present for moral support and helped in creating a fun-loving working atmosphere. I would still like to express my sincere gratitude to all my group members for helping me during my Ph.D. journey. I would like to thank Pooja and J.K who have closely worked with me and helped me in troubleshooting the challenges in experiments. I would like to thank Ali, Jabir, Nijil, Anindya, Varun, Satyajeet, Sarika, Anju, Tanya, Vardaan, Subith, Anirban, Vimlesh, Sandeep, Soumya, Shashi and Satyaranjan for all the constructive discussions. Their continuous support and care in both personal and professional fronts throughout my Ph.D. journey helped me sail through it smoothly. I thank my collaborator Dr. Rupesh for the discussions and the times he took out for me. I thank visitors in our group Pranav, Aanal for their help.*

*Doing a Ph.D. is not just about getting a degree, but it is to learn to believe in oneself and never lose hope, which in itself is an extremely challenging work. It is this time when the help and support of friends relieve the stress and makes the journey memorable. At first I would like to thank Disha for being one of the closest friends to me in PRL. She is one such person who inspires me in totality and is capable of giving wonderful suggestions in no time. I would like to thank Nidhi (thriller movie watching partner) and Arun for their unwavering support and love throughout my journey. It was and always will be a great fun to hang out with you both and pull each other's legs. I would also like to thank Priyank, Abdur, Sandeep, Prabir, Harish, Avik, Sushree, Deepika, Nisha and Surendra for the stress-relieving and funny moments that we shared together. Their instant help and positive support at all times kept me going. I also want to give a special mention to Dr. Arvind Singh and Pallavi mam for always inviting me at their place where I could have yummy food. I will cherish all the parties you hosted*

*throughout my life. I would also like to thank all the fellow researchers from PRL for being cool and friendly. Especially, I would like to mention Kaustav, Subir, Archita, Aarthy, Ankit, Abhay, Shivani, Wafikul, Rahul, Kuldeep, Siddhi, Masoom, Vishwesh, Hrushikesh, Rituparna and Madhusudhan. Kindly forgive if I have left out anyone's name and please know that I am thankful to all of you.*

*I would also like to thank my best buddy Ananya that I always look up to during tough times. I really enjoyed our time in Guwahati when we had late night discussions about superhero movies. I would like to mention my college buddies - Joy, Devaparna, Jasim and Abu who have kept me motivated always. Abhijit, Sourav, Kislay, Saikat, Hiranmoy, Abhishek and Soumadeep - my close friends from school who have always stood with me in every situation of my life.*

*Words would fail in expressing the love, strength, and encouragement of my parents, Shri. Apendra Nath Biswas and Smt. Rupali Biswas, for their support throughout my life and especially during the course of my research. They always believed in me, encouraged me to pursue my dreams, and have provided me with all kinds of support whenever I needed it. I would also like to thank my grandparents, for loving me at all the times. My thesis will be incomplete if I don't express my love and thanks to all my family members and friends for the love and support they have always given to me. Without their support, it would not be easy for me to reach this point in my life. A special thanks goes to Shefali who is not only my wife but also my best friend. She helped me a lot whenever I got stuck in coding as she's a pro. She always supported me in my tough times and helped me to handle them with calm. In the end and above all, I would like to thank God.*

**Ayan Biswas**

# Abstract

Security of Classical Key Distribution can be open to threats after the development of quantum computers. Shor's quantum algorithms can easily break the prime factorization and discreet log problem, which are crucial for providing security to classical cryptography. To provide unconditional security to the keys, Quantum Key Distribution (QKD) comes to the rescue. QKD is one of the most important applications of quantum mechanics in modern times. Photons are the most viable quantum system for QKD since they can be transported through free-space as well as through optical fiber. However, due to inherent loss in the fiber, it cannot be used for long distance QKD. Therefore, free-space quantum communication assumes importance as it is a precursor for satellite-based quantum communication needed for secure key distribution over longer distances. Though QKD provides unconditional security, practical implementation deviates from the ideal one, affecting the secure key rate. We have developed techniques to improve the key rates for BB84 and BBM92 QKD protocols and methods to characterize implementation loopholes. These loopholes creates vulnerabilities in proving the absolute security to the QKD protocol. Although QKD provides information theoretic security but, due to unavailability of ideal sources and detectors, adversary can take the advantage and guess the key that is being shared between communicating parties. This can be a major setback in implementing QKD systems in real scenarios. Even though there are true single photon sources but their efficiency is very less that reduces the key rate. Therefore, one uses weak coherent laser pulses as a source for prepare and measure protocols which can increase the key rate, however, can compromise the security. Therefore, it is necessary to characterize the source to quantify the amount of information leakage due to the side channel. We have discussed how one can characterize the QKD source for side-channel leakage as

a function of different source parameters. Also, we have quantified this information leakage in terms of cross-correlation between two signals. It is also seen that for some parameters this leakage is considerable, while it is negligible for others. Possible ways out to reduce the side channel have also been proposed. This can come in handy while making it ready for field deployment. For increasing the key rate using weak coherent laser pulses, the decoy state method is used, which adds complexity to the BB84 protocol. We introduce a novel quantum key distribution protocol, coincidence detection quantum key distribution protocol (Coincidence Detection (CD QKD). We show that in this protocol, the Poissonian nature of weak coherent pulses instead of posing a security risk can be used to achieve a secure key rate over a longer distance compared to standard GLLP (Gottesman, Hoi-Kwong Lo, Lutkenhaus and Preskill)method for quantum key distribution. This protocol will also be able to track the presence of Eve (Eavesdropper) from the multi-photon (mainly consisting of two and three photons) weak coherent laser pulses. Looking at the current trend for satellite-based optical communication, using satellite as a trusted device as in prepare and measure QKD protocols is fraught with danger. Therefore, entanglement-based protocols are preferred since, along with overcoming the distance limitation, one can take the satellite as an untrusted device. The most widely used EB QKD is the E91 protocol, but the key rate is less as a large fraction of the bits are sacrificed for Bell parameter (S) checking. This key rate can be increased by using the BBM92 protocol with a pre-characterized relation between S and QBER. This method efficiently increases the key rate without affecting the security of EB QKD.

**Keywords:** Quantum Cryptography, Quantum Communication, Quantum Key Distribution, Information Leakage, Cross-correlation, BB84 Protocol, BBM92 Protocol, Orbital Angular Momentum, Entanglement.

# Abbreviations

| | |
|---|---|
| **BS** | Beam Splitter |
| **EB QKD** | Entanglement Based Quantum Key Distribution |
| **EPS** | Entangled Photon Source |
| **EC** | Error Correction |
| **FC** | Fiber Coupler |
| **FPGA** | Field Programmable Gate Array |
| **HWP** | Half Wave Plate |
| **MI** | Mutual Information |
| **PA** | Privacy Amplification |
| **PBS** | Polarizing Beam Splitter |
| **PE** | Parameter Estimation |
| **P&M QKD** | Prepare & Measure Quantum Key Distribution |
| **QKD** | Quantum Key Distribution |
| **QBER** | Quantum Bit Error Rate |
| **QWP** | Quarter Wave Plate |
| **RNG** | Random Number Generator |
| **SPDC** | Spontaneous Parametric Down Conversion |
| **SPCM** | Single Photon Counting Module |
| **SPS** | Single Photon Source |
| **SLM** | Spatial Light Modulator |
| **WCP** | Weak Coherent Pulse |

# Contents

# List of Figures

# List of Tables

# Chapter 1

# Introduction

## 1.1 Classical Cryptography

Cryptography is a field of research that was born out of necessity for secure communication between trusted parties. It aims to ensure that communication remains confidential and inaccessible to a third party. Before $18^{th}$ century cryptography was only used in war times or at the times related to country's diplomatic talk with other countries. After the invention of the "Internet" the need for secure communication becomes more demanding year by year [1]. With more advancement in the telecommunication, the need for confidentiality becomes more important. In past three decades with the incoming of the internet banking and transaction of money through online (over the internet), this field gains the major spotlight. Now, the secure communication not only becomes the matter for diplomatic relations between nations but, also for common people communicating with each other. Internet has become a essential thing in this modern world where almost everyone is virtually connected. Without proper secrecy of messages going over the internet, communication is hard to imagine [1, 2].

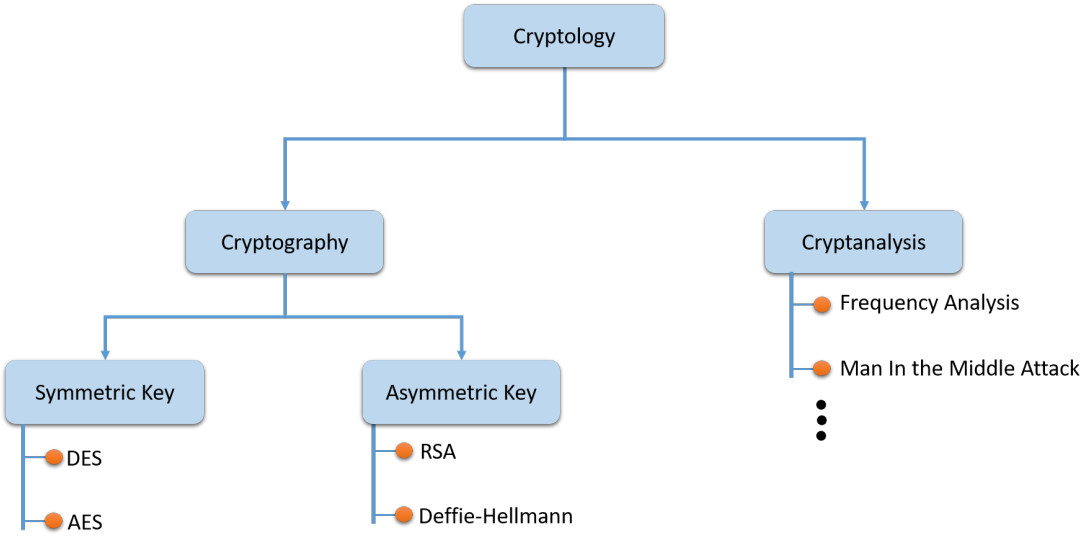



**Figure 1.1:** Various classes under Cryptology.

The art of encrypting (encoding a plain text message into code so that only the receiving party will know) becomes crucial for the modern day cryptographers. Cryptography is a subset of a much broader category know as cryptology [3–5]. Cryptology is the general technique used in both making and breaking the key. On the basis of its action on the key, cryptology is mainly divided into two major parts, cryptography and cryptanalysis, as shown in the Figure 1.1. The technique of writing the important message which is hidden in plain sight, in the form of symbols is called cryptography. It uses algorithm to encrypt a message with the help of a key, such that anyone other than the person of interest who has that key cannot be able to decode it. On the other hand, cryptanalysis deals with the technique of breaking the secure key within specified time (i.e Polynomial time ($P$)). This method uses the weakness in the encryption to break it without knowing the actual key. Because cryptanalysis is the only way to assure that a cryptosystem is secure, it is an integral part of cryptology. Cryptography and cryptanalysis complement each other to make a better crypto-system. Though there have been several attempt to break public crypto-systems they are still far from efficient in current times. Breaking crypto-systems in Polynomial time ($P$) is still a topic of cur-

rent study and many advancements have been done in these areas [4]. On the basis of algorithms and key sharing, cryptography is broadly divided into two categories; Symmetric cryptography and Asymmetric cryptography.

Conventionally the sender and receiver are called “Alice” and “Bob”. The adversary who intervenes the communication is “Eve” (there are many names in literature associated to this eg. “Oscar” but, these are famous among conventional cryptographers). For the rest of this thesis I will mainly stick to these names. The main problem starts when their is untrusted third party (Eve) intervening between Alice and Bob. The aim of Eve is to know everything about the information exchange happening between Alice and Bob without getting noticed. Eve can intercept in various ways eg. hacking the WiFi communication or listening to radio signals etc. There may be situations when Alice & Bob want to make their communication completely private from the rest of the world. For instance if Alice and Bob represent two officers of a phone manufacturer, and they are transmitting documents containing the business strategy for launching new phones in upcoming years; these documents should not get into the hands of their competitors or other agencies. For this Alice and Bob must communicate secretly between themselves and symmetric key cryptography serves as a strong tool for this.

### 1.1.1 Symmetric Key Cryptography

In symmetric key cryptography Alice and Bob use same key for encryption and decryption of the message whose schematics is given in Figure 1.2. Alice encrypts her message ‘$x$’ with help of secret key $K$ using a symmetric algorithm (either by Data Encryption Standard (DES), Advanced Encryption Standard (AES), simple substitution cipher or simple XOR operation between $x$ & $K$) yielding the cipher text ‘$y$’. Bob re-

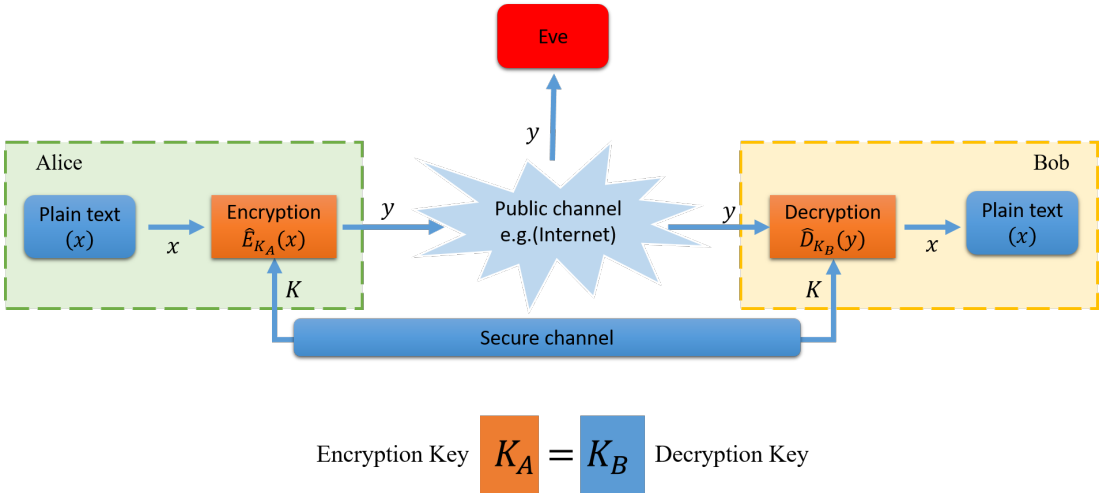



**Figure 1.2:** Cryptography with symmetric algorithm. Alice and Bob share same key between them to decrypt the cipher text.

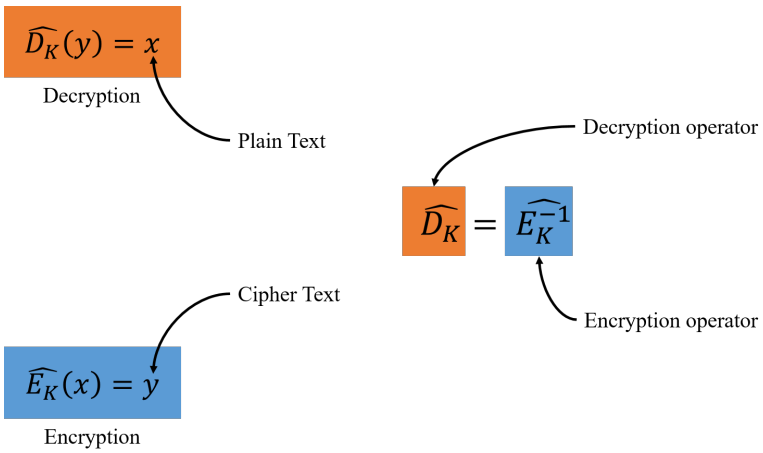



**Figure 1.3:** Diagram of symmetric encryption and decryption method.

ceives the cipher text and decrypts it [6]. Decryption is thus the inverse of encryption in these types of algorithms. After encryption the cipher text looks as a random set of letters which confuses Eve about the actual message $x$. This way message can be securely communicated between Alice and Bob. Figure 1.3 gives a basic mathematical illustration about symmetric encryption and decryption mechanism.

For this secret sharing between Alice & Bob to happen, the key must be delivered to the communicating parties via secure channel, for example a trusted human

transporting booklet of keys to Alice and Bob. An example of this in real scenario is pre-shared keys used in WiFi Protected Access (WPA), encryptions in wireless LANs. Generally, the encrypting and decrypting algorithm is known to public [3]. This does not make it easy for the eavesdropper to decrypt only using the cipher text. The key is still unknown to Eve and decrypting without it is still a hard problem in terms of computation. Public announcement of the algorithm in other way makes it easier for Bob to decipher it quickly to increases the communication rate. The basic symmetric key algorithm using XOR operation is given by

$$y = K_A \oplus x \tag{1.1}$$

now, this cipher text is sent to Bob and he decrypts as

$$K_B \oplus y = \tilde{x} \tag{1.2}$$

For $x$ and $\tilde{x}$ to be equal requries that $K_A = K_B = K$. It is evident from Eq.(1.1) and Eq.(1.2). The one way nature of the XOR operation is evident from Eqs.(1.1) and (1.2). Without knowing $K$, it is extremely difficult to know about the message $x$ [3, 4, 7]. In practical scenario the algorithm used in symmetric cryptography is Data Encryption Standard (DES). DES uses blocks (groups of bits operated together on the key, unlike individual bitwise operation) for encryption with an iterative algorithm. The basic idea which makes this encryption strong according to Claude Shannon [7] is

- **Confusion**

  A clever way to hide the relationship between key and the message (plain text). The most common example is simple substitution (eg. $A \rightarrow X, B \rightarrow Y$) of letters in message with some other. Advanced version of this technique is used in DES,

AES, Enigma machine etc.

- **Diffusion**

  The result of encryption operation of a plain text is spread over many cipher text symbols to avoid any kind of frequency based attacks. These attacks takes the advantage of the words (or data patterns) that are repetitive in the message, even though they are encrypted but, are easily recognisable as the pattern of cipher text are repetitive. Therefore, by guessing the words that are mostly used in a particular language one can decrypt the cipher text. A simple example is


**Figure 1.4:** Diffusion process in block cipher.

  bit permutation which is used in DES [6] and illustrated in Figure 1.4 with two plain texts only differing by one bit. it is clear that no statistical correlation can be found between two cipher texts.

DES uses series of confusion and diffusion operations for encryption of message with keys, decryption is just the reverse process. It uses the principle of *Feistel network*, details of which can be found in [5, 6]. A brief description of DES is given in Figure 1.5. Now a days more layers have been added and slight modification of this scheme is used in present day cryptography [4, 6, 8]. These algorithms are very strong against any attacks (hacks) even in recent times.

It is crucial to note that Eve must not get hold of the key, once she gets, it is easier for her to decipher. So, the key transmission should be done very securely between the two parties. This becomes the main bottle neck of this process. Also, this process is very cumbersome to implement. The complexity of process increases with increase

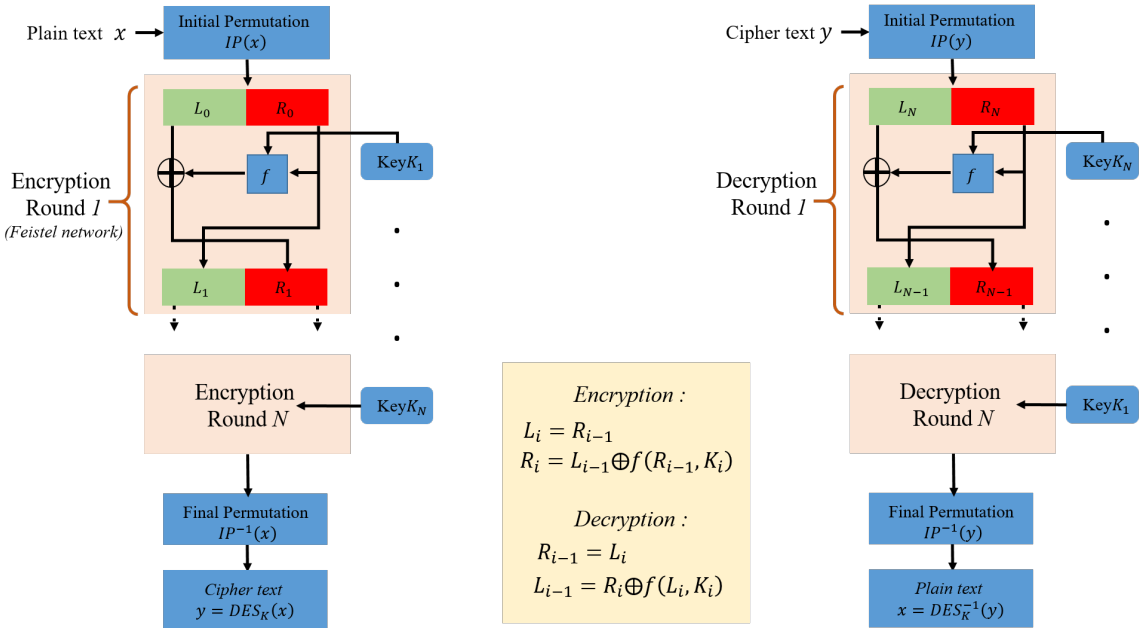



**Figure 1.5:** DES Schematics using Feistel networks

in the number of users. The major problem in this scheme is the key distribution. That has partly been taken care of by implying asymmetric cryptographic technique, it also solves the problem of increasing complexity with number of users taking part in communication.

### 1.1.2 Asymmetric Key Cryptography

It was first introduced by W. Deffie, Martin Hellman and Ralph Merkle [9]. In practice, the modern banking, online transactions etc. include this type of cryptographic technique. Here Alice encrypts the message $x$ with a public key and Bob decrypts it with his private key. A schematic of the process is given in Figure 1.6. The encryption and decryption are done with different keys in asymmetric cryptography. The advantage of this method is that secure communication is possible between large number of users without much complexity. Also, unlike symmetric key for which both the keys must be equal for faithful communication, here the two keys can be different which

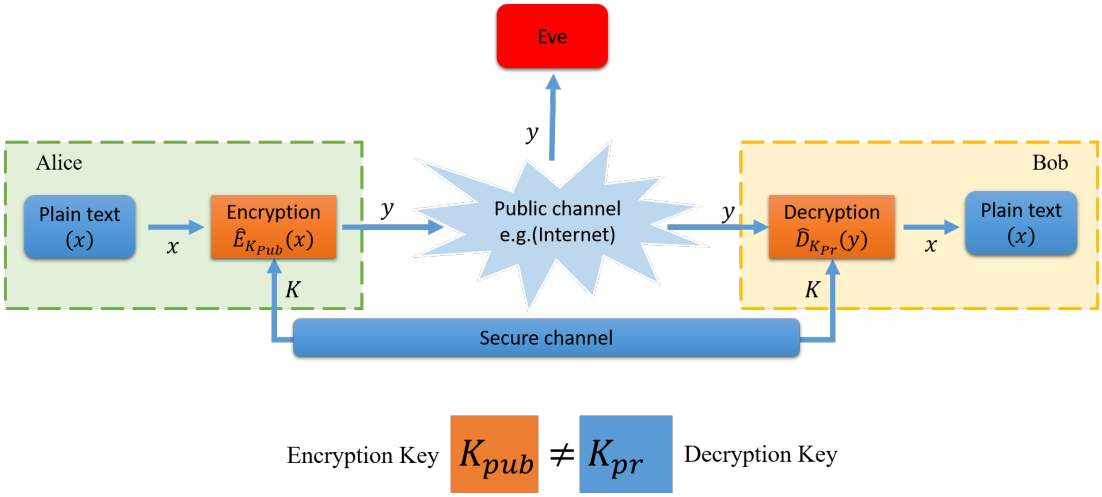



**Figure 1.6:** Symmetric Encryption and Decryption method. Alice uses her public key to encrypt and Bob used his private key to decrypt.

also makes it partially immune to key distribution problem. The encryption is done in such a way that deciphering the message without knowing the key falls under hard problem in terms of computational complexity [1, 5].

One such method for doing asymmetric key cryptography is by RSA algorithm. Rivest, Shamir and Adlemen were the first to come up with this idea in 1979 [10]. The basic steps involved in RSA algorithm are as follows:
The process in basically divided into two parts, first generating keys, second encrypting and decrypting.

- The initial key generation procedure begins with selecting two large digit prime numbers $p$ & $q$ and multiply them to get $n$, this becomes one of the elements of the key.

- For generating public key, a number $e$ is chosen such that

$$e = \begin{cases} 1 < e < \phi(n) \mid \phi(n) = (1-p)(1-q) \\ \text{numbers coprime with } n \ \& \ \phi(n) \end{cases} \tag{1.3}$$

  where $\phi(n)$ is the number of elements that are co-prime (no common factor with $n$) with $n$. The above equation means that $e$ is a number co-prime with $n$ and $\phi(n)$. This process generates public key and is $K_{pub} = (e,n)$.

- Private key is generated from public key and one of the variable $d$ is so chosen that

$$de \pmod{\phi(n)} = 1 \tag{1.4}$$

  where, mod $\phi(n)$ means that the result of the multiplication is divided by $\phi(n)$ and the remainder is taken.

- The method of encryption from public key is written as

$$E_{k_{pub}} = C = x^e \ (mod\ n) \tag{1.5}$$

  where $C$ is the cipher text after the encryption of the message $x$ with public key $e,n$.

- Decrypting $C$ through private key $(d,n)$ is then

$$x = C^d \ (mod\ n) \tag{1.6}$$

The above process describes briefly the RSA algorithm. From Eq.(1.6) and Eq.(1.5) it is clear [1, 4] that knowing only public keys $(e,n)$ doesn't makes easier to decipher. Finding $d$ form $K_{pub}$ means finding the prime factors of $n$ which is unique for a number.

This becomes computationally hard as the digits of $n$ becomes large. This means one can tighten the security of this algorithm by increasing the number of digits (bits) in the key as it increases the complexity.

## 1.2 Key Distribution Problem

One crucial thing that the two types of cryptography need, is the transmission of the "secret key" by a secure channel. One of the way to solve this key distribution problem is through Deffie-Hellmann key exchange which is given in Figure 1.7. From

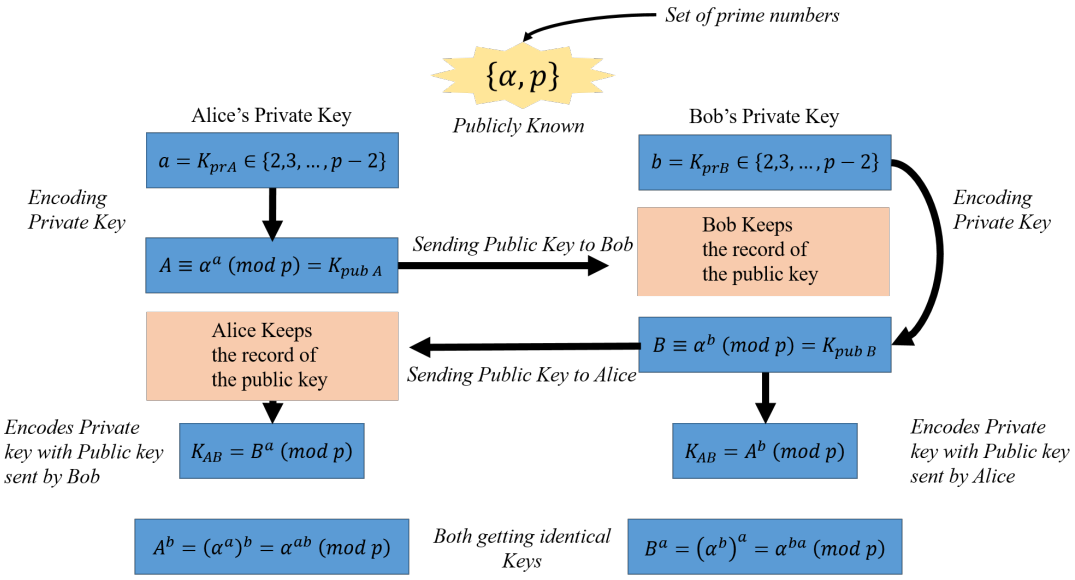



**Figure 1.7:** Flow diagram of Diffie–Hellman key exchange.

the description it is clear that how communicating parties can exchange secret key between them through the channel.

In all the above discussion it is quite clear that the role of security in the key transmission is crucial and important. We see that the security of the crypto-systems is embeded inside the hardness of the problem to solve the algorithm for breaking the encryption. It is difficult to detect an adversary intercepting the communication in real

time in classical cryptography. In classical cryptography the security is mainly related to the computational complexity of the encryption and decryption process. Computational complexity means that given present computing power to Eve, how much time (in terms of number of steps performed in programming) will she take to decipher the message. The complexity increases as one increases the number of bits in the encryption key. This assumption breaks down after the invention of quantum computer and quantum computing algorithms [1, 11, 12]. These problems are solvable in polynomial time using quantum computer. These algorithms work perfectly against discreet log problem (DLP) and prime factorization problem as shown by Peter Shor [13]. Currently, Shor's quantum algorithm for prime factorization has been tested experimentally by factoring the number 21 ($21 = 7 \times 3$) [14, 15]. Therefore, after the invention of quantum computer Eve could efficiently break the RSA algorithm [1, 13, 16]. The whole backbone of the security of classical cryptography is based on present computational hardness (such has factorization and discreet log problem) [13]. Even if quantum computer is not put into place, the security of cryptography stands upon the pillar about $P$ Vs $NP$ conjecture. Though other problems that are still proven to be secure against quantum algorithm exist, it is just a matter of time before one discovers an algorithm to break them [1, 16]. If in future somebody proves $P = NP$ then even with classical computers, all $NP$ hard problems could be broken in principle as they can be solved in polynomial time.

### 1.2.1 Introduction of Quantum Cryptography

The problem of securely exchanging the keys between the communicating parties still remains hanging. With the increase in work on quantum computing and quantum information there comes quantum safe cryptography which provides a secure way of transferring keys between the parties. Quantum cryptography provides information

theoretic [3, 4, 7] security, which means it is secure even against quantum algorithm. Even though without quantum cryptography one can make algorithm which are secure against quantum attacks such as Shor's algorithm. This approach is post quantum cryptography, and is compatible with the current crypto infrastructure. Google has showed demonstration of these types of algorithms [16, 17]. The major drawback of this is they are only secure against presently known quantum attacks. As a result these algorithms may not provide future proof security against all possible attacks. To counter all these problems the concept of quantum key distribution has been implemented. Quantum Key Distribution (QKD) is a part of quantum cryptography which uses quantum mechanics to distribute keys between two or more parties. The first approach is put forward by BB84 protocol, using the concept of conjugate coding and quantum money [18, 19].

One more important aspect that draws attention towards QKD is the fact that one can get unlimited supply of secure key from single pre shared secret. In classical cryptography once the secure key is distributed between communicating parties, which has finite size, it is difficult to amplify. After each turn of passing message both have to discard used keys to remain invulnerable. Time will come when both run out of secret keys. Quantum mechanically this key amplification process can be achieved easily that gives unlimited secret keys. This phenomenon of quantum key growing [20] makes QKD important not only for research purpose but also for other real life applications such as in banking or military.

## 1.3 Quantum Cryptography

Quantum Key Distribution or QKD uses quantum bits (qubits) unlike classical bits ($\{0,1\}$) used in conventional key distribution. They are quantum states having some

basic properties as follows [11]:

- **Quantum State**

  Any degrees of freedom of light can be used to encode or represent bits like polarization, orbital angular momentum (OAM), time, frequency of photons etc. The qubit in horizontal polarization is represented as $|H\rangle$ while in vertical polarization $|V\rangle$. One can have superposition of $H$ & $V$ polarization which is represented as $c_1|H\rangle + c_2|V\rangle$ where, $c_1$ and $c_2$ are the probability amplitudes (can be complex numbers) of $H$ and $V$ states.

- **Projective Measurement**

  Measuring qubits will project them in the eigenbasis of the measurement operators. The below example makes the statement clear. Measuring in $\{H,V\}$ basis means the projectors are $\mathbb{P}_H = |H\rangle\langle H|$ & $\mathbb{P}_V = |V\rangle\langle V|$, indicates projection of states on corresponding polarization. Let the initial state of the system be $|\psi\rangle_{in} = |H\rangle$ then measurement result leads to

$$|\psi\rangle_f = \frac{\mathbb{P}|\psi\rangle_{in}}{{}_{in}\langle\psi|\mathbb{P}|\psi\rangle_{in}}, \tag{1.7}$$

  $|\psi\rangle_f$, final sate after measurement. The subscript in $\mathbb{P}$ can either be $H$ or $V$ based on the projection used in the measurement which will tell the fate of $|\psi\rangle_f$. Here, $|\psi\rangle_f$ in $\mathbb{P}_H$ will be $|H\rangle$ and in $\mathbb{P}_V$ will be 0. If initial state is in superposition $|\psi\rangle_{in} = c_1|H\rangle + c_2|V\rangle$ then, in $\mathbb{P}_H$, final sate $|\psi\rangle_f = c_1|H\rangle/\sqrt{c_1^2+c_2^2}$ with probability $|c_1/\sqrt{c_1^2+c_2^2}|^2$ and if $\mathbb{P}_V$ then $|\psi\rangle_f = c_2|V\rangle/\sqrt{c_1^2+c_2^2}$ with probability $|c_2/\sqrt{c_1^2+c_2^2}|^2$. This basically indicates that measurement of state in wrong basis will give random results [11, 18].

- **Quantum Entanglement**

  The property of a composite quantum system in which one of the subsystems ($A$) is dependent on the other ($B$). Property of one subsystem can be known by measuring the other. For composite system $AB$ (made by subsystems $A$ and $B$) it can be written as

$$\begin{aligned} |\psi\rangle_{AB} &\neq |\psi\rangle_A \otimes |\phi\rangle_B \\ |\psi\rangle_{AB} &= c_1|\psi\rangle_A \otimes |\phi\rangle_B + c_2|\phi\rangle_A \otimes |\psi\rangle_B \end{aligned} \tag{1.8}$$

  Physically, Eq.(1.8) can be interpreted as the probability of occurrence of one state collapses the other.

These properties form the backbone of quantum computing and quantum information [21, 22]. There is more maths to this but one needs these basic properties to understand working of the QKD.

### 1.3.1 Quantum Key Distribution

The main goal of QKD is to achieve information theoretic security for the communicating parties. It uses quantum mechanics to distribute the keys between Alice (sender) and Bob (receiver) secretly over insecure quantum channel (free space or optical fiber). Only the distribution process is quantum, rest all the process is classical. This brings out an ease of realising it in practice as it can be done using existing resources. QKD not only provides a way of secure communication but also hopes to detect the eavesdropper in real time. Therefore QKD can serve as an integral part of secure communication in modern age.

**Prepare & Measure Protocol (BB84 Protocol)**

The first QKD protocol was proposed by Bennett and Brassard in a conference held at IISc Bangalore [23], where they explained their protocol for distributing keys securely from any interception by eavesdropper (Eve). The protocol is briefly as follows.

- Alice randomly chooses a basis ($\{H,V\}$ or $(0,90)$, $\{D,A\}$ or $(-45,45)$) which form a set of MUBs (Mutually Unbiased Bases) for sending polarization states of photon to Bob.
- After choosing the basis she prepares the states in random polarization and represent them as $H \to 0, V \to 1, D \to 0, A \to 1$.
- Alice sends photons through quantum channel (trace preserving channel of the quantum states) to Bob for detection.
- Bob randomly chooses his measurement basis and records the result.
- After this measurement process, both Alice & Bob discuss over the public channel about their basis choice (not the measurement results).
- Alice and Bob only keep those results in which their basis are compatible. This process is called sifting. Both of them can form the key after that.
- They take out a small part of the key and announce the result publicly to check the errors. If it is below threshold they call the protocol successful and use the rest of key for communication.

The wrong basis choice of Bob will give random result as explained in Eq.(1.7) but, the correct choice will give right result. These points also being explained through an illustration in Figure 1.8. This protocol was first experimentally demonstrated in 1992

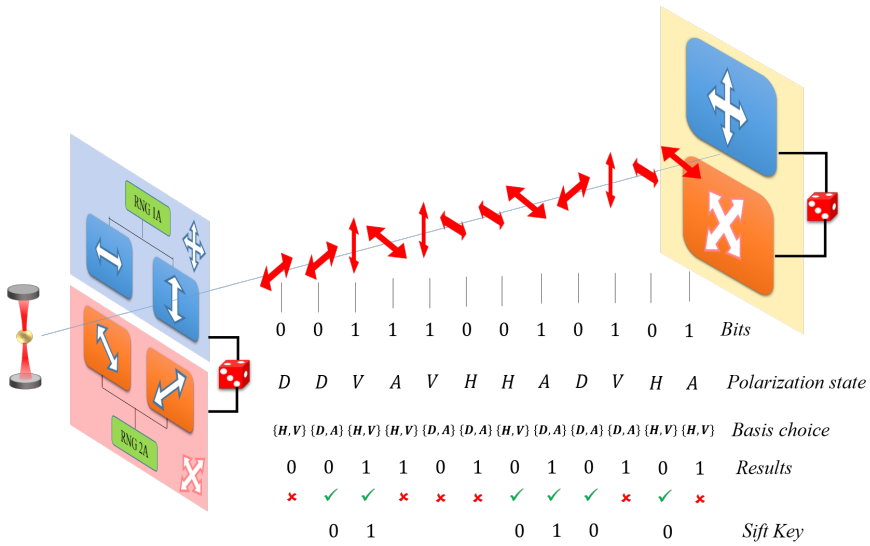


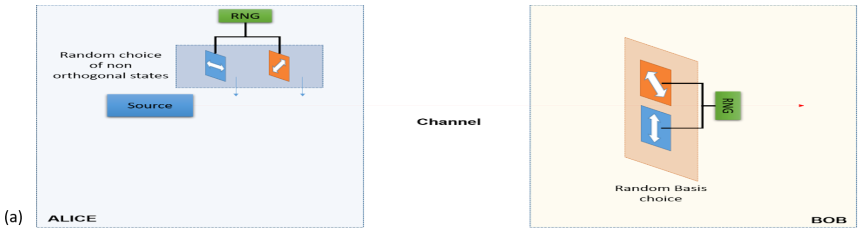

**Figure 1.8:** Schematics of BB84 protocol.

[24]. In practical scenario two more steps are required after sifting for getting secret keys. First, correcting the errors in the rest of the keys to make it identical and second keeping the keys secret from the third party (eavesdropper) while correcting the keys, this process includes hashing to shrink the keys. These process are error correction (information reconciliation) (EC) and privacy amplification (PA). Importance of them is in proving the security which is discussed in chapter 2. A few years after BB84, a similar protocol B92 was proposed, which tells about how one can do QKD with just two non orthogonal states [25]. The schematics of which is given in Figure 1.9. BB84 is much of a prepare & measure type protocol. It creates states at the senders' end (Alice) which is transferred to Bob for measurements.

### Entanglement Based QKD

Another type of protocol which uses the principle of quantum entanglement for key distribution was proposed by Arthur Ekert in 1991 and known as E91 protocol [26]. The protocol is briefly described below.

- A common sender 'Charlie' prepares $|\psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ and sends them to




(b)

| ALICE | | | BOB | | | |
|---|---|---|---|---|---|---|
| Bits | State | Basis | Basis | State | Result | Bits |
| 0 | H | {H,V} | {H,V} | H (can come either from "H" or "D") | Inconclusive | - |
| 1 | D | {D,A} | {H,V} | V (can come only from "D") | Conclusive | 1 |
| 1 | D | {D,A} | {D,A} | D | Inconclusive | - |
| 0 | H | {H,V} | {D,A} | A (can come only from "A") | Conclusive | 0 |
| 0 | H | {H,V} | {D,A} | A | Conclusive | 0 |

KEY

**Figure 1.9:** Schematics of B92 protocol. (a) Alice randomly prepares photons in either of the two non orthogonal states and sends them to Bob which he randomly measures in two basis. (b) Shows the table for key generation procedure in B92 protocol.

Alice and Bob through quantum channel (fiber or free space).

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

This protocol is secure against any eavesdropping strategy, as the security is based on the monogamy of entanglement. If maximal entangled state is used for key distribution then the Bell parameter below $2\sqrt{2}$ (for ideal channel) will be considered as insecure

for this protocol for a given channel [26–30]. For real situations both $S$ and QBER are measured, if $S$ is less than $2\sqrt{2}$ and there is QBER in the generated keys, then one goes for EC and PA to distill secret keys [31–33]. The drawback of this protocol is that it has low key rate as maximum of the generated raw bits from the measurements are used for security check through Bell violation. This is also clear in the Figure 1.10. Another similar type of protocol used for EB QKD is BBM92 protocol [34]. It avoids

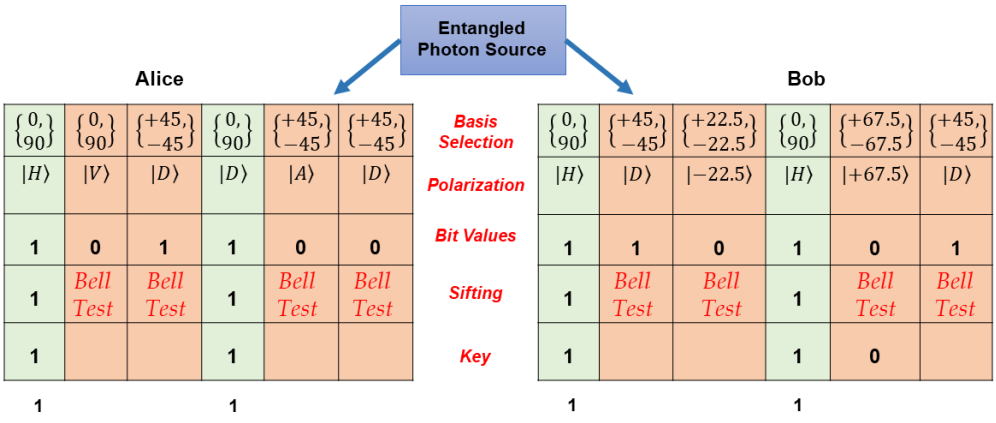



**Figure 1.10:** Schematics of Ekert (E91) Protocol

measuring the Bell's inequality violation. Only the compatible basis on Alice's and Bob's side will form the key. This increases the key rate but makes it less secure.

All the above quantum cryptographic techniques to distribute the keys quantum mechanically seem to be safe and help in eliminating the key distribution problem. Ideally all of the above QKD techniques provide unconditional security (information theoretically) but, implementation of them in practice deviates from this.

The main challenge is to build a QKD system with minimalisitc complicated devices

with maximum security. Presently there are many implementations of the protocols [16, 17, 35, 36] but, either their key generation rate is low or security is low. There is a soft trade-off between key generation rate and security of the protocol.

Some of the recent developments in the field of quantum key distribution are happening on two grounds, security of the protocol and experimental implementation. In theoretical work, the main idea is to go more towards proving the security of existing protocols [17, 37, 38], creating new QKD protocols with their security proof, also methods for increasing the key rate. Though the QKD was first proposed in 1984 but its security proof came much later. The first security proof based on uncertainty principle was given by Mayers [39, 39]. Mayers' proof was modified into much simpler one by Lo and Chau (1999) [40] using entanglement distillation protocol (EDP). This idea was improvised from the work on quantum privacy amplification [31] and ED [32]. The proof of Lo Chau is based on the existence of a quantum computer. This complication was later eased by Shor and Preskill [41] based on quantum error correcting codes (CSS codes) [12]. They proved the security for Prepare & Measure type protocols from entanglement based protocol in Lo Chau [42, 43]. Later on security definition was put forward with much more mathematical rigor [44, 45] and detailed analysis. Now, people are developing security proofs for finite key size limits [37, 46], which was not considered in earlier proofs. Device imperfections are also very important in modelling QKD protocols in practice. This modifies the key rate equations as security of the protocol now depends on various parameters. The first proof taking into account for device imperfections was by Mayers [47], that was generalised in Gottesman [48]. Various protocols have been developed other than BB84 such as COW, DPSK and SARG [49–51] and with different degrees of freedom of light (photons) [52, 53]. To eliminate the source imperfection and increase the key rate with same security decoy state protocol is implemented [54–56]. It allows to do QKD with weak coherent

laser pulses (WCP). Measurement Device Independent (MDI) QKD removes the fear of side channel attack at the detection end [57].

The first experimental implementation of QKD was done in 1992 with a channel distance of 32.5 cm [24]. Much later than that several experiments have been performed [16, 58]. The recent landmark in the free space quantum key distribution is secure communication between ground to satellite done by China [59]. Previously, free space QKD has been done between 200 km in La Palma island [60] and also from aircraft to ground QKD link has been established [35]. In fiber (ultra low loss) recently the distance achieved in QKD is of 500 km [61]. Experiments to demonstrate high key rate has also been performed [57] as this is an important parameter for communication. The key rate for fiber channel has been increased from 1MBps [62] to 10 MBps [63]. Work on techniques to improve key rates with current resources is also going on. Other than research labs, companies like ID Quantiqe, Qasky, Toshiba Europe etc. been involved in making QKD systems for governments and corporates [17].

QKD ensures to secure two or more communicating parties against malicious activities such as hacking. Even though the field is mature but still more improvements are required on implementing it in real scenario. Reaching to the point of ideal information theoretic security is a big task. Attacks such as detector blinding [64] can hack the QKD system with current devices. Countermeasure for such attacks without changing the setup's hardware are still unknown. Increasing the key rate with current resources is still a formidable challenge. To make any QKD protocol faster and secure with minimum resources is the main goal.

## 1.4 Objective of the Thesis

Quantum Key Distribution (QKD) is becoming essential means for secure communication in modern day. It can be done using the present day setup used for communication and quantum optical experiments. While other developments in the field of Quantum Technologies demands more resources for operation. Being less resource intensive QKD promises to integrate with current communication setup within coming years. After the successful demonstration of satellite to ground quantum communication by China, other nations are targeting to launch their own satellite for quantum key distribution [51, 59].

Free space QKD is essential not only for satellite communication, but also for terrestrial communication, where fiber cables are hard to reach. Though free space communication seems feasible but implementing it has several challenges. One has to keep the security of QKD system as close to ideal as possible. High security with high key rate is the modern day challenge of QKD. In free space photon loss due to beam divergence is the main issue. Therefore, decoy state QKD protocol comes into picture to increase the key rate. For implementing decoy state one needs extra post processing time information about decoy states. This slows down the process. Moving to Device Independent (DI) QKD also becomes difficult as the key rate is very less. Through EB QKD one can achieve DI QKD but rate will be low as entangled photon pairs generated will be less on first place.

Here, we discuss how one can increase the key rate just by using Weak Coherent Pulse (WCP). This method requires no extra hardware or post-processing information of extra pulses. Noting down the coincidences between the detectors gives us hints about the channel and presence of eavesdropper. If the coincidences fall below some

threshold one can declare the channel to unsafe for further communication.

One of the protocols used for DI QKD is E91 protocol but the key rate is very low. A short method that we have explored is to find out how to increase key rate of EB QKD using existing hardware. The main idea of our work is to find out techniques in free space QKD to increase key rate and security of the protocols without installing complicated hardware.

### 1.4.1 Overview of the Thesis

Quantum Key Distribution (QKD) is the secure way to communicate between sender (Alice) and receiver (Bob) by exchanging the secure key. In my thesis, I have implemented QKD protocols to understand the practical challenges involved in experimental demonstration of the same. The objectives of my thesis are enumerated below.

- To design and study the key generation rate of Discrete Variable Quantum Key Distribution protocols (BB84 and BBM92).
- To characterize the BB84 QKD source to constrain Eve's information by quantifying side-channel leakage.
- To develop a technique to increase the key rate of BB84 protocol with coherent weak pulses (WCP) using coincidence detection method.
- To find the relation between CHSH Bell parameter $S$ and QBER for entanglement based QKD to improve the key rate.

# Chapter 2

# Theoretical Background for Secure Key rate of QKD Protocols

One of the most important sub class of quantum cryptography (QC) is Quantum Key Distribution (QKD). Just like classical key distribution QKD also ensures in distributing the keys between two or more communicating parties. The distribution method of QKD uses the principles of quantum mechanics. Unlike its classical counterpart the security of distributing the keys is unconditional. The use of QKD requires a predefined authenticated classical channel [16, 20]. The main benefit of using QKD is that it can provide information theoretic security [47, 65], unlike its classical counterpart that is based on computational hardness. It is known from information theoretic security point of view that key should be random and must be used only once [7, 66, 67]. Therefore, at a point two parties will run out of stored secret key. To grow the key again with the remaining pre shared secret key, QKD provides the most secured solution and this process is called quantum key growing [20, 65, 68]. However, this security is based on assumed ideal conditions that is not the case in practice. Therefore, security

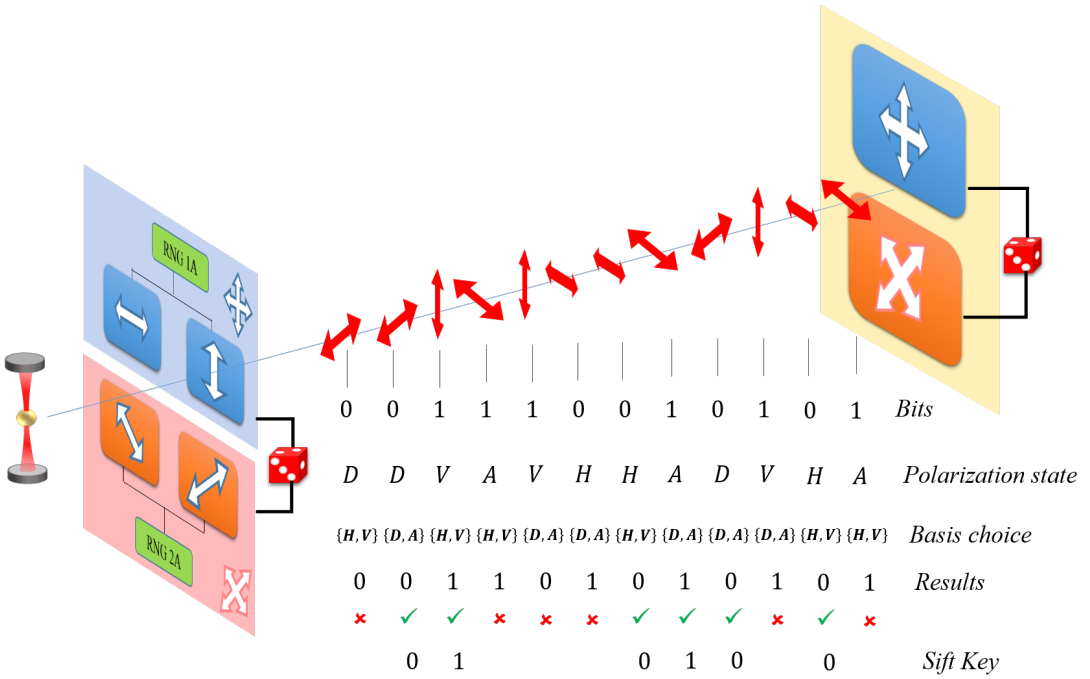



**Figure 2.1:** BB84 protocol.

analysis for a practical implementation becomes very important. In this chapter, we will be discussing security of mainly two protocols BB84 and BBM92 given in Figure 2.1 and 2.2, which we have already discussed briefly in the previous chapter.

## 2.1 Basic Security

The process of QKD does not end after sifting, one need to check weather Alice and Bob receive the identical keys or not. To ensure keys with Alice and Bob are secret and identical requires doing error correction and privacy amplification. The identical keys must be secure in order to use them for further communication. The protocol for consideration here is mainly BB84 and BBM92. The basic principles which guide the idea of security in any QKD (Prepare and measure (P&M) or Entanglement Based (EB)) protocol are as follows.

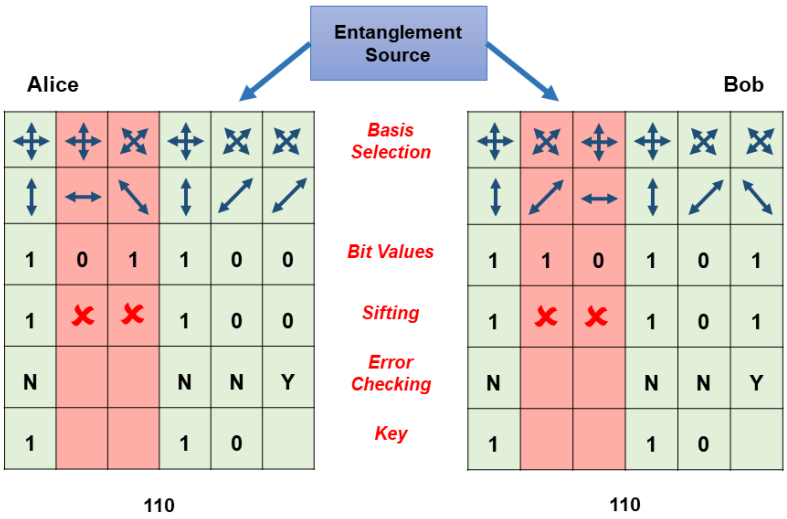



**Figure 2.2:** BBM92 protocol.

- **No Cloning Theorem**

  A universal machine cannot be created to copy an arbitrary quantum state. The laws of quantum mechanics do not allow to copy an unknown quantum state [69]. This makes QKD protocols immune to counterfeiting and eavesdropping while exchanging information. Alice and Bob can easily send and share secrets with each other without worrying about the copying of their qubit state. The short proof of this theorem is as follows.

  We have a quantum state $|\psi\rangle$ that needs to be copied by copying machine $\mathbb{U}$ on the blank state $|b\rangle$. The operation can be given as

$$\mathbb{U}(|\psi\rangle \otimes |b\rangle) = |\psi\rangle \otimes |\psi\rangle. \tag{2.1}$$

  Similarly, for $|\phi\rangle$

$$\mathbb{U}(|\phi\rangle \otimes |b\rangle) = |\phi\rangle \otimes |\phi\rangle. \tag{2.2}$$

Now, let us take a general state $|x\rangle = (\alpha|\psi\rangle + \beta|\phi\rangle)$ (say), for copying this state using same unitary operation gives

$$\begin{aligned}\mathbb{U}(|x\rangle \otimes |b\rangle) &= |x\rangle \otimes |x\rangle \\ &= (|\alpha|^2|\psi\rangle \otimes |\psi\rangle + \alpha\beta|\psi\rangle \otimes |\phi\rangle + \beta\alpha|\phi\rangle \otimes |\psi\rangle + |\beta|^2|\phi\rangle \otimes |\phi\rangle),\end{aligned} \tag{2.3}$$

from which two points can be drawn . One, the states that we wanted to copy is $|x\rangle$ for which the result of Eq.(2.3) should be $(|\alpha|^2|\psi\rangle \otimes |\psi\rangle + |\beta|^2|\phi\rangle \otimes |\phi\rangle)$ instead we are getting the cross terms, which is not the output we wanted. This indicates that there is no universal copying machine that can copy all kinds of states at once, as it contradicts the unitarity of quantum mechanics. Two, for preserving the unitary operations in Eq.(2.1) and (2.2) it demands that $\langle\phi|\psi\rangle = |\langle\phi|\psi\rangle|^2$ which can be possible if and only if, both the states are orthogonal or parallel. Therefore, it is impossible to copy any arbitrary state without prior knowledge.

- **Uncertainty Principle**

  Two variables that are canonically conjugate [18, 70]) cannot be simultaneously measured with arbitrary accuracy. The variables can be position and momentum $(\hat{X}, \hat{P})$, rectilinear polarization and diagonal polarization $(\sigma_Z, \sigma_X)$ or angle and orbital angular momentum of photons $(\theta, l)$. The relation is given by

$$\Delta\sigma_X \Delta\sigma_Z \geq \frac{\hbar}{2} \tag{2.4}$$

  where, $\Delta\sigma_X$ is uncertainty in $X$ (diagonal) polarization and $\Delta\sigma_Z$ is uncertainty in $Z$ (rectilinear) polarization.

  This property has advantage in providing security to any QKD protocol as result

of the measurement in one basis, randomises the result in the conjugate basis [11, 18, 23]. For example suppose we have a state $|H\rangle$, measuring it in $\{H,V\}$ $(Z)$ basis, will have a deterministic result but, if $\{D,A\}$ $(X)$ basis is used then the result will be random. Linear polarization $|H\rangle = \frac{1}{\sqrt{2}}(|D\rangle + |A\rangle)$, can have both $D\&A$ in equal superposition, which results in equal probability of $D$ and $A$ after measurement. So, the result in $\{D,A\}$ basis becomes random and impossible to guess weather it comes from $H$ or $V$. This is an important principle which ensures eavesdropping is impossible without creating any disturbance.

- **Entanglement Monogamy**

  In quantum physics, if the two particles or systems are entangled with each other then, there is no way a third party can be correlated with any one of them. This is explained in Figure 2.3.

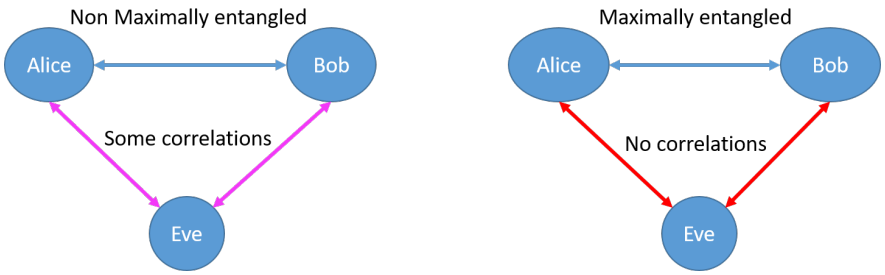



**Figure 2.3:** Schematics for Entanglement Monogamy.

It basically says that quantum entanglement cannot be shared by arbitrarily many systems [71]. This provides advantage in security of QKD protocols (especially EB QKD) which says that eavesdropper cannot have information about the key. If Alice and Bob share a maximally entangled pair between them, which eventually will form the final key, then Eve will have no correlations with any one of them. This eventually leads to perfectly secret key shared between Alice and Bob.

## 2.2 Basic Security of BB84 Protocol

There are various aspects involved in proving security of BB84 protocol [16, 18, 24]. The first exhaustive security proof was presented by Mayers [39, 72] but was difficult to grasp. Then Lo and Chau [40] proved the protocol's security by the process called entanglement distillation protocol (EDP) [31]. It basically gives the threshold error (bit error and phase error) for the secure key that can be generated during the protocol. The security proof presented by Lo and Chau [40] uses quantum error correction for rectifying the qubits distributed by Eve. Their method (EDP) requires that Alice and Bob have pre-shared EPR pairs (maximally entangled Bell sate) with them [40, 73]. Alice can do *CNOT* [11] operation with her qubit say $|H\rangle$ and one of the qubits from EPR pair as ancillia then check the measurement result. This result is then shared publicly to Bob who also does the same operation (*CNOT*) with his received qubit. Both check for the error by declaring the measurement outcomes over public channel, which can then be corrected. Both bit and phase error correcting operations commute only for pre-shared Bell states [17, 40].

The difficulty of doing the above procedure ([40]) means, one should have the pre-shared EPR pairs and the distributed qubits stored in quantum memory that is hard to realise in practice [20]. Later, Shor and Preskill's security proof relaxed the requirement of EPR pairs shared between Alice and Bob. They suggested that it is sufficient to correct the bit and phase error just by using Calderbank-Shor-Steane (CSS) quantum error correcting code [12, 41]. It decouples bit and phase error which can later be corrected by classical error correction (EC) and privacy amplification (PA) respectively [17, 41, 48]. This also brings the security of prepare and measure (*P&M*) through entanglement based (EB) protocol. The end expression of the secure key rate is same as in Mayer's proof [72], only the error threshold is slightly changed. In Shor and

Preskill's proof they considered only ideal source and detectors. Later, Koashi [42] proved the security of BB84 protocol using complementarity principle. Also, another aspect of proving security of QKD is through entropic uncertainty relations [44, 45]. Security proofs against individual [74] and collective attacks [75] have also been done which leads to the same expression as in [41].

The basic security of the protocol can be understood as finding some parameter which could track the presence of Eve in the system along with distributing identical (error free) keys. For checking the security of any protocol one has to calculate the difference between its ideal condition and the real conditions in which the protocol is implemented. This difference can be calculated by trace distance between the two states of the systems as [37]

$$T(\rho_{ideal}, \rho_{real}) := \frac{1}{2}||\rho_{ideal} - \rho_{real}||. \tag{2.5}$$

Where $\rho_{ideal}$ is the density matrix for ideal and $\rho_{real}$ is the density matrix of real systems. The parameter that serves as smoking gun in tracking the presence of Eve in experiments is QBER (Quantum Bit Error Ratio/Rate). This quantity gives a fair indication as when to abort the protocol and when to go for further post-processing to extract secure keys. QBER also tells about the estimated key rate in real implementation scenario. The implication of QBER helps in creating secure key which will be seen in the subsequent sections.

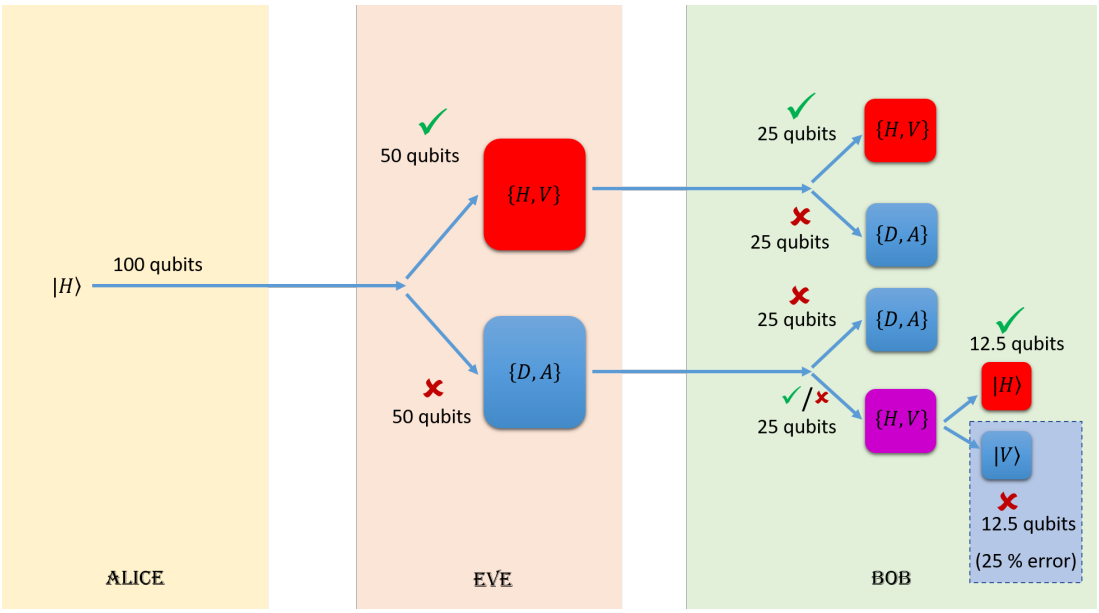



**Figure 2.4:** Intercept and Resend eavesdropping in BB84 protocol

### 2.2.1 QBER for Standard Intercept and Resend (IR) Attack on Individual Qubits

Alice prepares her photon polarization (qubits) randomly in $\{H,V\}$ and in $\{D,A\}$ basis for key distribution. Let us consider the case when Alice prepares state, say in $|H\rangle$ polarization and sends it to Bob. Eve in between intercepts it and sends to Bob a state based on the measurement results that she got. Then the error rate that Bob gets in his key is about 25% which can be seen in the Figure 2.4. For a given basis Eve guesses 50% of the time correctly which Alice has sent. The key that Bob gets has 25% error in it. After Eve's interception, half of the bits sent by her gets received in correct basis by Bob. The other half that Eve wrongly projected and is received by Bob randomly gives measurements in correct (according to Alice) and wrong basis. Half of the results in correct basis would give correct polarization state (Figure 2.4) rest will give wrong (as measurement results will be considered random). After sifting process Alice and Bob will take out small portion of key and check that the bits measured in compatible

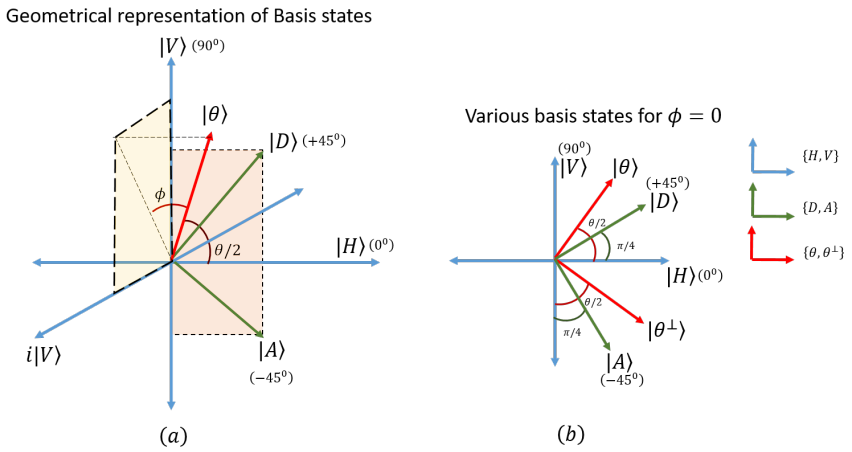



**Figure 2.5:** Schematics for intermediate state in Intercept Resend type attacks.

basis are same or not. In the discussed case, Eve steals half of the sifted key. Checking QBER will surely bring out her presence but extracting keys will not be possible [73].

Eve can do much more than just projecting the states into random basis. Instead, she projects the states in intermediate basis (Breitbart basis [24, 76]) to gain more information about the qubits sent by Alice. For a given basis the corresponding intermediate projection is written in the Eq.(2.6) and Eq.(2.7) as

$$|\theta\rangle = cos(\theta/2)|H\rangle + e^{i\phi} sin(\theta/2)|V\rangle \tag{2.6}$$

$$|\theta^\perp\rangle = sin(\theta/2)|H\rangle - e^{-i\phi} cos(\theta/2)|V\rangle. \tag{2.7}$$

Where $\theta$ and $\phi$ are the angle and phase between two states as shown in Figure 2.5 (a) represents the general case ($\theta \neq 0$, $\phi \neq 0$ ) and Figure 2.5 (b) represents the simple case for $\phi = 0$ that can be easily implemented in experiments. The above measurement returns to $\{H,V\}$ basis for $\theta = 0, \phi = 0$ and $\{D,A\}$ basis for $\theta = \pi/2, \phi = 0$. Provided the basis is known, Eve associates her measurement result with corresponding initial

state that is sent by Alice. Eve associates bit value 0 to her outcome $\theta$ and 1 to her outcome $\theta^{\perp}$. The conditional probabilities are then given by

$$P(\theta|H) = |\langle\theta|H\rangle|^2 = cos^2(\theta/2) \tag{2.8}$$

$$P(\theta|D) = |\langle\theta|D\rangle|^2 = \frac{1+sin\theta\ cos\phi}{2}. \tag{2.9}$$

Equation (2.8) tells the fact that given Alice sends $H$, what is the probability that Eve gets outcome $\theta$. Similarly, Eq.(2.9) tells about the occurrence of $\theta$ if the initial state is $D$. For all possible combinations of measurement outcomes and initial states sent, conditional probabilities are calculated in similar fashion which are given below.

$$P(\theta^{\perp}|V) = cos^2(\theta/2) \tag{2.10}$$

$$P(\theta^{\perp}|A) = \frac{1+sin\theta\ cos\phi}{2} \tag{2.11}$$

$$P(\theta^{\perp}|H) = P(\theta|V) = sin^2(\theta/2) \tag{2.12}$$

$$P(\theta^{\perp}|D) = P(\theta|A) = \frac{1-sin\theta\ cos\phi}{2} \tag{2.13}$$

Assuming that Eve already knows the basis declared by Alice during basis matching, the success probability for her is given by

$$P_E^{\{HV\}} := P(H|\theta) = |\langle H|\theta\rangle|^2 = P(V|\theta^{\perp}) = |\langle V|\theta^{\perp}\rangle|^2 = cos^2(\theta/2) \tag{2.14}$$

$$P_E^{\{DA\}} := P(D|\theta) = |\langle D|\theta\rangle|^2 = P(A|\theta^{\perp}) = |\langle A|\theta^{\perp}\rangle|^2 = \frac{1+sin\theta\ cos\phi}{2}. \tag{2.15}$$

The main aim of Eve is to maximize these probabilities in both bases which can be mathematically described as

$$P_E = \underset{\theta,\phi}{max}\left(P_E^{\{HV\}}, P_E^{\{DA\}}\right). \tag{2.16}$$

For a symmetric attack (i.e Eve intercepts both the basis equally) the success probability becomes equal which is the case for optimal strategy. From Eq.(2.14) and Eq.(2.15), the mutual information between Alice and Eve can be written as [77–79]

$$I^{HV}(A:E) = 1 - H\left(P_E^{\{HV\}}\right) \tag{2.17}$$

$$I^{DA}(A:E) = 1 - H\left(P_E^{\{DA\}}\right) \tag{2.18}$$

Where, $H(p)$ is the binary entropy function that is $H(p) = -p\log(p) - (1-p)\log(1-p)$. Equation (2.17) and (2.18) represents the mutual information in $\{H,V\}$ and $\{D,A\}$ basis respectively, and overall information that Eve gains for symmetric attack will be $I_E = [I^{HV}(A:E) + I^{DA}(A:E)]/2$. The optimal guessing probability for Eve will be $P_E^{\{HV\}} = P_E^{\{DA\}} = P_E^I$ which is

$$P_E^I = \left(1 + 1/\sqrt{2}\right)/2 = 0.85 \tag{2.19}$$

The guessing probability for Eve i.e $P_E$ is increased from 75% to 85% as we see in Eq.(2.19). For the case when Eve uses the strategy of either projecting in $\{H,V\}$ or

$\{D,A\}$ basis then the success probability for guessing correct bit becomes

$$P_E^{II} = 0.75, \tag{2.20}$$

result in Eq.(2.20) can be understood as if Eve chooses correct basis (either $\{H,V\}$ or $\{D,A\}$) then probability of guessing right bit is maximum while for the case of wrong basis choice it becomes 50% (from BB84 protocol).

Although $P_E^I$ is greater than $P^{II}$ but the mutual information (MI) gives different results for the two cases,

$$\begin{aligned} I^I(A:E) &= 1 - H(0.85) \\ &= 0.4, \end{aligned} \tag{2.21}$$

and for the case of Eq.(2.20) it becomes

$$\begin{aligned} I^{II}(A:E) &= 1 - H(0.75) \\ &= 0.19. \end{aligned} \tag{2.22}$$

It is clear that the MI for intermediate basis case ($II$) becomes less than MI for the case $I$ where Eve randomly projects in two basis [73]. However, QBER in both the cases remains same which is discussed below.

The QBER can be calculated as the conditional probability between Bob and Alice's bits for compatible basis. For a given basis provided that Alice sends a polarization state $|H\rangle$ as given in Eq.(2.23), the probability of its flipping can be written as

$$\begin{aligned} P_{error}^{\{HV\}} = P(V|H) &= P(V|\theta)P(\theta|H) + P(V|\theta^{\perp})P(\theta^{\perp}|H) \\ &= 2cos^2(\theta/2)\ sin^2(\theta/2) \\ &= sin^2\theta/2. \end{aligned} \tag{2.23}$$

In Eq.(2.23) the first term says the conditional probability that Alice sends $H$ and Eve gets $\theta$, then she sends that state to Bob and he gets the result as $V$. It is similar for the second case when Eve gets the outcome of $\theta^{\perp}$. For both the cases i.e for $P(V|H)$ and $P(H|V)$ error probability remains the same. In the same way error probability can be evaluated for $\{D,A\}$ basis. The error probability for that is $P_{error}^{\{DA\}} = P(A|D) = P(D|A) = (1 - sin^2(\theta)\ cos^2(\phi))/2$ therefore, the average error probability is given by

$$\begin{aligned} P_{error} &= (P_{error}^{\{HV\}} + P_{error}^{\{DA\}})/2 \\ &= [1 + (1 - cos^2\phi)\ sin^2\theta]/4 \end{aligned} \tag{2.24}$$

The value of $\theta$ and $\phi$ for optimizing Eve's guessing probability will be $\theta = \pi/4$ & $\phi = 0$. From Eq.(2.24) the QBER between Alice and Bob is then 0.4 (25%). Though the error rate is same but Eve has more potential to guess the incoming sates by using intermediate basis. The secure key rate between Alice and Bob is [75]

$$R = I(A:B) - I(A:E). \tag{2.25}$$

Non zero secure key can only be generated if $I(A:B) > I(A:E)$. For the case ($I$) MI between Alice and Bob is

$$\begin{aligned} I^I(A:B) &= 1 - H(QBER) \\ &= 0.185. \end{aligned} \tag{2.26}$$

Where QBER is 0.4, the mutual information between Alice and Bob comes out to be 0.185 bits per symbol. $I^{II}(A:B)$ is same as Eq.(2.26) because the QBER is same as it has been seen in Figure 2.4. Already seen from Eq.(2.21) and Eq.(2.22) that $I(A:E)$ is more than $I(A:B)$ therefore, it is impossible to extract non zero secret key.

### 2.2.2 QBER Against General Attacks by Eve for Ideal Sources and Detectors

Eavesdropping the key distribution between Alice and Bob can occur in various ways. It can be classified on the basis of number of qubits involved in the attack and the process of measuring them. These can be *individual*, *collective* or *coherent*, which are briefly explained below.

- **Individual attack**:

  Eve attaches her ancillary qubits (probe) to Alice's qubits then she makes unitary operation on them. The result will make entangled state with Alice's qubits. Eve keeps her ancilla (probe) and sends the other to Bob. She then makes measurement on the individual system (as shown in Figure 2.6) before Alice sends other qubit. Eve can optimally gain the information of individual qubits by designing her measurements on them. As she has to do this before the next qubits's arrival, she can't take the advantage of classical communication for error correction between Alice and Bob.

- **Collective attack**:

  The attack procedure is same as the "Individual" attack only, the measurement is taken differently. After entangling the probe, Eve stores her qubits in quantum memory and wait till Alice sends all her qubits. She then makes measurements

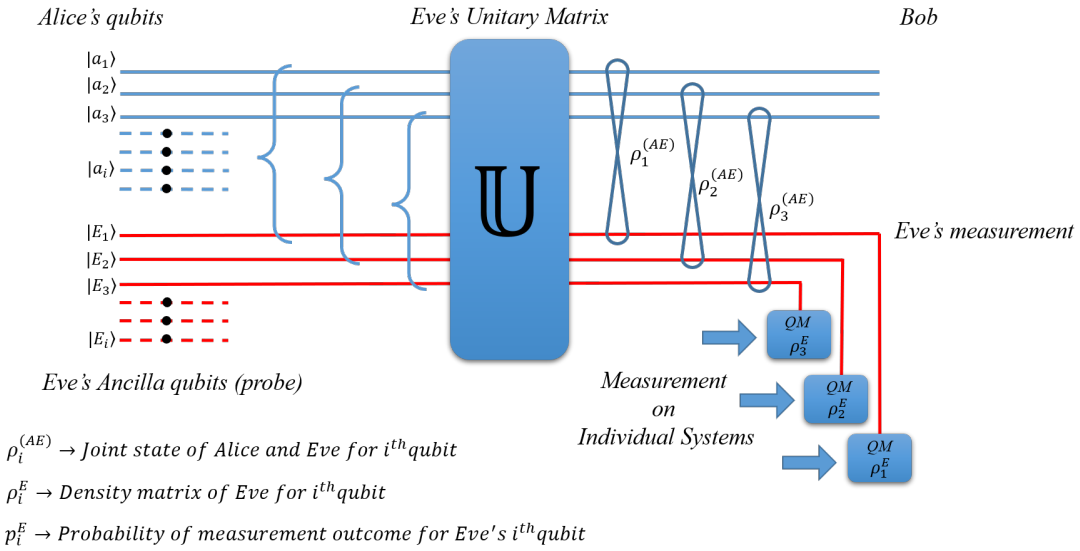



**Figure 2.6:** Individual attack for QKD protocol. Eve attaches her probe (Red) with Alice's qubits (blue) and does the unitary interaction to make them entangled and stored in her quantum memory (QM). Eve then measures them individually by tracing out Alice's qubit after she sends them to Bob.

on collective system of the qubits ($\rho^E = \rho_1^E \otimes \rho_2^E \otimes ...$) as shown in Figure 2.7. Storing of all the probe qubits by Eve waiting at the end to make measurements gives her advantage of listening to all the basis information about the qubits revealed during classical communication. The maximum information that Eve can get out of the stored qubits with extra knowledge of basis is bounded by Holevo information [11, 80]. Eve measures this information on the collective system to get the knowledge about the key.

- **Coherent attack**:

  It is the most general attack as shown in Figure 2.8 and also the most powerful one. Eve attaches a single higher dimensional probe to all of the Alice's qubits. She jointly performs measurements on the higher dimensional probe after classical communication between Alice and Bob. Here, Eve's single probe is entangled with all the qubits sent by Alice. The measurement on Eve's probe

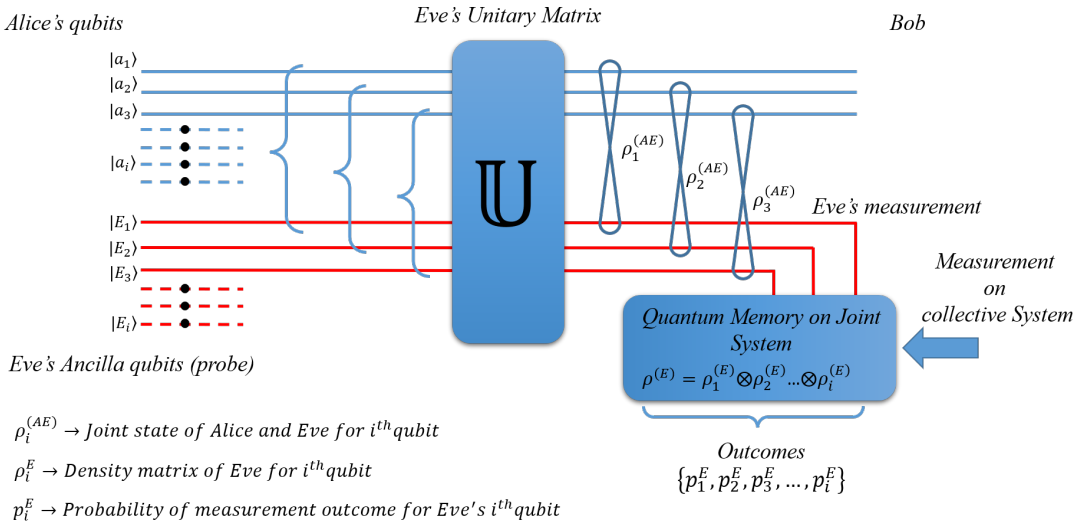



**Figure 2.7:** Collective attack for QKD protocol. Eve attaches her probe with Alice's qubits (similar to Fig. 2.6). Eve then measures her probe on collective system after taking the help of basis information and classical communication between Alice and Bob.

will reveal the correlation between the individual qubits that might provide additional information to prepare her measurement setting to figure out the correct bit. Correlation between qubits is helping Eve to gain additional information therefore, these kind of attacks are called joint or coherent attacks. These attacks are difficult to implement and hard to analyse mathematically as well. For most of the cases for proving unconditional security collective attacks are considered as special case of joint or coherent attack [81].

### Key Rate and QBER Threshold Against Individual Attacks

The key rate analysis in this chapter deals with various situations. First the key rate against individual attack is calculated and the error threshold is obtained. Then against collective attack this rate is modified and similarly QBER is calculated. Lastly, for realistic sources how one can generate secure key rate against some known attacks are discussed.

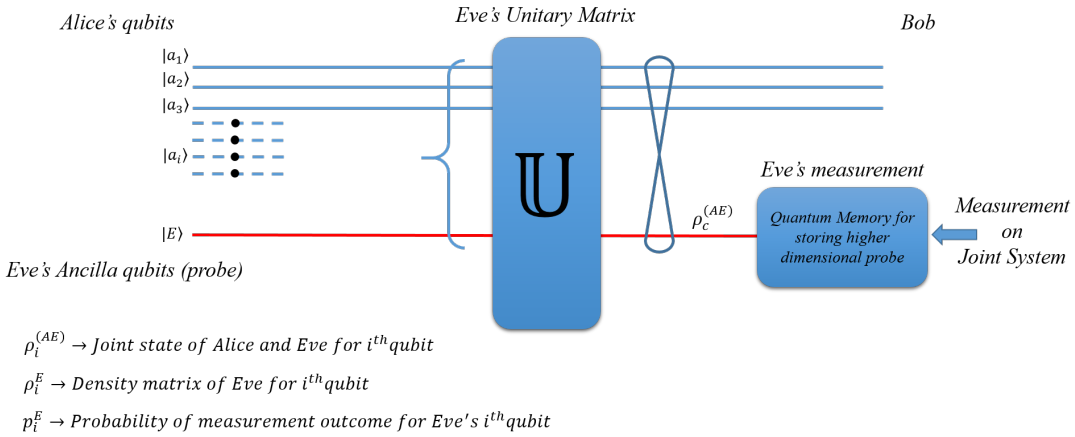



**Figure 2.8:** Coherent attack for QKD protocol. Eve attaches her single large dimensional probe with Alice's qubits. The resultant joint state is correlated with the other Alice's qubits. She then stores her state in quantum memory and make measurements after classical communication.

### QBER Threshold Against Individual and Collective Attacks for BB84 Protocol with Ideal Setup

From the above definitions it is clear that preparing Eve's state in individual and collective attacks are same, only the measurement process is different. Eve can make her ancilla qubits entangled with the Alice through some unitary transform. Then after storing her part she sends the original qubits to Bob. Based on the type of attacks the corresponding error bounds can be set. The unitary transform that Eve makes is given by

$$\begin{aligned} \mathbb{U}|H\rangle|E\rangle &= |X\rangle \\ \mathbb{U}|V\rangle|E\rangle &= |Y\rangle. \end{aligned} \tag{2.27}$$

where, $\mathbb{U}$ is the unitary operation done by Eve, $|E\rangle$ is the initial state of her probe, $|X\rangle$ and $|Y\rangle$ are the joint state of Alice and Eve's system for $H$ and $V$ states respectively. The same unitary operation for Alice's qubits sent in $\{D,A\}$ similarly results in sates

$|U\rangle$ and $|V\rangle$. From Eq.(2.27) there can be various forms of joint states of Alice and Eve (specifically various Eve's states), which can give some information about the states of Alice to Eve. The joint system of Alice and Eve is $|X\rangle$ for state $|H\rangle$ chosen by Alice. The joint system of Alice and Eve may or may not be entangled. The composite system of Alice and Eve can be written in the form of Schmidt decomposition as [11]

$$|X\rangle_{AE} = \sum_i \lambda_i |i_A\rangle |i_E\rangle. \tag{2.28}$$

Where $|i_A\rangle$ are the states belonging to Alice's system and similarly $|i_E\rangle$ belonging to Eve. $\lambda_i$ are non negative real values called as Schmidt coefficients satisfying $\sum_i \lambda_i = 1$. As discussed in detail [16, 74] that for optimal eavesdropping, the Schmidt decomposition of the joint states $(|X\rangle, |Y\rangle, |U\rangle, |V\rangle)$ must take the form [74, 82]

$$\begin{aligned} |X\rangle &= \sqrt{F_{HV}}|H\rangle|E_{HH}\rangle + \sqrt{\delta_{HV}}|V\rangle|E_{HV}\rangle \\ |Y\rangle &= \sqrt{F_{HV}}|V\rangle|E_{VV}\rangle + \sqrt{\delta_{HV}}|H\rangle|E_{VH}\rangle, \end{aligned} \tag{2.29}$$

when Alice sends in $\{HV\}$ basis. For the states sent in $\{DA\}$ basis

$$\begin{aligned} |U\rangle &= \sqrt{F_{DA}}|D\rangle|E_{DD}\rangle + \sqrt{\delta_{DA}}|A\rangle|E_{DA}\rangle \\ |V\rangle &= \sqrt{F_{DA}}|A\rangle|E_{AA}\rangle + \sqrt{\delta_{DA}}|D\rangle|E_{AD}\rangle. \end{aligned} \tag{2.30}$$

Here the final state of Eve $|E_{HH}\rangle$ means that given Eve gets the result "$H$"(upon measurement) the probability that Alice sent her state in "$H$" similar to (Eq.(2.8)-Eq.(2.13)). In general the final state of Eve's probe ($|E_{ij}\rangle$) are non orthogonal (i.e., $\langle E_{ii}|E_{jj}\rangle \neq 0$) where $i, j \in H, V, D, A$. $\sqrt{F_{ij}}$'s and $\sqrt{\delta_{ij}}$'s are the Schmidt coefficients for corresponding states. Here, $F_{HV}$ is the fidelity for Eve that represents the success in predicting the state of Alice for $H, V$ basis [16, 82]. $\delta_{HV}$ is the disturbance created by her while measuring it. $\delta_{HV}$ and $\delta_{HV}$ denotes the QBER for $H, V$ and $D, A$ basis,

that Alice and Bob observe while doing parameter estimation (PE).

Applying the conditions of inner products to the corresponding states, the connection between the two different basis states of Eve's output becomes

$$\begin{aligned} 2\sqrt{F_{DA}}|E_{DD}\rangle &= \sqrt{F_{HV}}(|E_{HH}\rangle + |E_{VV}\rangle) + \sqrt{\delta_{HV}}(|E_{HV}\rangle + |E_{VH}\rangle) \\ 2\sqrt{F_{DA}}|E_{AA}\rangle &= \sqrt{F_{HV}}(|E_{HH}\rangle - |E_{VV}\rangle) + \sqrt{\delta_{HV}}(|E_{VH}\rangle - |E_{HV}\rangle). \end{aligned} \tag{2.31}$$

Similar expression can be obtained for $|E_{ij}\rangle$. All the above equations represent the Alice and Eve's system in most general QKD scenario. Here, Eve is only bounded by the laws of physics and can use quantum memory to perform attacks. Eve's aim is to minimise the error in both the basis so that she could eavesdrop optimally. For, optimal eavesdropping in the most general setting, the errors (QBER) should be symmetric (error in $\{H,V\}$=error in $\{D,A\}$) [74, 82]. This means

$$\delta_{HV} = \delta_{DA} = \delta, \tag{2.32}$$

i.e., QBER imparted by Eve in both the basis must remain same. Same goes for the case of fidelity ($F_{HV} = F_{DA} = F$). Eve can create various kinds of interactions and corresponding matrices; to make her eavesdropping effective. Among those various states only the optimal choice will give maximum information to Eve. So, hunt for optimal interaction which can give Eve maximum information is the main task. On physical ground the Schmidt coefficients must be real, that denotes orientation with respect to some basis. While choosing these interactions Eve must make a note that her probes must follow [74, 83]

$$\begin{aligned} \langle E_{ii}|E_{ij}\rangle &= 0 \qquad\qquad i \neq j \\ \langle E_{ii}|E_{jj}\rangle &\neq 0, \end{aligned} \tag{2.33}$$

using above conditions along with the unitarity operation of Eq.(2.27), one of the ways to parametrize them is given by [74]

$$\begin{aligned}
|E_{HH}\rangle &= |H\rangle|H\rangle \\
|E_{HV}\rangle &= |V\rangle|H\rangle \\
|E_{VV}\rangle &= \cos\alpha|H\rangle|H\rangle + \sin\alpha|V\rangle|H\rangle \\
|E_{VH}\rangle &= \cos\beta|H\rangle|V\rangle + \sin\beta|V\rangle|V\rangle.
\end{aligned} \tag{2.34}$$

Where $\alpha$ and $\beta$ are the angles between the states $|E_{HH}\rangle$, $|E_{VV}\rangle$, $|E_{HV}\rangle$ and $|E_{HV}\rangle$. Equation (2.34) looks simpler and can be realised in a practical framework. From $\langle E_{AA}|E_{AA}\rangle = 1$ and using this value in Eq.(2.31) for basis conversion, we get the value of disturbance as

$$\delta = \frac{1-\cos\alpha}{2-\cos\alpha+\cos\beta}. \tag{2.35}$$

$\alpha = \beta$ gives the situation for symmetric distribution, this brings the value of error as

$$\delta = (1-\cos\alpha)/2. \tag{2.36}$$

This value also gives maximum information gain (guessing probability) to Eve. The expression of QBER ($\delta$) indicates maximum information that Eve can get. The joint state of Alice and Eve after the interaction for $\{H,V\}$ basis is given by

$$\begin{aligned}
\rho_X^{AE} &= \left(F|H\rangle|E_{HH}\rangle\langle H|\langle E_{HH}| + \sqrt{F\delta}|H\rangle|E_{HH}\rangle\langle V|\langle E_{HV}|\right) \\
&\quad + \left(\sqrt{\delta F}|V\rangle|E_{HV}\rangle\langle H|\langle E_{HH}| + \delta|V\rangle|E_{HV}\rangle\langle V|\langle E_{HV}|\right) \\
\rho_Y^{AE} &= \left(F|V\rangle|E_{VV}\rangle\langle V|\langle E_{VV}| + \sqrt{F\delta}|V\rangle|E_{VV}\rangle\langle H|\langle E_{VH}|\right) \\
&\quad + \left(\sqrt{\delta F}|H\rangle|E_{VH}\rangle\langle V|\langle E_{VV}| + \delta|V\rangle|E_{VH}\rangle\langle V|\langle E_{VH}|\right)
\end{aligned} \tag{2.37}$$

Now, taking partial trace over the Alice's system the state left to Eve is

$$\begin{aligned}\rho_X^E &= F|E_{HH}\rangle\langle E_{HH}| + \delta|E_{HV}\rangle\langle E_{HV}| \\ \rho_Y^E &= F|E_{VV}\rangle\langle E_{VV}| + \delta|E_{VH}\rangle\langle E_{VH}|\end{aligned} \tag{2.38}$$

After declaration of basis by Alice, from the above set of states, Eve needs to make measurement that successfully discriminates between two density matrices ($\rho_X^E$ and $\rho_Y^E$). This is not an easy task as the process is non deterministic because the density matrices are non orthogonal. The method that Eve can apply [75] is, first discriminate between $|E_{ii}\rangle$ and $|E_{ij}\rangle$ as they are orthogonal. Then she can discriminate between $|E_{ii}\rangle$ and $|E_{jj}\rangle$ (in this case $|E_{HH}\rangle$ and $|E_{VV}\rangle$). As, the states are non orthogonal ($|E_{ii}\rangle$ and $|E_{jj}\rangle$) Eve can at best probabilistically distinguish between them. Trick to find these states has been described in [84]. The overlap between $E_{HH}$ and $E_{VV}$ is "$\cos\alpha$" as can be seen from Eq.(2.34). The maximum probability with which Eve can successfully discriminate between them is "$(1+\sin\alpha)/2$". This probability is same for rest of the states as the attack is symmetric. This probability is with which Eve can successfully determine the state sent by Alice. Therefore, $P_E^{success} = (1+\sin\alpha)/2$ is the success probability of Eve and the mutual information between the Alice and her is

$$I(A:E) = 1 - H\left(\frac{1+\sin\alpha}{2}\right) \tag{2.39}$$

and the mutual information for Alice Bob can be obtained from $\delta$ as

$$I(A:B) = 1 - H\left(\frac{1-\cos\alpha}{2}\right). \tag{2.40}$$

Finding the cutoff error (QBER) which determines the successful running of the pro-

tocol and secret key extraction is then given by [73]

$$\begin{aligned} I(A:E) &= I(A:B) \\ \frac{1+\sin\alpha}{2} &= \frac{1-\cos\alpha}{2}. \end{aligned} \tag{2.41}$$

The Eq.(2.41) gives the value of $\alpha = \frac{3\pi}{4}$, which indicates that the QBER is

$$\delta = \frac{1-\frac{1}{\sqrt{2}}}{2} = 0.1465. \tag{2.42}$$

For individual attacks, when Eve uses quantum system for her information gain, the QBER for the ideal BB84 QKD system is 14.6% [74]. One can extract the non zero secret key if the QBER is less than this value, under the assumption that Eve is attacking the qubits individually.

### Key Rate and QBER Threshold Against Collective Attacks

For collective attack, the state preparation is same as that of individual attack, but only it is different in the measurement process. Here, Eve knows the classical post-processing information along with the knowledge of basis choice of Alice and Bob and exploits this to gain information. Optimization for attack strategy requires that Eve must make measurement on whole qubit system. Since the use of conjugate basis is perfectly symmetric, so the optimal strategy is through ancilla interaction which have symmetric eigenstates. Here the Eve's combined state for all the qubits sent by Alice is given by as already seen in Eq.(2.38)

$$\rho_a = F|E_{ii}\rangle\langle E_{ii}| + \delta|E_{ij}\rangle\langle E_{ij}|. \tag{2.43}$$

Where $a, a^{\perp} \in (X, Y, U, V)$ and the above density matrix is same for all the other polarization states. As, the basis information is already known to Eve, the states between which she needs to distinguish are given by

$$\begin{aligned} \rho_a^E &= F|E_{ii}\rangle\langle E_{ii}| + \delta|E_{ij}\rangle\langle E_{ij}| \\ \rho_{a^{\perp}}^E &= F|E_{jj}\rangle\langle E_{jj}| + \delta|E_{ji}\rangle\langle E_{ji}|. \end{aligned} \tag{2.44}$$

The occurrence of these states in Eve's memory is equally likely and random moreover, since Eve knows about the basis which Alice sends, the only challenge is to distinguish between above two states $\rho_{a^{\perp}}^E, \rho_a^E$. The mixed state that Eve has is $\rho^E = (\rho_{a^{\perp}}^E + \rho_a^E)/2$. Even under the optimal strategy the total information gain by Eve can't exceed the Holevo information bound of the channel between Alice and Eve. As already discussed in section (2.2.2) for collective attack (Figure 2.7), the maximum amount of information that Eve can take to her advantage is given by Holevo information $\chi(A:E)$ [11, 75, 80].

$$\chi(A:E) = S(\rho^E) - \frac{S(\rho_{a^{\perp}}^E) + S(\rho_a^E)}{2}, \tag{2.45}$$

where $S(\rho)$ is the Von Neumann entropy of the density matrix $\rho$ [11]. The key rate is then given by

$$R = I(A:B) - \chi(A:E) \tag{2.46}$$

For forward reconciliation it is the difference between the mutual information of Alice-Bob system and the Holevo information of Alice-Eve system. From Eq.(2.44) it can be shown that from $\langle E_{ii}|E_{ij}\rangle = 0$, $\rho_a^E, \rho_{a^{\perp}}^E$ can be diagonalized [75]. The Von-Neumann

entropy of the individual states can be written as

$$\begin{aligned} S(\rho_a^E) &= -Tr[\rho_a^E \log \rho_a^E] \\ &= -F \log F - \delta \log \delta \\ &= -(1-\delta)\log 1 - \delta - \delta \log \delta = H(\delta). \end{aligned} \tag{2.47}$$

Similar result will be there for the case of $S(\rho_{a\perp}^E)$. So, the second term in Eq.(2.45) will be Shannon entropy $H(\delta)$. It is already known from Eq.(2.26) that the first term in Eq.(2.46) is $1 - H(\delta)$, this leads to the secret key rate as

$$R = 1 - S(\rho^E). \tag{2.48}$$

Now, the task is to find the value of $S(\rho^E)$ in the Eve's system. Even though Eve uses quantum memory but the maximum amount of accessible information she can get from the state is

$$\chi = S(\rho^E) - \left(\sum p_i S(\rho_i)\right) \tag{2.49}$$

From the properties of Von Numann entropy it can be shown that [11]

$$S(\rho) \leq \sum p_i S(\rho_i) - \sum p_i log p_i. \tag{2.50}$$

The above equation holds equality only if the density matrices are orthogonal, where $p_i$'s are the probability of density matrix $\rho_i$. Here, $\rho_i$'s are the two density matrices $\rho_F^E$ and $\rho_\delta^E$ with corresponding probabilities $F$ and $\delta$ so that it ($\rho^E$) can be decomposed as the orthogonal mixture of these two density matrices as

$$\rho^E = F\rho_F^E + \delta\rho_\delta^E. \tag{2.51}$$

Following the relation in Eq.(2.50) it can be seen that

$$\begin{aligned} S(\rho) &= (FS(\rho_F) + \delta S(\rho_\delta)) - (F\log(F) + \delta\log(\delta)) \\ S(\rho) - (FS(\rho_F) + \delta S(\rho_\delta)) &= -(F\log(F) + \delta\log(\delta)) \\ S(\rho) - (FS(\rho_F) + \delta S(\rho_\delta)) &= H(\delta). \end{aligned} \tag{2.52}$$

As, we already know $F = 1-\delta$, putting it in Eq.(2.49) we get

$$S(\rho^E) - \left(\sum p_i S(\rho_i)\right) = H(\delta) \tag{2.53}$$

Second term in the L.H.S can be shown from the proof derived in [75] that it is equal to Shannon entropy of error $\delta$. Therefore, the key rate equation against collective attack becomes

$$R = 1 - 2H(\delta) \tag{2.54}$$

where, $\delta$ is the QBER. The above proof is already done by Shor and Preskill [41] where they give the QBER threshold as 11%. The Eq.(2.54) serves as the generic equation for calculating the key rate from QBER for ideal sources and detectors. For asymmetric attack, the secure key rate in Eq.(2.54) is modified as

$$R = 1 - H(\delta_b) - H(\delta_p). \tag{2.55}$$

Where $\delta_b$ is the bit error rate and $\delta_p$ is the phase error rate (errors in $\{H,V\}$ and $\{D,A\}$ respectively).

The expression in Eq.(2.55) is only for ideal case. QKD in real scenario will incorporate all the information leaked out due to device imperfections into the secret key rate formula [20, 73]. These modifications are device and setup dependent and will

change accordingly. Keys can be shortened due to these leakage during error correction (EC) and privacy amplification (PA). Key rate's basic mathematical structure for real life QKD implementation is given by

$$R = (1 - H(\delta) - \text{leak}_{EC}(\delta)), \tag{2.56}$$

where, $H(\delta)$ is binary entropy and $\text{leak}_{EC}(\delta)$ is leakage of extra information during error correction due to device imperfection.

### 2.2.3 Secure Key Rate for Realistic Sources

The key rate equation 2.55, cannot be used directly for realistic conditions as device imperfections will reduce the rate further. Including device imperfections in the key rate was first incorporated by Mayers *et.al* [47, 72]. Though there are several calculations of key rate that have been done [20, 38, 48] but, Mayers follows straight forward approach. This includes standard EC and PA calculation after the protocol due to all realistic factors.

Let, $\overrightarrow{K}$ is a random variable (RV) giving private keys shared between Alice and Bob in each turn $\overrightarrow{K} \in \{k_1, k_2, k_3, ..., k_n\}$. Length of the secret key is $m$ bits so its domain is $\overrightarrow{K} : \{0,1\}^m$ which has possible dimension of $2^m$ ($2^m$ possibilities of keys). $V$ is RV associated with the Eve's knowledge about the key for any attack strategy. $V \in \{v_1, v_2, v_3, ..., v_n\}$. Two main criterion needs to be defined for the security of QKD which are stated below.

- **Privacy**

  The key that Alice and Bob generated must be completely private from rest of the "world" (Eve). Privacy between Alice and Eve's key is given by the conditional

information

$$H(k|v) \geq m. \tag{2.57}$$

Where, $k$ is the key string shared between Alice and Bob and $v$ is the Eve's knowledge. This information must be atleast '$m$' bits (length of the final key). For realistic condition it is impossible to achieve completely private key from Eve and the value is slightly less than $m$ and Eq.(2.57) is rewritten as

$$H(k|v) \geq m - \varepsilon_1(N,m). \tag{2.58}$$

Here, $\varepsilon_1(N,m)$ is a small value ($\geq 0$) which depends upon various factors such as channel effect, final key length, total signal sent ($N$) (depends upon QKD system and post processing technique) [72]. This value goes to zero for very large value of $N$ and indicates that a protocol is "$\varepsilon_1$" private.

- **Integrity**

  Even after passing the validation test in parameter estimation (PE) the probability that Alice and Bob cannot generate secret key must be very small. Mathematically it can be shown as

$$Pr(\text{no private key} \cap \text{pass in PE}) < \varepsilon_2(N,m), \tag{2.59}$$

the function $\varepsilon_2(N,m)$ takes very small value. It depends upon the fact that there might be a finite possibility of error mismatch from the QBER in PE bits, than the bit string which did not go for PE. This can create problem in EC if it exceeds the QBER threshold and secret key will not be generated. The $\varepsilon_2(N,m)$ becomes negligible for asymptotic limit and depends upon the samples [72].

These two criteria perfectly describe the condition for generating secret key in ideal picture. The above two conditions (Eq.(2.58) and Eq.(2.59)) mainly define the security proof as given in Mayers' *et.al*. Similar approach is followed by almost all other types of key generation protocols [49, 51, 65]. These conditions are based on the fact that both Alice and Bob have ideal devices. For device imperfection more conditions have to be implied based on the experimental conditions. BB84 protocol uses weak coherent laser pulses (WCP), in practice as they are coherent states they are not true single photons. This nature of the source can compromise the unconditional security of the protocol. For achieving same level of security as before few more modifications must be added in security definition.

For WCP in picture, average number of photons per pulse ($\mu$) is known to Alice and Bob. The probability of two or more photons per pulse is

$$P_{\geq 2}(\mu) = 1 - e^{-\mu} - \mu e^{-\mu}. \tag{2.60}$$

This probability multiplied by the laser repetition rate will give the number of multi-photon pulses $M$. $M$ is dependent upon $\mu$ as seen from Eq.(2.60). $M_{max}$ is the maximum value of multiphotons that is allowed in the protocol ( $M$ going to zero indicates $\mu$ also tending to zero, which is not desirable as no signals will be received). Probability that $M$ exceeding $M_{max}$ is given by

$$Pr(M > M_{max}) < e^{-\tau_M^2 N}, \tag{2.61}$$

where, $\tau_M$ is constant value depends upon experiments [72]. This goes negligible for large $N$. The above equation tells the probability of multi-photons exceeding the pre-decided value must be very less or asymptotically negligible. The output state from

the laser can be written as the coherent state [85, 86].

$$|\alpha\rangle = e^{\frac{-|\alpha|^2}{2}} \sum_{j=0}^{\infty} \frac{\alpha^j}{\sqrt{j!}} |j\rangle \tag{2.62}$$

The state of a single pulse coming out the laser can be written as [87, 88]

$$\begin{aligned} \rho &= \frac{1}{2\pi} \int |\alpha\rangle\langle\alpha| d\{\alpha\} \\ &= \frac{1}{2\pi} \int_0^{2\pi} ||\alpha|e^{i\phi}\rangle\langle|\alpha|e^{i\phi}| d\phi \end{aligned} \tag{2.63}$$

considering phase randomization (making phase of each pulse random) so that the above state can be considered as the mixture of Fock states ($|n\rangle$). Phase randomization is important as it can lead to various information leakage to the eavesdropper [89]. The state $\rho$ of the single pulse is

$$\begin{aligned} \rho &= e^{-|\alpha|^2} \sum \frac{|\alpha|^{2j}}{j!} |j\rangle\langle j| \\ &= \sum_j p_j |j\rangle\langle j| \end{aligned} \tag{2.64}$$

where $p_j$ ($p_j = e^{-\mu}\mu/j!$) is probability of $j$ photons in the corresponding pulse and $\mu = |\alpha|^2$. From this equation one can fix the value of average photon number by looking at the intensity ($|\alpha|^2$). It should be made sure that the multi-photon probability must be negligible ($P(M > M_{max}) \ll 1$). The detection efficiency is independent of the basis selection by Bob. The condition for minimum detection rate ($r_{min}$) to continue the protocol is

$$1 > r_{min} > M_{max}/N \tag{2.65}$$

Equation (2.65) indicates that the minimum detection rate $r_{min}$ (as some of the photons may get lost in the channel) must be greater than the detection rate of multi photon fraction ($M_{max}/N$) [20, 81].

In the protocol, basis choice by Alice is given by $\alpha_i \in \{HV, DA\}$ and the bit choice is given by $g_i \in \{0,1\}$ which comes from possible sates $(|H\rangle, |V\rangle, |D\rangle, |A\rangle)$. The total number of detection results consist of set $\mathscr{D}$. Also Bob's basis choice is $b_i \in \{HV, DA\}$ and bit choice is $h_i \in \{0,1\}$. Total signals registered by Bob is the raw key size detected by Bob ($n = |\mathscr{D}|$). Alice's basis set for $N$ signals sent is $\overrightarrow{a} = (a_1, a_2, ..., a_N) \in \{HV, DA\}^N$ and Bob's detected basis is then $\overrightarrow{b} = (b_1, b_2, ..., b_N)$. The bits of Alice and Bob are $\overrightarrow{g} = (g_1, g_2, g_3, ..., g_N)$ and $\overrightarrow{h} = (h_1, h_1, ..., h_N)$ respectively. In realistic channel Bob receives less amount of signals than Alice, so bit length of the raw key is the number of signals received by Bob.

The number of bits that goes for validation testing (parameter estimation) with probability $P_R$ is $\mathscr{R}$ which belongs to subset of $\mathscr{D}$ (signals detected by Bob). Sifting belongs to the set where Alice and Bob performed their measurements in compatible basis. Alice announces the times when they detected the signals in same basis to Bob i.e $\Omega = \{i \in \mathscr{D} : a_i = b_i\}$. The test signals of Alice belongs to set $T = \Omega \cap \mathscr{R}$ which goes for PE. The remaining signals which will finally form the sift key and will go for correction are given by $\mathbb{E} = (\Omega \cap \bar{\mathscr{R}})$. $|\mathbb{E}|$ $(= l\text{bits})$ is the sift key length that is left after PE as shown in the Figure 2.9. The final sifted key vectors for Bob is then $\overrightarrow{g}(\mathbb{E})$ (basis choice) and $\overrightarrow{h}(\mathbb{E})$ (bit values obtained).

The error correcting procedure follows linear codes which are easier to implement [90, 91]. The number of errors that can be corrected is then given by

$$\delta(1 - P_R)|\Omega|, \tag{2.66}$$

where $\delta$ is the error for 1 bit of key generated. Equation (2.66) tells that the error corrected keys are the ones taken from the rest of the set which does not go for parameter estimation. For realistic cases as mentioned by [47] more errors might be needed for

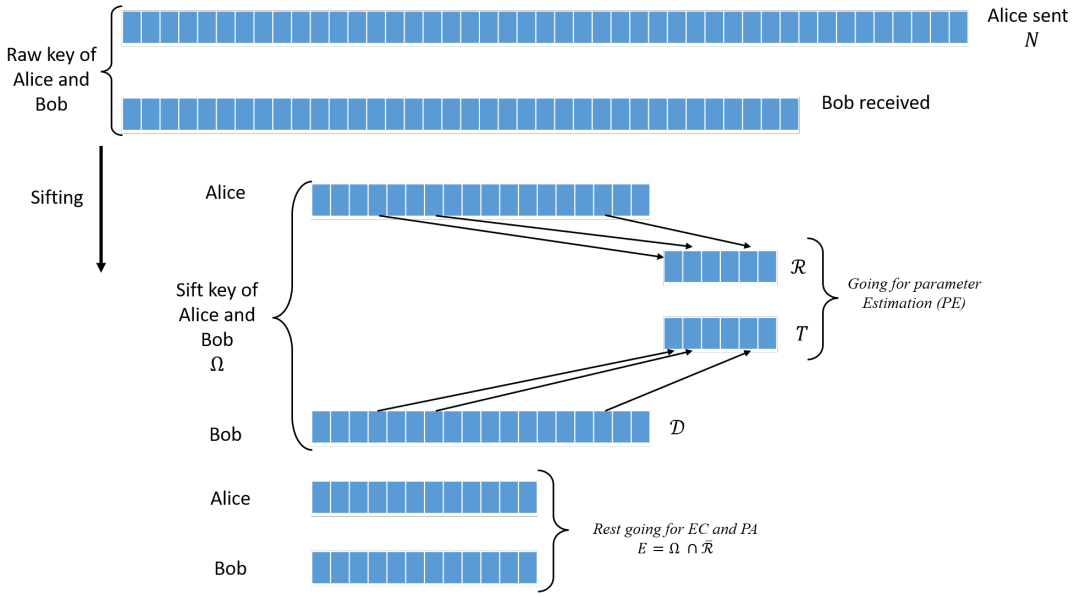



**Figure 2.9:** Schematics for post processing before PA. Sifting process equalises the number of keys between Alice and Bob. Part of some keys being sacrificed during parameter estimation (PE), rest going for EC and PA

correction

$$(\delta + \tau_{ec})(1 - P_R)|\Omega|. \tag{2.67}$$

Equation (2.67) sets a bound on the correctness of the key, if the error is less than Eq.(2.66) then both Alice and Bob can have same keys i.e.

$$\overrightarrow{h}(\mathbb{E}) = \overrightarrow{g}(\mathbb{E})$$

After privacy amplification the final secret key of Alice and Bob is given by

$$\overrightarrow{K} = K(\overrightarrow{h}) = K(\overrightarrow{g}), \tag{2.68}$$

where, $K(x)$ is the operation done to shrink it to that level where Eve has negligible knowledge of the key [92]. For final keys to be extracted, the number of errors should be less than half of the key bits that is needed for privacy amplification [81, 93]. There-

fore, the minimum number of bits going for extraction that will give secret key is given by

$$\frac{l_{min}}{2} \geq (\delta + \tau_{ec})(1 - P_R)n, \tag{2.69}$$

where, $\tau_{ec}$ is parameter fixed according to the error correction protocol used specifically for finite key case. For a simple case where the duration of the protocol is very large, as a result number of signals received are huge i.e., in the asymptotic limit this boils down to

$$\frac{l_{min}}{2} \gtrsim \delta n. \tag{2.70}$$

$\delta n$ is the total number of error bits. The limit for extracting secret keys after parameter estimation and error correction is basically given by Eq.(2.70). The above analysis is general method to find out the keys that are going for PA. For pure single photon source the key rate for finite size is given by

$$\frac{m+r}{l} \leq 1 - H(2\delta) - \tau \tag{2.71}$$

where, $m$ is the number of bits that one gets after contraction (privacy amplification), $r$ is the number of parity bits needed for error corrections, $l$ is the number of sifted bits after the protocol. $H$ is the binary entropy and $\delta$ is the errors in the key and the factor $\tau$ is fixed that comes from finite size effect of the key [72].

This key rate must be modified when someone uses realistic sources such as WCP or spontaneous parametric down conversion (SPDC) based source.

### Key Rate for BB84 protocol with Weak Coherent Pulse

Analysis for WCP source for extracting secret key in PA requires some basic formalism which is discussed below.

Let the total signals sent by Alice be $\mathscr{A} : \{1,2,....N\}$. The probabilities for corresponding state of the laser pulse - $p_1 \in \mathscr{S}$ is the single photon probability, $p_m \in \mathscr{M}$ is multi-photon probability and $p_v \in \mathscr{V}$ is the no photon (vacuum state) probability of a pulse. The set $\mathscr{A} = \mathscr{M} \cup \mathscr{S} \cup \mathscr{V}$ denotes the total signals sent. In the realistic source some multi-photon state may be known to Eve as she can do PNS attack [luth, sanders,rev. paper gisin] which might not show up in QBER. These states ($\Sigma$) form the subset of $\mathscr{A}$ ($\Sigma \subset \mathscr{A}$). It is assumed that all the multi-photons are not secure and Eve has every information of the polarization state sent through them. The lower bound of the number of bits in the sift key, which contains no multi-photon pulse ($\bar{\mathscr{M}}$) should come from the set $|E \cap \bar{\mathscr{M}}|$ (those photon pulses which go for error correction and do not contain any multi-photons).

The channel loss must not be too high, since distinguishing between the single photons and the multi-photons would be difficult (the portion of counts at the detector due to single photons must be greater than the channel loss) [81]. If this happens then Eve might send some of the photons with lossless channel to match with the total counts or received signals by Bob. Eve has

$$\eta^{(E)} > \eta^{(original)}, \tag{2.72}$$

i.e. the channel transmissivity for Eve ($\eta^{(E)}$) is much higher than the actual channel transmissivity ($\eta^{(original)}$) between Alice and Bob. This benefits Eve and in the worst case scenario she might block all the single photon pulses and sends only the multi-photon pulses to match the total counts at Bob's detector. The situation can be troublesome as Eve might have access to all the information about the key.

The key extraction during EC and PA will filter out the multi-photon contributions as they are vulnerable to PNS attack [48, 81]. Making the key private from Eve requires

to have the knowledge of upper bound of the multi-photons and lower bound of single photons. The minimum number of bits that contain only single photon signals is $\hat{l} = |E \cap \bar{\mathscr{M}}|$ and its associated RV is $L \in \{l_1, l_2, ..., l_n\}$. The minimum bits ($l_{min}$) generated in the sift key should be proportional to single photon signals

$$l_{min} = \left[\frac{1 - P_R}{2} - \hat{\tau}\right](n - M_{max}) \tag{2.73}$$

where, $n$ is the total signals sent. This is also proportional to the half of the total signals received, details for which can be found in [72]. We already know that for successful key extraction the signal rate should be greater than multi-photon rate ($M_{max}/N < r_{min}$) and there must be keys left after parameter estimation for key extraction ($\frac{1 - P_R}{2} - \hat{\tau} > 0$). For large number of received signals it is

$$\hat{l}_{min} \propto (n - M_{max}). \tag{2.74}$$

The joint probability that total counts at Bob exceed the predicted number of photons ($n > r_{min}N$) that are received through channel and the bits needed for key extraction is less than $l_{min}$ should be very less and becomes negligible for asymptotic limit [47].

$$P(l < l_{min} \cap n > r_{min}N) \leq e^{-2\tau^2(r_{min}N - M_{max})} + e^{-2\tau_M^2 N} \tag{2.75}$$

Equation (2.75) is defined as an extra security condition that needs to be fulfilled for WCP source. The important aspect of this equation is to fix mean photon number ($\mu$) for securing the key. The multi-photon signal rate ($M_{max}$) should be very less than the total signal rate ($r_{min}N$) received at Bob to make this probability ($P(l < l_{min} \cap n > r_{min}N)$) negligible. The probability also decreases for increase in number of received photons (i.e the channel must have low loss).

After fixing the mean photon number, now let us go for the key rate that can be securely extracted from the weak coherent pulses. As explained previously the equations for the key rate must be modified. Finding the bound for secret key after parameter estimation, the Eq.(2.71) is rewritten as

$$m+r \leq \hat{l}_{min}\left[1-H\left(\frac{(\delta+\tau_f)(1-P_R)n}{\hat{l}_{min}}\right)-\tau\right]. \tag{2.76}$$

In Eq.(2.76) $H$ is binary entropy for the single photon error contribution. $\tau$ is some fixed constant which is generally used for finite size effects of the key. $m$ is the number of bits left after the privacy amplification and $r$ is the parity bits needed for error correction.

In asymptotic limit i.e., for very large number of data received, the quantity $\hat{l}_{min}$ which is the minimum number of sift bits due to single photons can be approximated as

$$\hat{l}_{min} = l_s \sim \frac{(1-P_R)}{2}(n-M). \tag{2.77}$$

The acceptable error for all signals in the protocol for this limit also modifies to

$$(\delta+\tau_{ec})(1-P_R)|\Omega| \sim \delta(1-P_R)l. \tag{2.78}$$

Here, $|\Omega|$ is the total number of bits received by both Alice and Bob (sift bits left after parameter estimation). Maximum errors expected in the sift key for large number of detections is $\delta l$ that can be shown from Eq.(2.78). The parity bits required for error correction is $r$ that approximates to

$$r(\delta l, l) \sim lH(\delta). \tag{2.79}$$

The above expression signifies that for asymptotic limit, $\delta l$ errors can be corrected

with $r$ parity bits as derived from Shannon's limit [7, 47, 66]. It accounts for error corrections due to single and multi-photons. By, putting all the approximations in Eq.(2.77),Eq.(2.78) and Eq.(2.79) in Eq.(2.71) we get

$$m + lH(\delta) = \frac{1-P_R}{2}(n-M)\left[1 - H\left(\frac{\delta(1-P_R)n}{l_s}\right)\right], \tag{2.80}$$

plugging the value of $l_s$ and separately solving for second term inside the bracket of R.H.S in Eq.(2.80) we get

$$\begin{aligned} H\left[\frac{\delta(1-P_R)n}{l_s}\right] &= H\left[\frac{2\delta(1-P_R)n}{(1-P_R)(n-M)}\right] \\ &= H\left[\frac{2\delta(1-P_R)n/N}{(\frac{n}{N} - \frac{M}{N} - \frac{P_R n}{N} + \frac{P_R M}{N})}\right], \end{aligned} \tag{2.81}$$

$P_R$ is the probability by which Bob and Alice select the bits which will go for parameter estimation (PE). For large number of bits, $P_R \sim 0$ as the bits taken for parameter estimation is assumed to be very small compared to the bits going for EC and PA. This modifies the Eq.(2.81) to

$$\begin{aligned} &= H\left[\frac{2\delta n/N}{(\frac{n}{N} - \frac{M}{N})}\right] \\ &= H\left[\frac{2\delta p_D}{p_D(1 - \frac{p_M}{p_D})}\right] \end{aligned} \tag{2.82}$$

Where, $p_D$ is the probability of detection or the minimum signal detection rate which is $n/N$, $p_M = M/N$ is the multi-photon probability sent by the source. Now, again

putting the value of $H$ in Eq.(2.80) we get

$$\begin{aligned} m &= \frac{1}{2}(n-M)\left[1-H\left(\frac{2\delta}{(1-\frac{p_M}{p_D})}\right)\right]-lH(\delta) \\ \frac{m}{l} &= \frac{n}{2l}\left(1-\frac{p_M}{p_D}\right)\left[1-H\left(\frac{2\delta}{1-\frac{p_M}{p_D}}\right)\right]-H(\delta) \end{aligned} \tag{2.83}$$

Due to random basis selection, number of sift bits ($l$) is almost half of the total bits received ($n$) for asymptotic limit. The final secure key rate equation for weak coherent pulse (WCP) is written as

$$\frac{m}{l} = \left(1-\frac{p_M}{p_D}\right)\left[1-H\left(\frac{2\delta}{1-\frac{p_M}{p_D}}\right)\right]-H(\delta). \tag{2.84}$$

The major significance of the above equation is, it says that we can extract $m$ bit keys from $l$ bits of sift keys if we only consider the single photon detection. The first multiplicative term in Eq.(2.84) is the single photon fraction in a given signal.

Equation (2.84) gives the key rate for realistic source but assumes that the detectors are ideal. For realistic sources and detectors the above expression modifies to [GLLP].

$$\frac{m}{l} = \left(1-\frac{p_M}{p_D}\right)\left[1-H\left(\frac{\delta}{1-\frac{p_M}{p_D}}\right)\right]-H(\delta), \tag{2.85}$$

$m/l$ is called as the secure key rate $R$ of the protocol per channel use. The Eq.(2.85) differs as the argument inside $H_1$ is $\left(\delta/(1-\frac{p_M}{p_D})\right)$ instead of $\left(2\delta/(1-\frac{p_M}{p_D})\right)$ in Eq.(2.84). Equation (2.85) is used in almost all the experiments for calculating secure key rate in reality [16, 17]. The expression is mainly divided into two main parts, one contributions from single photon sates in the WCP and another error correction and PA due to leakage from multi-photons.

### 2.2.4 Increasing Key Rate with Decoy Pulses

In Eq.(2.85) $1-\frac{p_M}{p_D}$ is the contribution only due to single photons at the receiver. This can be called as the gain of single photons at the Bob's end that is

$$Q_1 = 1-\frac{p_M}{p_D}. \tag{2.86}$$

Here, $Q_1$ is the joint probability that given Alice sends single photon state and Bob detects that with 100% certainty. Similarly, the QBER due to single photons ($e_1$) can be written as

$$e_1 = \frac{\delta}{1-\frac{p_M}{p_D}}. \tag{2.87}$$

Rewriting the Eq.(2.85), the key rate $m/l$ for WCP with realistic error correcting efficiency is

$$R = Q_1[1-H(e_1)] - Q_\mu f(\delta)H(\delta). \tag{2.88}$$

Where, $f(\delta)$ denotes the error correction efficiency of the code that is used in the protocol that is generally $\geq 1$. This is used to cut out the additional information exchange during classical communication due to device imperfection.

It has already been seen that the QKD protocol will take place only if the channel loss is very low, otherwise the secure key rate will fall down drastically in lossy situation. For increasing the key rate Decoy state protocol is implemented that can be explained in the following steps [54, 56].

- Alice randomly inserts the decoy pulses in between signal photons. Decoy pulses are also WCP but does not contain any polarization information.
- It is assumed that Eve do not know about the time signature of Decoy pulses

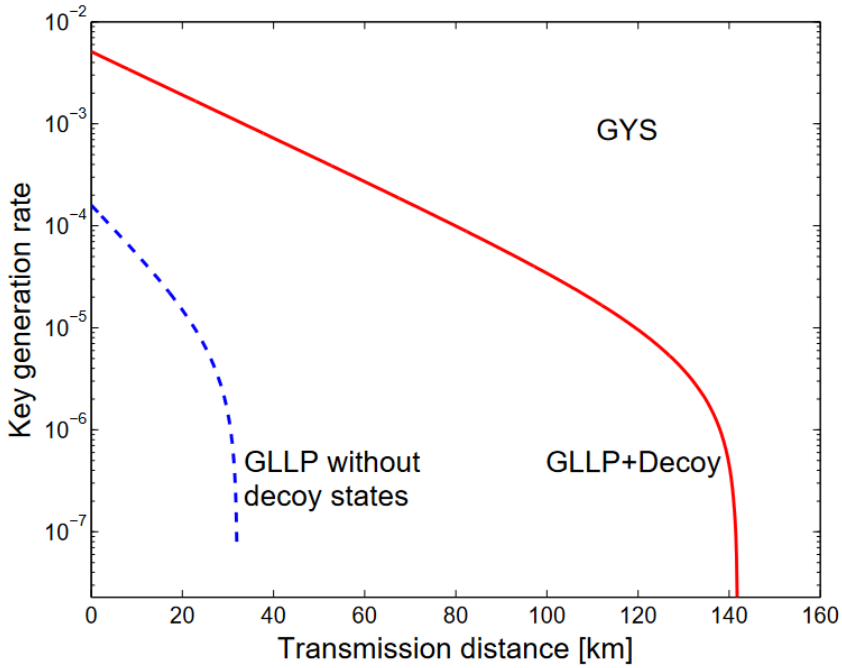



**Figure 2.10:** Key rate comparison between BB84 decoy state protocol (red) and GLLP protocol (dashed blue).[Hoi Kwong Lo, Xiongfeng Ma, and Kai Chen, *Phys.Rev.Lett.* ***94****, 230504(2005)*]

before hand.

- During sifting process, Alice intimates about the timing of decoy pulses she sent to Bob.

- Both Alice and Bob match the loss of signal photons and decoy photons they received. If both suffer different loss then, it is confirmed Eve used the channel and the protocol is aborted.

This inclusion of extra pulses (decoy) increases the key rate as the controlling factor $\mu$ of Eq.(2.88) also increases. Optimizing the key rate for specific channel transmissivity will give an upper bound on $\mu$. Plot shown in the Figure 2.10 indicates that decoy state increases $\mu$ which results into increase in the key rate greater than GLLP protocol.

## 2.3 Basic Security of BBM92 Protocol

From the expression of the key rate against individual attack the key rate for EB QKD follows from entanglement monogamy. For maximally entangled state shared between Alice and Bob the security can be given in terms of Bell's parameter [74]

$$S = 2\sqrt{2}(1-2\delta). \tag{2.89}$$

As, BBM92 protocol is just the entangled version of BB84 protocol so, key rate remains the same as for BB84. The error tolerance for BBM92 is same as BB84 against individual attacks [94] These rates are the basic rate for QKD protocols in ideal or near ideal conditions. Further we discuss how to improve the rate without adding any extra hardware. In realistic conditions several factors play role in decreasing the key rate of QKD protocol.

# Chapter 3

# Experimental Techniques for implementing QKD Protocols

Implementation any QKD protocol in practice can be quite tricky. Making an experimental setup working as close to the ideal one, can be challenging. It is known from the previous chapter (section 2.1) that to take complete benefit of any QKD protocol ideal sources and detectors are required.

Ideal single photon source (SPS) are still not realisable commercially [95] and lots of research is going in that area [96]. The available SPS are not efficient in producing on demand single photons [38, 96]. Currently, their emission rate is probabilistic and low that results in decreasing the key rate of the protocol. To circumvent this problem researchers have come up with the solution of using weak coherent pulses (WCP) or SPDC sources (heralded single photon source [97]). WCP are attenuated laser pulses that are assumed to take single photons in a given pulse. The laser pulses are attenuated to such a level that multi-photon probability is negligible. SPDC sources are also used

as heralded single photon sources, but the key rate produced by them is less compared to WCP. They are mainly used for entanglement based QKD (EB QKD). These source produce qubits in desired degree of freedom according to the protocol. These qubits are then sent through quantum channel which could be free space or fiber.

For achieving unconditional security [41, 64, 73] one needs ideal single photon detectors. Some of them are commercially available by companies like ID Quantique, Hamamatshu, etc. They are bulkier and be difficult to use in the field. Their photon number resolving power get easily saturated for more than $20-25$ incoming photons per unit time and can be used only in a very low background photon region such as dark rooms. Compared to this superconducting nanowire based single photon detectors (SNSPDs) are fast and highly efficient but requires bulkier setup for operation [98]. They are more like click detectors that gives a pulse on incoming photons (that can be one or many). Installing them requires big and heavy cooling systems as they work on the principle of superconductor. The most widely used single photon detectors are avalanche photon detectors (APDs), they have a compact form factor and are quiet efficient (not as good as SNSPDs). They are also click detectors (threshold detectors) and can be easily integrated in the setup for field experiments.

Using non ideal sources and detectors open several loopholes in the security of QKD protcol [99]. These can be dealt by proper calibration of the sources and detectors and other components used in the setup.

## 3.1 Preparation of Quantum States

### 3.1.1 Preparation of States for Prepare and Measure (P&M) Protocols

#### Random Number Generation through FPGA

States preparation involves generating the qubits in perfect polarization states for sending them to Bob. Field Programmable Gate Array (FPGA) can be used to drive laser diodes randomly for state preparation [100]. FPGA consists of a series of logic gates, flip flops, registers etc., which performs desired logical operations.

The most common method to generate random numbers using FPGA is through the Linear Feedback Shift Register (LFSR) technique [101]. Its is used to generate Pseudo Random sequence of bits (PRNG) though a series of shift registers and a fixed random seed. These shift registers are connected in series with a feedback [102, 103]. This feedback is taken from two or many (according to random bits generated) outputs and fed into the input (first register). The working principle of this is described in the following steps.

- At the rising edge of the clock, signal moves froward through the register from one bit to another (left to right), this process continues till it reaches end.
- Some outputs of shift registers are combined by XOR operation to form a feedback mechanism.
- The output of XOR gate is then fed into inputs for generating random pulse sequence with incoming input clock.

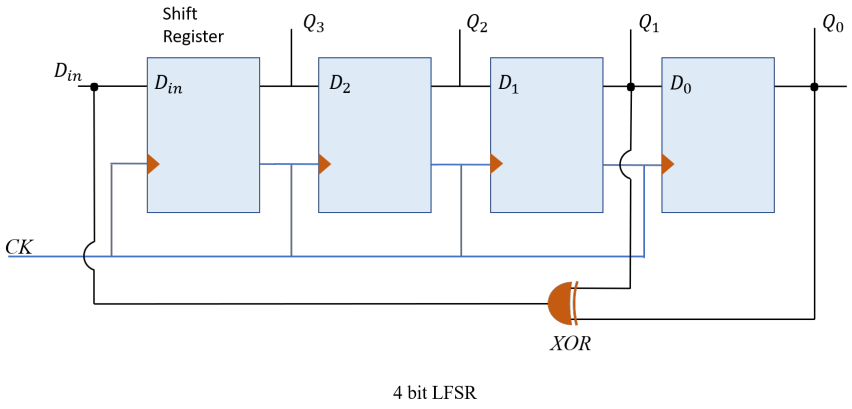


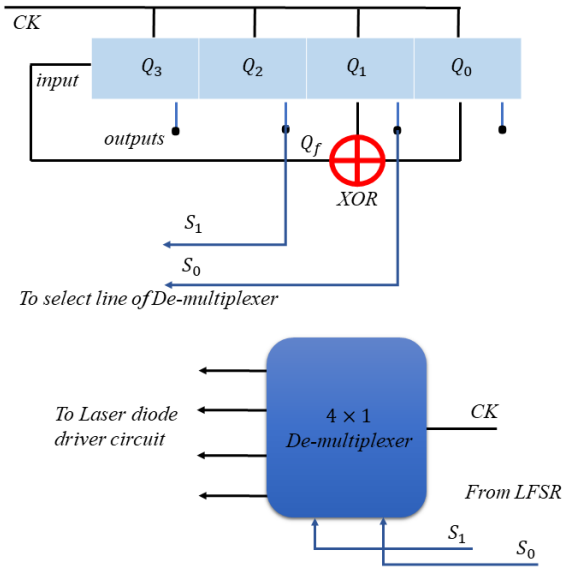

**Figure 3.1:** Schematics of 4 bit LFSR with sift registers. $D_{in}$ is the input and $CK$ is the clock and $Q_i$'s are the outputs of LFSR.

LFSR generates pseudo random pulses with a pre-defined state (seed) given to all the register at the first clock cycle (excepts for all 0$s$). The speed of pseudo random number generator (PRNG) depends upon the input clock frequency. Figure 3.1 and 3.2 show the schematics of LFSR with outputs fed into the multiplexer. In real scenario this inital seed can be changed frequently to increase the quality of randomness. Figure 3.3 shows the random driving of laser pulses.

### Preparation of Four Polarization States with Laser Diode Driver Circuit

We take the output random sequence through the FPGA and feed them into the driver circuit for switching of laser diodes. For operating the laser diodes in pulsed mode with short pulse width requires an extra electronic circuit [104]. Figure 3.4 gives a detailed circuit diagram of the laser diode driver. Picture of the circuit that is being used in the experiment is shown in Figure 3.5.

One input of this circuit is taken from FPGA and other from constant power supply. The advantage of this circuit is that the pulse width is narrow ($\sim$ 900 $ps$ shown in Figure 3.6) and it works for any laser diodes [105]. It is easy to implement in the field




*Output table of LFSR*

| $Q_3$ | $Q_2$ | $Q_1$ | $Q_0$ | $Q_f$ |
|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 0 |
| 0 | 1 | 1 | 1 | 0 |
| 0 | 0 | 1 | 1 | 0 |
| 0 | 0 | 0 | 1 | 1 |
| 1 | 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 | 1 |
| 1 | 1 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 | 1 |
| 1 | 0 | 1 | 1 | 0 |
| 0 | 1 | 0 | 1 | 1 |
| 1 | 0 | 1 | 0 | 1 |
| 1 | 1 | 0 | 1 | 1 |
| 1 | 1 | 1 | 0 | 1 |
| 1 | 1 | 1 | 1 | 0 |

**Figure 3.2:** Schematic representation of Random sequence fed into driving circuit. In the figure the outputs $Q_1$ and $Q_0$ are $XOR$ed as a feed back $Q_f$ and fed into input. The outputs $Q_2$ and $Q_3$ served as random sequence that is fed into the select line of the De-multiplexer for laser operation. In actual experiment 16 bit LFSR is used.

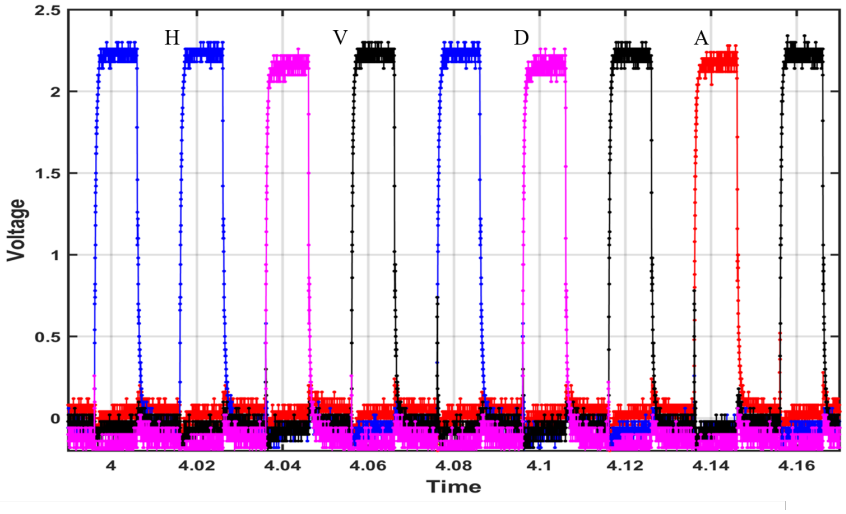



**Figure 3.3:** Output random pulse through FPGA going to the driving circuit.

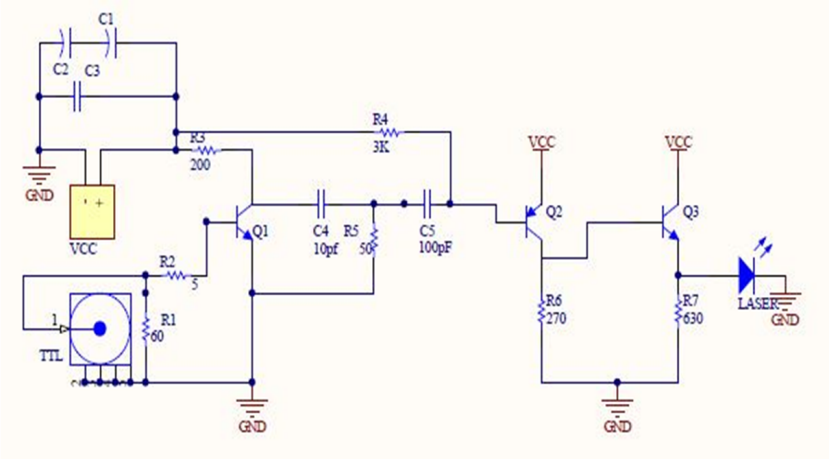



**Figure 3.4:** Circuit diagram of the Laser driver circuit used for generating 4 polarization states. Q1 and Q3 are n-p-n transistor and Q2 is p-n-p type transistor with high frequency response ($\sim$ GHz). VCC is taken to be maximum 8 Volts (DC) and the TTL signal's peak to peak voltage is greater than 2 Volts.

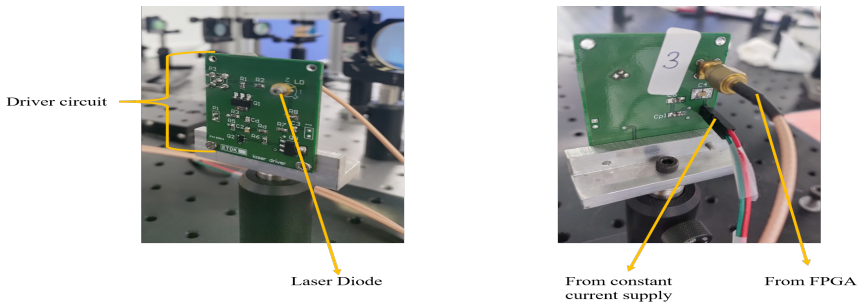



**Figure 3.5:** Pictorial representation of Laser diode driver circuit used in the QKD experiment.

experiments and comparatively cost effective (Figure 3.5).

### Making Optical Multiplexer

Once we get the outputs from the laser diodes next tasks is to assign polarizations to each of them. This is done by either fixing polarizers before them or placing the combinations of Polarizing Beam Splitters (PBS) followed by Half Wave Plates (HWP) as illustrated in Figure 3.7. All the four polarization states must overlap on a single path before departing to Bob. This is done so that Eve must not be able to distinguish the

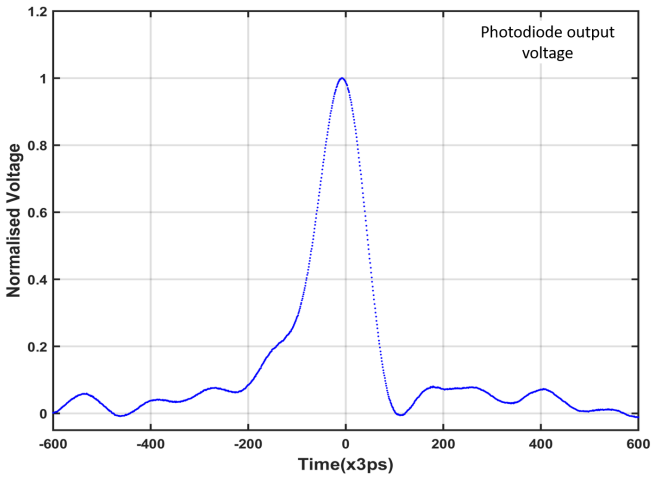



**Figure 3.6:** Optical pulse output from the laser that is measured from photo detector and recorded in oscilloscope.

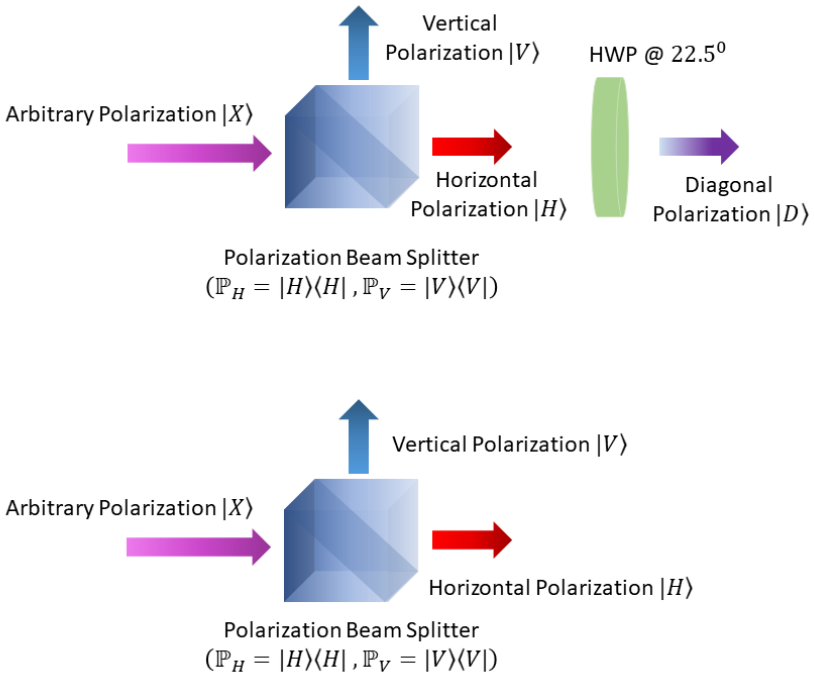



**Figure 3.7:** Change of polarization state with linear optical components. First diagram shows how the arbitrary polarization can be converted into diagonal polarization. Second diagram shows getting horizontal or vertical polarization by operating arbitrary polarization with PBS

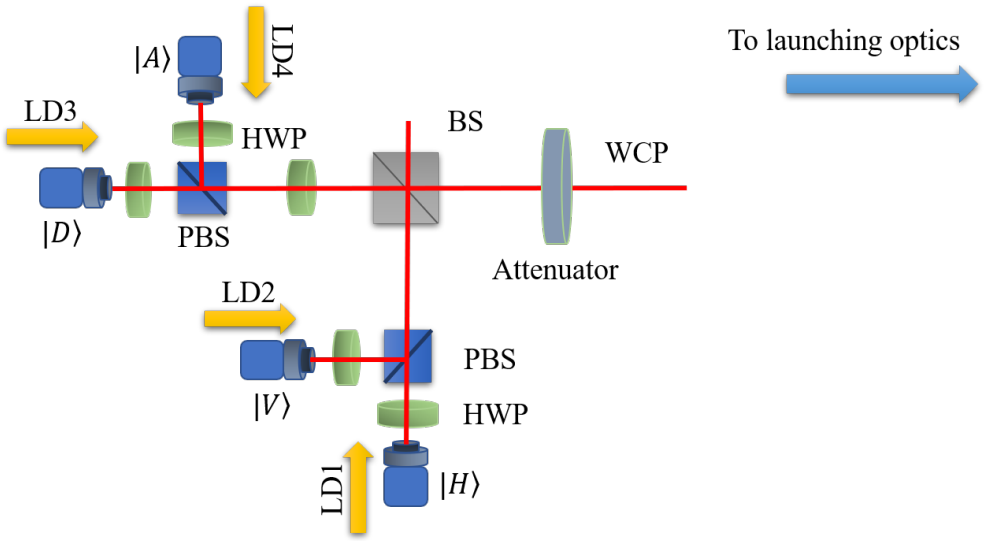



**Figure 3.8:** Schematics of optical multiplexer. Photons from all the four laser diodes are combined with the help of PBS and BS then it is attenuated to send them to Bob.

states based on their spatial separation [105, 106]. There are various ways of combining (multiplexing) the polarization states [60, 107]. Optically, we used combinations of PBS and BS for this purpose which is described in Figure 3.8. After combining to single path they are injected into a small patch of single mode fiber to clean modes. For getting qubits through weak coherent pulse, the laser intensity is attenuated. The attenuated laser beam is classical in nature [65, 108], but the multi-photon probability in the pulses remains very less. This is ensured by putting a variable optical attenuator then a power meter or photon counter after that. We vary optical attenuator such that on an average less than one photon per pulse is recorded at the Single Photon Counting Module (SPCM) shown in Figure 3.9. From this measurement mean photon number ($\mu$) is fixed for safe operation of the protocol [109]. Fixing actual $\mu$ from the counts is

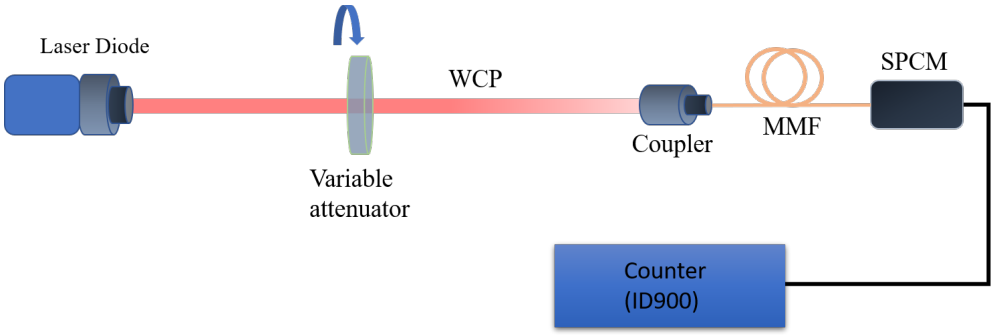



**Figure 3.9:** Schematic representation for calculating the mean photon number ($\mu$).

given by

$$\begin{aligned}\mu &= \frac{\text{Photon counts}}{\text{Pulses sent} \times \text{detector efficiency} \times \text{coupler efficiency}} \\ &= \frac{N}{\nu_{rep} \times \eta_{det} \times \eta_{cup}}\end{aligned} \tag{3.1}$$

The above formula is valid for very lower values of $\mu(\leq 0.4)$. An accurate characterization for higher values of $\mu$ requires more number of detectors [110]. Ascertaining

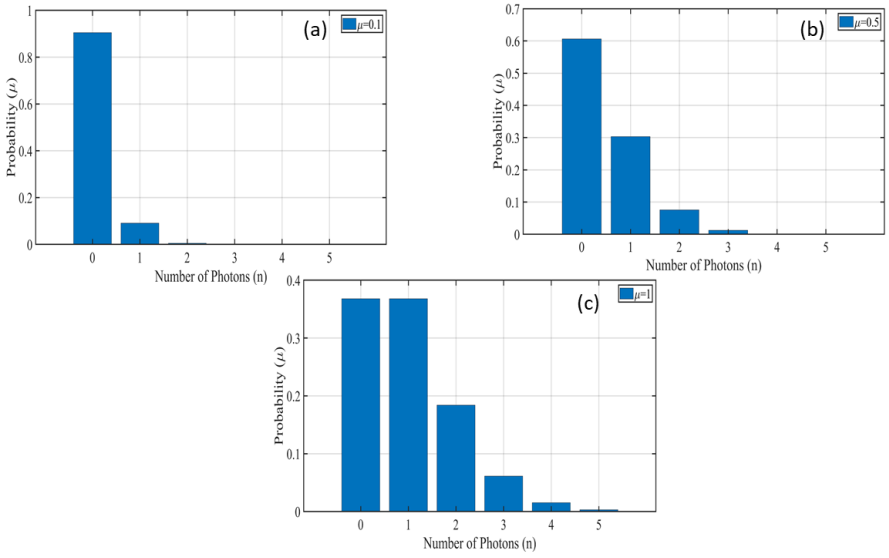



**Figure 3.10:** Photon number probabilities for different values of $\mu$. Graph represents different photon occurring probabilities for different $\mu$ ($\mu = 0.1$(a),$\mu = 0.5$(b),$\mu = 1.0$(c)).

the exact number of photons per pulse without using number resolving detector is not

possible. However, for performing QKD using WCP one needs to measure the average number of photons per pulse ($\mu$). This is done by recording the photon counts per unit time and dividing it with the frequency of the laser pulses (repetition rate). Plots in Figure 3.10 shows the multi-photon probabilities for various $\mu$. Now, the states are ready to be sent to Bob for key distribution protocol (BB84 protocol).

### 3.1.2 Preparation of States for EB Protocols

Preparing states for EB QKD requires non linear process called spontaneous parametric down conversion (SPDC) [111–113]. This simultaneously destroys one incident photon (pump photon) and creates a pair of photons such that the total energy and momentum of the system remains conserved. Thus one can get two entangled photons from a single incoming photon of the laser. It is due to the interaction of the photon with the vacuum fluctuations inside the medium that spontaneously splits it into two correlated photons [108, 111, 114]. The second order contribution to the energy is given by [111]

$$\mathscr{H} = \int_{\mathscr{V}} \mathbf{P}^{(2)}(\mathbf{r},t) \cdot \mathbf{E}(\mathbf{r},t)\, d^3r$$

$$\mathscr{H} = \varepsilon_0 \int_{\mathscr{V}} \chi^{(2)} \mathbf{E}^2(\mathbf{r},t) \cdot \mathbf{E}(\mathbf{r},t)\, d^3r. \tag{3.2}$$

Where $\mathscr{V}$ is the volume of the non-linear medium. This is the general expression for contribution to the total energy due to second-order non-linear optical effects. However, in parametric down conversion, the above expression for the total energy takes the following form; writing the fields in form of operators [111, 115]

$$\mathscr{H} = \varepsilon_0 \int_{\mathscr{V}} \chi^{(2)} \widehat{E}_P(\mathbf{r},t) \widehat{E}_S(\mathbf{r},t) \widehat{E}_i(\mathbf{r},t)\, d^3r. \tag{3.3}$$

For every hermitian operator we can write

$$\widehat{E}_P(\mathbf{r},t) = \widehat{E}_P^{+}(\mathbf{r},t) + \widehat{E}_P^{-}(\mathbf{r},t)$$

Then the interaction Hamiltonian for SPDC is given by

$$\mathscr{H} = \varepsilon_0 \int_L \chi^{(2)} \widehat{E}_P^{+}(z,t)\widehat{E}_S^{-}(z,t)\widehat{E}_i^{-}(z,t)\, dz. \tag{3.4}$$

We have considered the length of crystal very small compared to its transverse dimension so the integration will be mainly on z (propagation direction). One more reason to consider this, as in most of the experiments, the beam waist of the pump photon is much smaller in size compared to the cross section of the crystal (Figure 3.11). The state of the two photons output can then be written with the help of Schrodinger's equation.

$$|\Psi(t)\rangle^{tp} = exp\left[\frac{-i}{\hbar}\int \mathscr{H}(t')dt'\right]|\Psi(0)\rangle^{tp}$$

The initial state is the vacuum state. Writing the fields in terms of their Fourier sum and putting them into Schrodinger's equation we get the two photon state as

$$|\Psi\rangle^{tp} = \int\int_0^{\infty} d\omega_S d\omega_i V(\omega_S+\omega_i)\Phi(\omega_S,\omega_i)e^{i(\omega_S+\omega_i)t}|\omega_S\rangle|\omega_i\rangle \tag{3.5}$$

Where $V(\omega_P = \omega_S + \omega_i)$ is the amplitude of the pump beam and $\Phi(\omega_S,\omega_i)$ is the phase matching function which takes care of the conservation of energy and momentum [115].

$$|\Phi(\omega_S,\omega_i)\rangle = \int_{-L}^{0} dz\, e^{i[k_{Pz}(\omega_P)-k_{Sz}(\omega_S)-k_{iz}(\omega_i)]z}$$

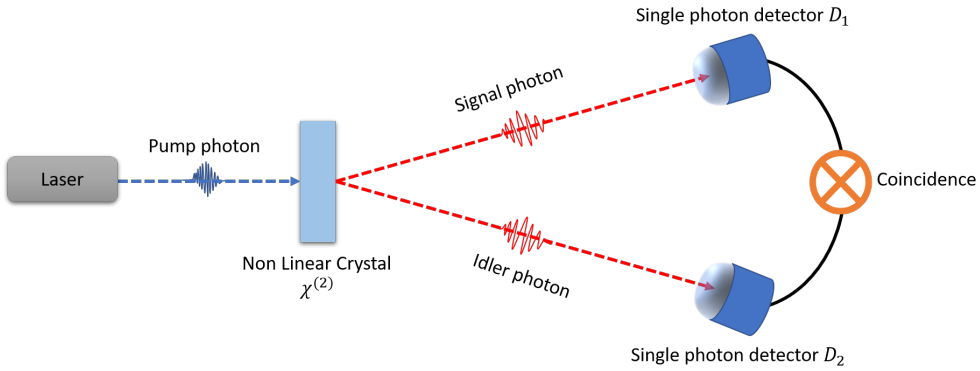



**Figure 3.11:** Experimental schematics of spontaneous parametric down-conversion.

From this we can get the energy and momentum conservation as [108, 114]

$$\omega_P = \omega_S + \omega_i \tag{3.6}$$

$$\mathbf{k}_P = \mathbf{k}_S + \mathbf{k}_i + \Delta k \tag{3.7}$$

where $\Delta k$ is the phase mismatch. For perfect phase matching and maximum output $\Delta k = 0$. The above expression (3.5) approximates as

$$|\psi\rangle \propto \int |\omega_s\rangle|\omega_i\rangle d\{\omega\} \tag{3.8}$$

where $\omega_s$ and $\omega_i$ are the frequency of signal and idler. For discrete variables such as spin, polarization etc., Eq.(3.8) can be modified as

$$|\psi\rangle \propto \sum C_{ij}|s_i\rangle|s_j\rangle \tag{3.9}$$

where $s_i$ and $s_j$ are the spins states and $C_{ij}$ are complex amplitudes. Based on what type of entanglement we want there are Type-0, Type-1 and Type-2 phase matching in SPDC [108].

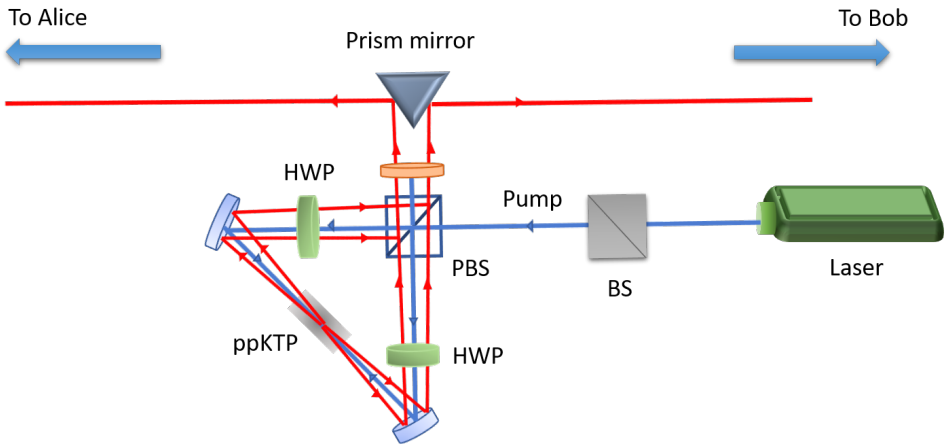



**Figure 3.12:** Schematics of entangled photon source generation using sgnac interferometer for quantum key distribution.

Using this one can generate various kinds of Bell states in polarization/OAM degrees of freedom. For the time being we take the example of polarization entanglement which uses the Bell state [116, 117]

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|HH\rangle + |VV\rangle\right) \tag{3.10}$$

for QKD as shown in Figure 3.12. These states can be combined to the launching optics and can be sent to Alice and Bob separately for key distribution.

## 3.2 Sending of States Through Quantum Channel

A quantum channel can be any communication link which preserves the "trace norm" (i.e. trace of density matrix of states) of the quantum state [11, 16]. For sending qubits in polarization degree of freedom, one can use free space or polarization maintaining optical fibre as a quantum channel. It preserves the state as it was at the beginning [118]. We have used free space as a quantum channel for sending qubits. For long distance or satellite communication it is the best way to establish link between communicating parties. Before sending qubits to free space, launching the optics is required to effectively send them to Bob.

### 3.2.1 Launching and Receiving Optics

Launching optics generally consists of two lens combination with different focal length $f_1$ and $f_2$. Usually $f_2 > f_1$ such that the beam size should not exceed the lens diam-

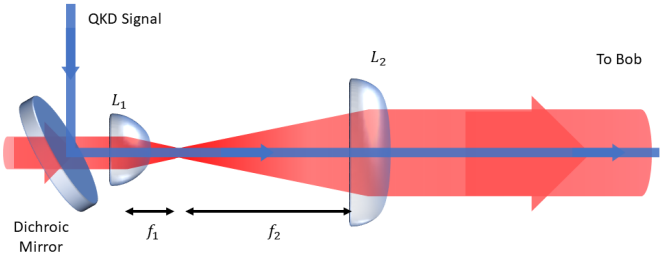



**Figure 3.13:** Schematics of launching optics.

eter or aperture size of the second one. This beam expanding configuration is used because as the beam size increases, its divergence is reduced ($w_0 = 1/\theta$) [119, 120].

This increases the amount of signal received at the Bob's end. Figure 3.13 shows the schematics of launching optics. For much longer distances, proper telescopes must be used. The beacon beam from another laser is mixed with the QKD signal and sent through this launching optics. Receiving optics as shown in Figure 3.14 is similar to the launching one just that the lenses are kept in reverse way. Short focal length lens

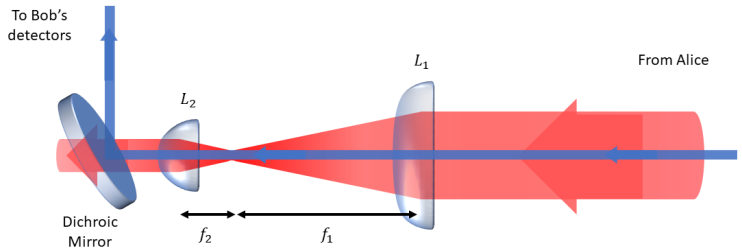



**Figure 3.14:** Schematics of collecting optics.

before Bob's detection setup makes the beam converge on to the detectors.

## 3.3 Detection of Quantum States

Measurement operations for P&M and EB QKD protocols remains the same. This is because the detection mechanism for the polarization states is a standard procedure in quantum optics [11, 108].

### 3.3.1 Projective Measurement

The projective measurement on the qubits for polarization degree of freedom is done with the combination of PBS and half wave plate (HWP) followed by SPCMs [121].

Bob's detection setup consists of a 50-50 BS which acts a passive basis selector, that randomly projects the state onto $\{H,V\}$ or $\{D,A\}$ basis. Figure 3.15 shows the action of single photon on a 50-50 beam splitter is just like QRNG [122]. Here due to device

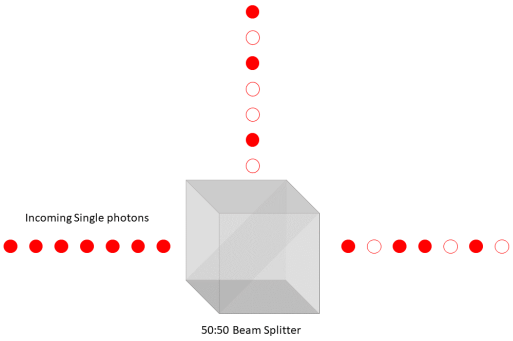



**Figure 3.15:** Single photons incident on 50:50 beam splitter (BS) (optical QRNG).

imperfection, the BS might not be completely 50-50, which might change the number of detections in $\{H,V\}$ and $\{D,A\}$ basis. WCP may contain multi-photons which also might contribute to error that leads to coincidences. For pre-checking one must get equal number of photon counts on the detector on either side of the beam splitter. Then measuring the state in $\{H,V\}$ or $\{D,A\}$ basis is done by keeping a PBS (for $\{H,V\}$) or PBS and HWP (for $\{D,A\}$). This collapses the state into one of the eigenstates of the projection operator in a given basis. The photon number received on either side of the PBS is recorded by single photon counting modules (SPCM). SPCMs consists of APD (Avalanche photo-diode) with pulse shaping and quenching electronic circuit. APD works on the principle of reverse bias voltage breakdown [123–125]. These are special photodiodes which produces more electron hole pairs for conduction with just single incident photons. They are heavily doped PiN photodetectors [125] which helps in multiplying the electron hole pair once they are generated through incoming photon. Figure 3.16 shows the basic diagram of APD. In this figure we see that there is a strong electric field in the heavily doped region which causes the avalanche effect. Electron hole pairs generated from the incoming photons in the "i" (intrinsic region)

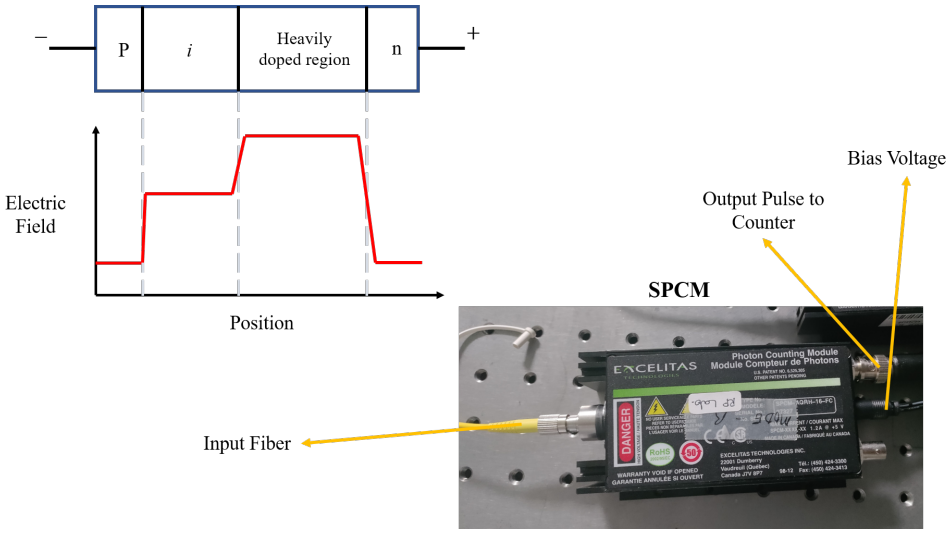



**Figure 3.16:** Electric field at the junction of the APD. SPCM used in the experiment

region (Figure 3.16) travels to their respective poles in the diode. While entering in the heavily doped region they collide with the atoms to give more free electrons, due to this impact ionisation, cascading effect is generated which leads to huge flow of electron hole pairs through the diode. This results in producing large amount of photo-current due to single photon incidence that can be measured [125]. This can be seen in equation as

$$I_d = M \times R_d \times P_{opt}, \tag{3.11}$$

where $I_d$ is the photo-current, $M$ is the multiplicative factor ($\sim 10^3$), $R_d$ is the responsivity of the detector and $P_{opt}$ is the optical power from the source. The current pulse is further fed into pulse shaping electronics and then to quenching circuit. Quenching is done to quickly bring the diode back to breakdown region from saturation region so that it is ready to detect another photon. This is done to improve the response time of the detector (maximum number of photons it can count per unit time). All these together form a SPCM which can be seen in Figure 3.16. The recorded pulses are integrated over time with the help of analogue to digital converter (ADC), to give the number of photons incident on the detector. Photon counts and their arrival times are

recorded on timing electronics that is discussed in the next section. For both P&M, and EB type of QKD protocols this detection method remains the same.

## 3.4 Post-processing the Data

The post processing of data is done through classical algorithms and involves a number of steps. It is a tricky task for any QKD protocol.

### 3.4.1 Collecting the Time-stamps

Sifting procedure requires that the photon arrival time and the time when they are launched must be known. For this Alice and Bob must synchronize with each other in order to correctly extract the signal data out of time stamps. The device that we have used for recording the time stamps is IDquantique-ID900. The task here needs to be addressed is the photons that Bob detects, were actually sent by Alice in a sequential manner. This requires to have the time signature at both ends. On the Alice side the pulses generated by FPGA are fed into ID900 to record time, as shown in Figure 3.17. Alice and Bob must know the time delay (can be calculated from the separation distance) between themselves. After quantum exchange, this delay helps Bob to locate the photons sent by Alice by analysing their timestamps. This is represented by Eq.(3.12)

$$t_B = t_A + \Delta \pm \delta_t, \tag{3.12}$$

where, $t_B$ $(t_A)$ is timestamp of Bob (Alice), $\Delta$ is the delay between them and $\delta_t$ is the time window. For this process to occur both the clocks of Alice and Bob must be synced (i.e., their clocks must start recording the timestamps at the same time). In the lab we first synchronize the two IDQs via 10 MHz sync-out. Then we take a pulse from one time controller (ID900) which will trigger the measurement process in

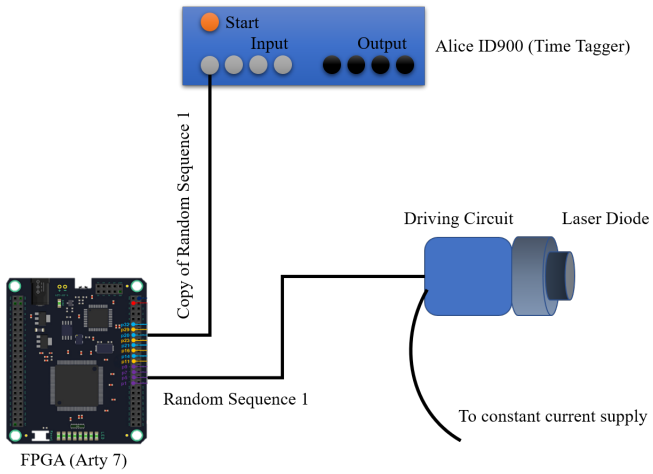



**Figure 3.17:** Time information recording at Alice's side which later be used for basis matching.

both of the time taggers to start the count. For free space QKD in the field, timing electronics of Alice and Bob are synchronized through WiFi attached with them or through RF communication. The triggering can be done by pulsed beacon laser that is being sent from Alice to Bob to their respective time taggers through photodetector outputs. The schematics of the time synchronization setup for lab is shown in Figure 3.18. This process makes both the clocks start at same time, which is crucial for BB84 protocol. For entanglement based protocol, time-stamps recorded at both ends should be matched for coincidences.

$$\begin{aligned} t_A &= \Delta_A \pm \delta_{tA} \\ t_B &= \Delta_B \pm \delta_{tB}, \end{aligned} \tag{3.13}$$

Some of the photons which get lost in the channel might not ultimately show up to Bob.

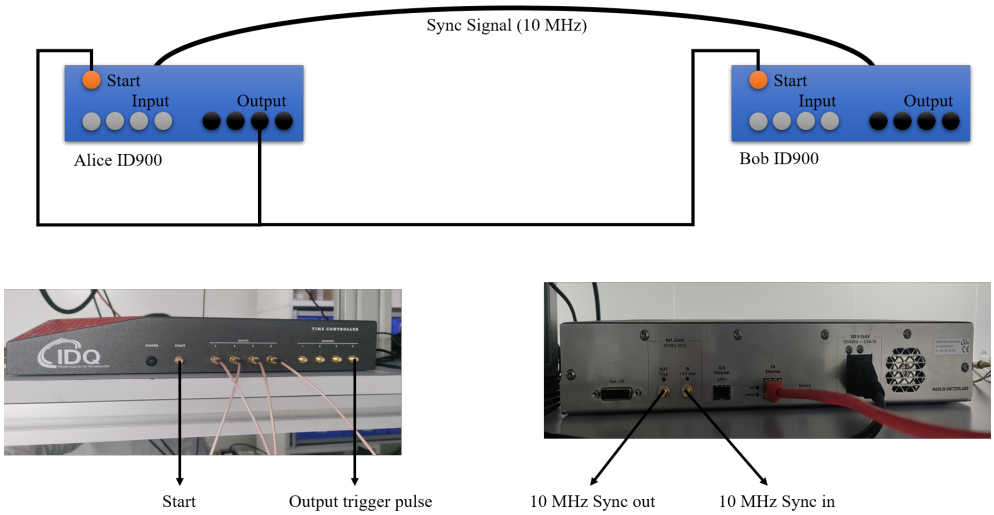



**Figure 3.18:** Device synchronization between two ID900 with starting trigger pulse at Alice's ID900.

### 3.4.2 Temporal Filtering

For distinguishing signal photons from noise, proper filtering mechanisms are required. Already we have screened-out background photons using band-pass filter at the detection end. This process of spectral filtering allows only the signal photons of specific wavelength to enter into the detectors [126]. In similar way temporal filtering filters out the photons which are outside the time window to increase the signal to noise ratio (i.e., one needs to choose $\delta_t$ such that SNR is maximum), as shown in Figure 3.19. The SNR is

$$SNR = \frac{1}{N_t} \underset{\delta_t}{max} \left( N_{sig}(\delta_t) \right). \tag{3.14}$$

Here, $N_{sig}(\delta_t)$ and $N_t$ are the signal and total counts at the detector. The signals can then be analysed for rest of the process. Signal with proper temporal windows and delay is integrated for sometime to give the estimation of the number of photons received. As we are using BS, from the total counts almost 50% of them will contribute to sift key

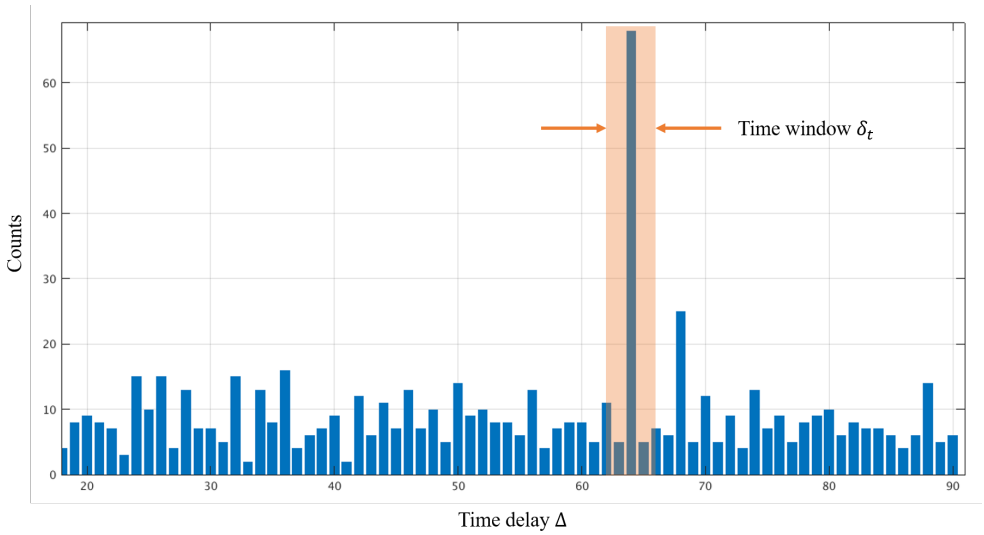



**Figure 3.19:** Choosing optimum time window for signal detection.

(BB84 protocol).

$$\begin{aligned} R_{raw} &= \frac{(N_H + N_V + N_D + N_A)}{T\,(\text{integration time})} \\ &= \frac{N_T}{T} \end{aligned} \tag{3.15}$$

Here, $N_T$ is the total signal counts in the detectors taken over time $T$. Estimation for sift key due to $50:50$ BS configuration gives [16]

$$R_{sift} = \frac{1}{2} R_{raw} \tag{3.16}$$

Exact basis matching can be done by TCP/IP protocol through public channel (ethernet cable). Quantum bit error rate (QBER) is calculated from the small portion of sift key. QBER is the fraction of photons detected wrongly in compatible basis.

$$\begin{aligned} QBER_H = \delta_H &= \frac{N_H^{wrong}}{N_H^{wrong} + N_H^{correct}} \\ &= \frac{N_H^{wrong}}{N_H^{total}} \end{aligned} \tag{3.17}$$

Where, $N_H^{wrong}$ is the counts in the wrong detector ($V$) for $H$ polarised photons and $N_H^{correct}$ is the counts in the right detector. Finding average QBER for all polarizations will tell us whether to proceed with the protocol or not. After parameter estimations, EC and PA are the main process which makes the key identical and secret.

### 3.4.3 Error Correction

In classical communication error correction codes are used to remove error caused by channel noise. This is done by adding extra bits in message also known as parity bits ($r$). For generating error correction codes generator matrix ($G$) is used at transmitter and parity check matrix ($F$) is used to calculate syndrome for decoding at the receiver. In QKD decoding operation is performed at only one of the nodes (Alice or Bob). Unlike classical communication only syndrome is transferred from Alice to Bob or vice versa. Based on syndrome the keys are modified and at the final stage keys at both nodes become equal. If the QBER is less than the threshold (set according to the protocol) in parameter estimation (PE), rest of the keys go for error correction. This makes both Alice or Bob's keys identical to each other. This error correction process can be done either considering Alice's bits to be correct or Bob's bits to be correct as shown in the schematics in Figure 3.20.

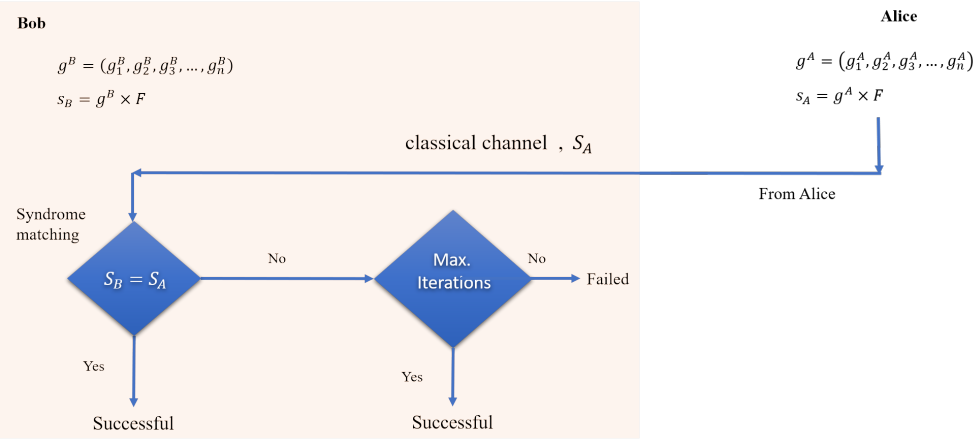



**Figure 3.20:** Error correction via syndrome matching between Alice and Bob. Alice sends his syndrome through classical channel for error correction.

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

$$\begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_r \end{bmatrix}_{r\times 1} = \begin{bmatrix} F_{11} & F_{12} & \cdots & F_{1l} \\ F_{21} & F_{22} & \cdots & F_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ F_{r1} & F_{r2} & \cdots & F_{rl} \end{bmatrix}_{r\times l} \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_l \end{bmatrix}_{l\times 1} \tag{3.18}$$

Equation (3.18) denotes the basic operation for finding syndrome. After multiplication with sift key this results in syndrome $[s]_r$ that is sent over public channel to Bob. Bob matches these blocks of syndrome with his ones for detecting the errors. The syndrome which does not matches are then corrected by maximum likely-hood technique [91]. There are several kinds of error correcting algorithms eg. parity checks, Hamming code, Low Density Parity Check (LDPC) [79, 127]. The common error correcting technique used in QKD is LDPC which is efficient and easy to implement in the system.

### 3.4.4 Privacy Amplification

Privacy amplification (PA) eliminates the leaked information by distilling the final secret key from a long-secret random sequence with a universal hash function. By addressing privacy amplification (using hash function) along with error correction (through LDPC or random codes) one can minimise Eve's information about the key which becomes negligibly small for asymptotic limit. This is done by choosing a hash function over the public channel. Alice and Bob make this choice only after the quantum exchange or else the Eve can decide her attack strategy [92, 128]. There are several hash functions for doing privacy amplification. One of the function is Toeplitz hashing, a 2-universal hash functions that is used to improve the quality of the randomness [129]. It requires completely random initial seed (which can be taken from the output of QRNG). By 2- universality of the hash function, means that if one considers the inputs $a_1$ and $a_2$ into a black box of randomness extractors or hash function with outputs $b_1$ and $b_2$, then the pairs $(a_1, b_1)$ and $(a_2, b_2)$ are pairwise independent. In other words, the probability of occurrence of each such pair must be lower than $1/|\mathscr{B}|^2$, where $|\mathscr{B}|$ is the length of the output bit string. The hashing of the error corrected bit string can be given by [130]

$$\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{bmatrix}_{m\times 1} = \begin{bmatrix} h_1 & 0 & \cdots & 0 & 0 \\ h_2 & h_1 & \cdots & 0 & 0 \\ h_3 & h_2 & \cdots & 0 & 0 \\ \vdots & h_3 & \cdots & h_1 & 0 \\ h_{m-1} & \vdots & \cdots & h_2 & h_1 \\ h_m & h_{m-1} & \cdots & \vdots & h_2 \\ 0 & h_m & \cdots & h_{m-2} & \vdots \\ 0 & 0 & \cdots & h_{m-1} & h_{m-1} \\ 0 & 0 & \vdots & \cdots & h_m \end{bmatrix}_{m\times l} \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_l \end{bmatrix}_{l\times 1} \tag{3.19}$$

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

$$m = l - t - s, \tag{3.20}$$

here $l$ is the error corrected sift bits, $t$ is the amount of knowledge exchanged between Alice and Bob to correct the error due to all possible reasons. Exchanging syndromes in error correction might leak some information to Eve that's why it is subtracted. Security parameter $s$ can be chosen according to the key one needs to compress in PA [128]. This parameter also depends on amount of bits sacrificed due to information exchange in EC. To check the quality of PA one can use randomness test suites, NIST, DieHarder, ENT etc. To finally test that the keys are identical, Alice encrypts a short message with the generated key for Bob to check weather he can decrypt or not.

## 3.5 Result for Field Demonstration of BB84 Protocol

We have demonstrated the BB84 QKD protocol over 200 meters of free space channel at night time over the terrace of PRL Ahmedabad as shown in Figure 3.21. The picture of basic transmitter (Alice) and receiver (Bob) is shown in Figure 3.22(a)

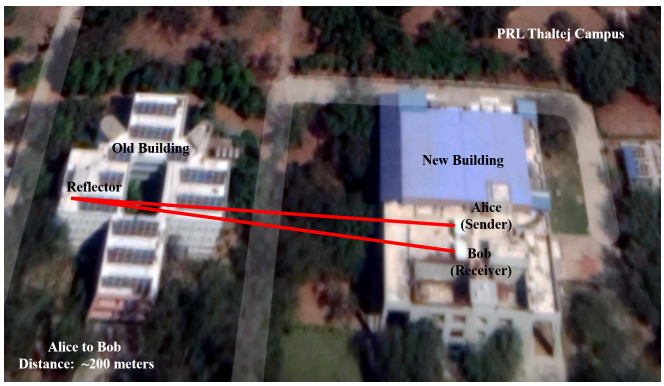



**Figure 3.21:** Overview of the free space QKD channel for BB84 protocol.

and 3.22(b). The schematics of the experiment is shown in the Figure 3.23.

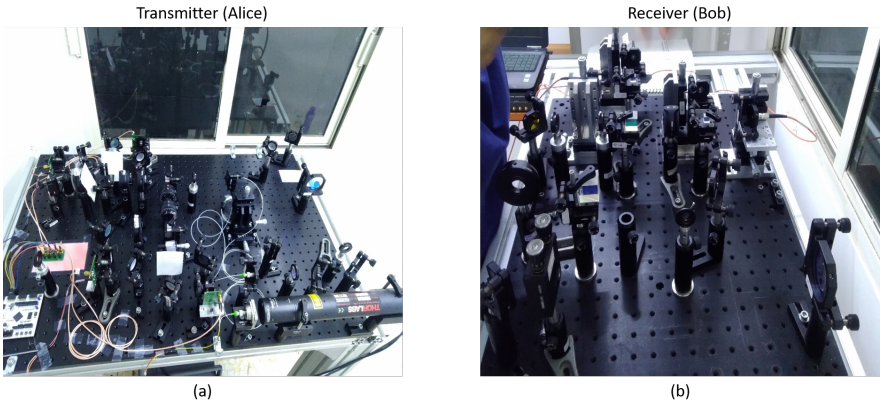



**Figure 3.22:** Picture of optical setup for QKD transmitter and receiver.(a) shows the optical setup of Alice, (b) shows the optical setup of Bob.

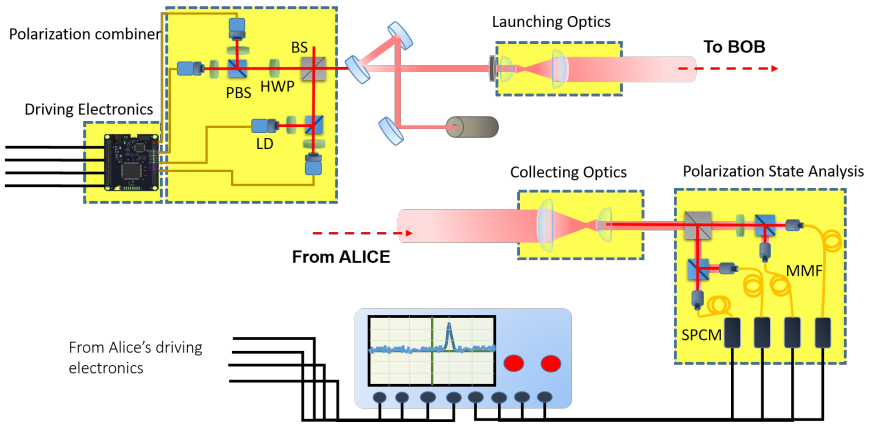



**Figure 3.23:** Schematics showing the optical setup for BB84 protocol. Alice's setup consists of optical multiplexer and beacon laser that is used for alignment. Bob's setup contains collecting optics with typical polarization analysis setup for state measurements after random selection through 50 : 50 BS.

### 3.5.1 Parameter Estimation of BB84 Protocol

The free space channel transmissivity ($\eta_{ch}$) is 70%, the overall detector efficiency including the fiber coupling efficiency is 40%. The mean photon number ($\mu$) is taken to be 0.3 with the repetition rate of 5MHz from the source. The sift key rate can be

calculated form the Table 3.1 The total sift key rate is calculated by multiplying the

Table 3.1: Showing QBER and key rate for some sets taken at random from detections of every 10 milliseconds.

| Set No. | Transmitted ($R_T$) | Detections ($R_D$) | Sift Bits ($R_D$) | Error Bits ($E_B$) | QBER (%) ($E_B/R_{sif}$) |
|---|---|---|---|---|---|
| 1 | 50462 | 6056 | 2154 | 62 | 2.8 |
| 2 | 50518 | 5656 | 1936 | 65 | 3.3 |
| 3 | 50546 | 5268 | 1894 | 44 | 2.2 |

sift bits with 100 (as the integration time is 10 milliseconds). The sift key rate comes out to be $\sim 200$ **Kbps** with QBER of $\sim 4\%$.

# Chapter 4

# Characterization for Information Leakage of BB84 Source

## 4.1 Background on QKD Source Implementation

The first QKD protocol was proposed by Bennett and Brassard in 1984 [23] and referred as the BB84 protocol. In this protocol, the secret key bits are encoded in the quantum states, for example, polarization of a single photon. The states to be sent are prepared in mutually unbiased bases (MUB).The intrinsic uncertainty in measurement of polarization in randomly selected MUB [18, 23, 24] makes this protocol secure in principle. There are QKD protocols, other than BB84, which use degree of freedom different from polarization. For example COW (Coherent One Way), SARG04 use phase instead of polarization to encode the states [51, 131]. These protocols lag behind on efficiency and easiness relative to BB84 in terms of practical implementation. All these protocols use various devices which are not perfect in reality and can be prone to attacks [64, 132–135]. To reduce the vulnerabilities in the QKD protocols due

to imperfect measurement devices, MDI (Measurement Device Independent) QKD schemes have been devised [57, 136–139], however, their implementations are much more difficult in practice. On the other hand BB84 has solid theoretical security backup [37, 83] against a wide range of attacks and widespread demonstrations around the world, which makes it a preferred protocol to apply in practice.

Even though there are several security proofs based on the attack strategies of Eve but most of them assume the devices and the optical elements used in the QKD setup to be ideal. There is a possibility that Eve might know the weakness of these devices and can work this out to her benefit in guessing the secret key. This so called side channel attack [73, 140] is very serious in any QKD system as Eve can get information about the key directly from the devices that are being used. One way to get rid of this is to use fully device independent QKD, however, it is still not widely used [56, 57, 141] since they are much more resource intensive unlike general prepare and measure protocol such as BB84, at the same time their key generation rate is quite low. Although one cannot avert side channel attack completely but can make sure that Eve's gain is minimized. This information leakage [106, 142, 143] to Eve will keep an upper bound on the key after error correction and privacy amplification (PA) [92]. For properly quantifying the amount of information going to Eve, one needs to know the limitations in the devices that are used in the QKD process. Devices at both ends (Alice and Bob) must be calibrated in order to quantify the side information to Eve. Device imperfections at the Bob's end are easy to measure as these can be verified through parameter estimation for QKD. A typical implementation of BB84 protocol for quantum communication uses four laser diodes for transmitting weak coherent pulses, which may not have the same characteristics. We have characterized these lasers for mismatch in various parameters such as spectral width, pulse width, spatial mode, peak wavelength, polarization and their arrival times at the receiver. This information is utilized

to calculate possible information leakage through side channel attacks by evaluating mutual information between source and eavesdropper. Based on our experimental observations of cross correlation between parameter values for different laser diodes, we suggest methods to reduce information leakage to Eve.

We are interested in calculating Alice's information leakage as the vulnerabilities associated with the source are highly prone to leakage. This is because signals passing through the quantum channel can always be under Eve's surveillance. Therefore, the primary concern is to evaluate the various source parameters for side channel attack. For quantifying this, one has to calculate the mutual information between the source and Eve. The inability of the source to produce ideal states for QKD will give information to Eve. This can depend upon various parameters characteristics to the source. To know the amount of information leakage, one has to meticulously calibrate the source for these parameters, which could be wavelength, photon arrival time, or any other parameter making the transmitted states distinguishable from each other such that Eve can easily gain some information out of it. Therefore, source calibration is essential for knowing the mutual information between the source and the adversary. Here, we calibrate our QKD transmitter consisting of four laser diodes through cross correlation for various parameters and use it to estimate the mutual information [16, 66] between Eve (E) and Alice (A), unlike [106] that calculates conditional probabilities to find out this information.

## 4.2 Information Leakage due to Imperfections

The average information in any event such as coin toss, die roll etc. is given by Shannon entropy [66, 79]

$$H(X) = \sum_i p_i(x) Log \frac{1}{p_i(x)}. \tag{4.1}$$

Where $p_i(x)$ is the occurrence probability of an event x. From Equation (4.1) indicates the information gained after the event has happened. Mutual information is basically the correlation between variables of the two parties involved in communication. It quantifies the amount of knowledge one has about the other. The mutual information between two parties Alice (A) and Bob (B) can be written as [16, 37, 66]

$$I(A:B) = H(A) - H(A|B). \tag{4.2}$$

$H(A)$ is the information entropy Alice has about her variables and $H(A|B)$ is the conditional entropy of Alice given Bob measured his. This can be further simplified in terms of corresponding probabilities

$$I(A:B) = H(A) + \sum_{a \varepsilon A} p(a) \sum_{b \varepsilon B} p(b|a) Log(p(b|a)), \tag{4.3}$$

where $p(a)$ is the probability of occurrence of an event "$a$" and $p(a|b)$ is probability of happening "$a$" given the event "$b$" has already occurred. The event "$a$" can be an outcome from the space $A$, similarly "$b$" can be an outcome from the space $B$ and $Log$ is taken in base 2. In practice this tells us how much Bob's information is correlated to Alice. The secret key rate for reverse and direct reconciliation in QKD protocol is

given by [16, 73, 83]

$$r_{DR} \geqslant I(A:B) - I(A:E) \tag{4.4}$$

$$r_{RR} \geqslant I(A:B) - I(B:E) \tag{4.5}$$

where subscript *RR* means reverse reconciliation in which Alice corrects the erroneous bits after sifting by comparing it with the Bob's key. *DR* means direct reconciliation where Bob makes correct changes in the key by verifying it with Alice after sifting. For secure QKD protocol this quantity should be non zero. For $r_{DR}, r_{RR} \geqslant 0$ implies that the mutual information between Alice and Bob ($I(A:B)$) must be greater than Alice and Eve ($I(A:E)$) and Bob and Eve ($I(B:E)$). $I(A:E)$ can be found out if we know the transmission channel and also the errors occurring at the source and $I(B:E)$ can be measured by looking at the imperfections in the detection unit setup by Bob. If the two parties happen to be Alice and Eve then Eq.(4.3) can be rewritten as [73, 106]

$$I(A:E) = 1 + \sum_{a \varepsilon A} p(a) \sum_{b \varepsilon E} p(b|a) Log(p(b|a)) \tag{4.6}$$

In Eq.(4.6), $b$ is the outcome of Eve's measurement in her device. Given the outcome $a$ at Alice's side, Eve's probability to measure bit $b$ is the conditional probability ($p(b|a)$). In reality, Alice doesn't know what method Eve will use; therefore, for quantifying this information, the measurement has to be done from Alice's side. It means she has to make sure how much Eve can guess about the states she is sending. To calculate the conditional probability for a variable, we use Bayes' Theorem by taking the source's parameter that deviates from the assumed value in the implemented protocol. Since we have used four different laser diode sources, due to differences in electronic fluctuations in the driving circuit, there may be a difference in wavelength ($\lambda$), pulse width ($w$), and other parameters. Equation (4.6) decides the amount of information

leakage to Eve due to imperfections in these parameters of the source. To characterize this quantity, we need to measure the amount of indistinguishability between various source parameters.

In Eq.(4.6), the primary quantity that needs to be calculated is the conditional probability $p(b|a)$, as this quantity decides the amount of information shared between Alice and Eve. Here, the parameters in consideration are wavelength ($\lambda$), pulse width ($w$), photon time arrival ($t$), polarization error at the source, and spatial mode ($x$). These are the events occurring in Alice's system and the bit value that Eve gets after measuring the states is $b$ (it can either be 0 or 1). $p(\lambda|b)$ can be calculated with the help of joint probability distribution ($p(\lambda,b)$). We can rewrite Eq.(4.6) in terms of experimental parameters

$$I(A:E) = 1 + \sum_{\lambda \varepsilon \Lambda} \sum_{b \varepsilon E} \frac{p(\lambda|b)}{2} Log\left(\frac{p(\lambda|b)}{2p(\lambda)}\right) \tag{4.7}$$

Here, $\lambda$ is the wavelength of the laser having a finite bandwidth (FWHM). $\Lambda$ is the space containing all values of $\lambda$. Just as wavelength ($\lambda$), Eq.(4.7) will be identical for other parameters also. For pulse width $\Lambda$ is replaced by $W$, similarly for photon time arrival it is $T$ and $X$ for spatial mode. Estimating $I(A:E)$ as given in Eq.(4.7) can be slightly time taking task if we are implementing the QKD source in the field. Instead we have come up with a method that can quickly give us the amount of information leaked to Eve quantitatively.

### 4.2.1 Cross-correlation and Mutual Information

For two different functions, cross correlation denotes the amount of similarity between them. This can be checked by moving one function $g(x)$ with respect to another function $f(x)$ with some interval ($\Delta s$). At each step moved the value of both the functions are evaluated and the corresponding cross correlation is calculated. This value basi-

cally indicates the similarity between the two functions with respect to the step taken. For discrete systems cross correlation between two functions is given by

$$R(\Delta s) = \sum_{i=0}^{\infty} f^*(x_i)g(x_i + \Delta s). \tag{4.8}$$

$R(\Delta s)$ is the cross correlation between function $f(x)$ and $g(x)$ when their origin is shifted by $\Delta s$ (Figure 4.1). For continuous functions the expression for cross correla-

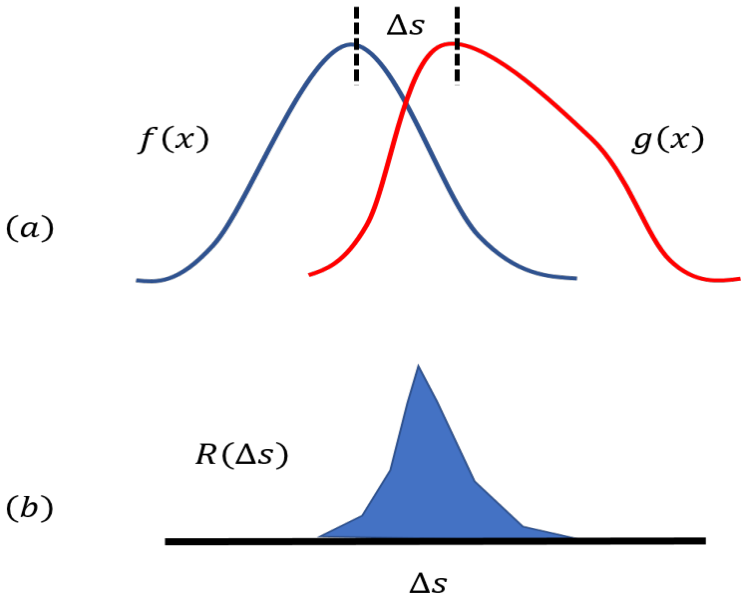



**Figure 4.1:** (a) Cross correlation between two functions with respect to delay $\Delta s$. (b) Shows the value of $R$ changes with respect to $\Delta s$, for the above case this gives maximum value for $\Delta s = 0$.

tion takes the form [144]

$$R(\Delta s) = \int f^*(s)g(s + \Delta s)ds. \tag{4.9}$$

Equation (4.9) tells us about the similarity between the two signals $f$ and $g$ as a function of $\Delta s$. The quantity $\Delta s$ is the shift of one signal with respect to other and the value of $R$ ranges from 0 to 1. We, need to calculate the cross correlation ($R$) between various

parameters of the two sources for the same basis in the QKD transmitter to quantify the amount of information leakage. The indistinguishability between the sources can be known from $R(\Delta s = 0)$ (more close to 1 means more similar to each other). Putting $R(\Delta s = 0)$ in Eq.(4.7) we get

$$I(A:E) = 1 + \sum \frac{R(0)}{4} Log\Big(\frac{R(0)}{4p(\lambda)}\Big). \tag{4.10}$$

$R$ is the measure of offset of the parameters like wavelength, pulse width etc. between the four laser diodes. It is impossible for Eve to predict the state of Alice's signal after measurement if the parameters of the sources are identical. $p(\lambda|b)$ tells about probability of guessing the correct initial state after the measurement by Eve. This value is half i.e upon getting a bit value 1 it is impossible to say whether it comes from source containing $\lambda_1$ or $\lambda_2$. Deviation from this value basically gives us the quantity of leaked information. $R(\Delta s = 0)$ represents the deviation from indistinguishability between the various parameters of the source. By argument, one can say that the quantity $R(\Delta s = 0) \times \frac{1}{2}$ is the guessing probability of Eve, so this quantity can be replaced with $p(\lambda|b)$. For exactly identical states, the quantity $I(A:E)$ will be zero as the parameters of the source are indistinguishable which can be verified using Eq.(4.10). Therefore, measuring the cross correlation between the various parameters gives a good idea about amount of information leakage to the eavesdropper.

## 4.3 Experimental Method

The schematics of the experiment is given in the Figure 4.2. In the setup, the measurement devices can be changed according to the parameters that need to be measured for the experiment. The scheme contains four laser diodes (ThorLabs L808P010) with driver circuit [104]. The pulse width coming out from the laser can be varied according

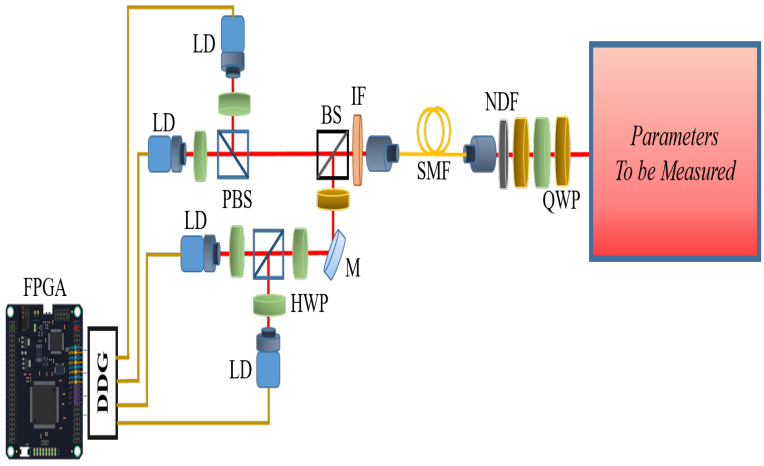



**Figure 4.2:** Experimental scheme for measuring the parameters involved in source characterization. For different parameters one has to change the measuring devices. **LD**: Laser Diode, **FPGA**: Field Programmable Gate Array, **PBS**: Polarizing Beam Splitter, **HWP**: Half Wave Plate, **QWP**: Quater Wave Plate, **M**: Mirror, **SMF**: Single Mode Fiber, **NDF**: Neutral Density Filter, **IF**: Interference Filter, **DDG**: Digital Delay Generator, **BS**: Beam Splitter.

to input bias voltage. We keep the average pulse width around (650 ps) and the repetition rate of the laser is 5 MHz. The laser driver circuit is connected to stable power supply (Keithley 2231A-30-3) and FPGA (Arty A7) for driving it randomly. The initial HWP and PBS combination is used for preparing specific polarization states for encoding Alice's signal. All of the four states coming out from the laser diodes are combined in the 50:50 beam splitter and coupled to a single mode fiber (SMF). The SMF is used to reduce any sort of misalignment error in the four lasers. Then a combination of QWP, HWP and QWP is used for compensating the polarization after propagation through the fiber [145]. For measuring wavelength, we just place an optical spectrometer (Ocean Optics HR4000), for pulse width it is a fast photodetector whose output is connected with oscilloscope for monitoring the signal. For measuring the spatial mode we use EMCCD camera. Photon arrival time is measured by placing a single photon counting module (Excelitas SPCM-AQRH-16) connected to time tagger (ID Quantique ID900). The clock of frequency equal to the driving frequency of the

laser is sent to TDC for starting the counting time of photon arrival. The histogram will give us the knowledge of time of arrival of photons with respect to clock.

## 4.4 Results and Discussion

Experimental results show that the proper source characterization should be done to quantify the amount of information leakage due to side channel attack by the adversary. The following parameters have been quantified for indistinguishability between the individual laser diodes of the BB84 source.

### 4.4.1 Information Leakage due to Wavelength Mismatch

The mismatch between the peak wavelengths for the laser diodes can give eavesdropper a chance of differentiating between different polarization states by looking at the mismatch between the wavelengths. The Figure 4.3 shows the wavelengths (nm) verses normalised intensity in terms of counts per second (cps) for four laser diodes and their mismatch in terms of peak difference.

The source is having the average wavelength of 795.6 nm.The measurements have been taken without putting any wavelength filters. Figure 4.3 shows the wavelength of the four laser diodes in the Alice transmitter unit. The information leakage due to wavelength difference between the four laser diodes calculated from the cross correlation between the lasers is $I_{\{H,V\}}(\Lambda : E) = 4.3 \times 10^{-3}$ bits/pulse where the subscripts $H,V$ denote the information leakage in H/V basis and $\Lambda$ and $E$ are the corresponding spaces on which a typical $\lambda$ and $b$ belong. Similarly $I_{\{D,A\}}(\Lambda : E) = 6.5 \times 10^{-3}$ bits/pulse and gives mutual information $I(\Lambda : E) \propto 10^{-3}$ bits/pulse.

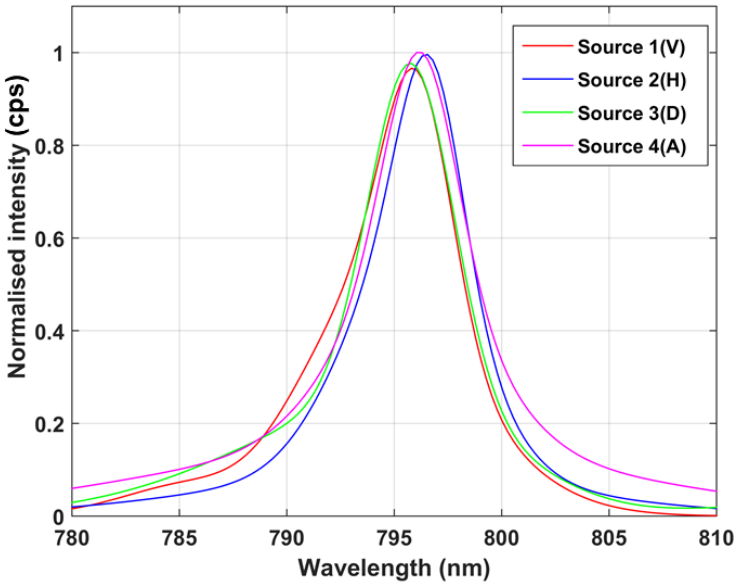



**Figure 4.3:** Spectrum of four laser diodes without using Interference Filter (IF)

### 4.4.2 Information Leakage due to Pulse width Mismatch

The difference between the FWHM of the pulses (pulse width) from the laser diodes can give eavesdropper a chance of differentiating the transmitted states. In our setup, the shape of the RNG output pulses from the FPGA that are fed into the driver circuit are identical but, the optical response of the four laser diodes is not completely identical leading to a difference in the pulse widths from each diode. Therefore, optical output pulse of the laser diode is independent of the RNG pulses fed through FPGA. This variation in the pulse width creates some degree of distinguishability which can be exploited by Eve. Eve can unambiguously detect the polarization states sent from Alice just by looking at their pulse width variation in her detector. For characterizing this error the measurement scheme is modified by replacing spectrometer with photodetector. The source has an average pulse width of 627 $\pm$ 75 ps as shown in Figure 4.4. In QKD mode (sending qubits to Bob) pulse height is made identical by applying different attenuation to different states. All the four sources then have identical

height hence having same mean photon number ($\mu$). The information leakage due to

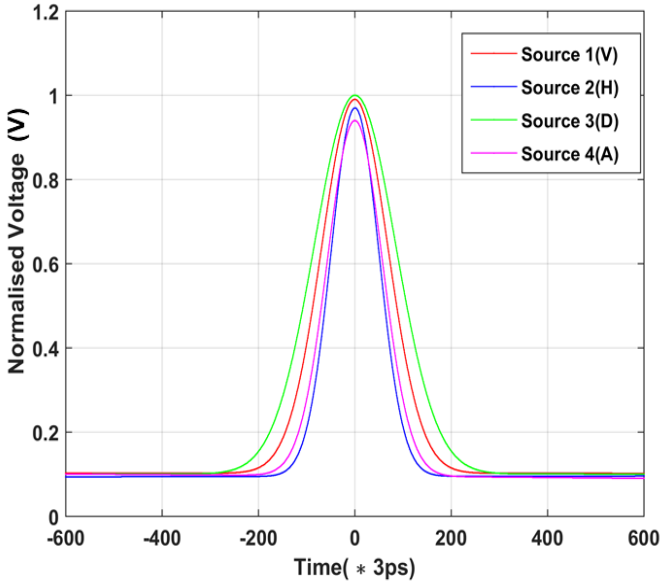



**Figure 4.4:** Pulse width of four laser beam coming out from different laser drivers

pulse width in laser diodes calculated from the cross correlation between the sources is $I_{\{H,V\}}(W:E) = 9.2 \times 10^{-4}$ bits/pulse, $I_{\{D,A\}}(W:E) = 1.2 \times 10^{-3}$ bits/pulse with mutual information $I(W:E) \propto 10^{-3}$ bits/pulse.

Eve can design optimized attacking strategies based on the knowledge of both wavelength and pulse width from which she can learn more about the state. In fact, Eve can also exploit all the side channels together which may allow her to extract more information. However, it is too complex to conceive a best attack strategy which is out of scope of this article. Nevertheless, we will try to consider it in our future work.

### 4.4.3 Information Leakage due to Arrival Time Mismatch

The arrival time of photons will depend on at what time the photons from different laser diodes are leaving the Alice's QKD transmitter. The difference in the initial timing will give a hint to eavesdropper about the corresponding states being sent to Bob. Even if

the optical circuit is perfect, the driving electrical circuit which triggers the on and off time of the laser diodes is subject to jitter. This will result in pulses from different diodes leaving the transmitter at different times causing a difference in the photon arrival times. This can be exploited by Eve to extract information about the states sent from Alice to Bob by looking into the timing information that is disclosed during the sifting stage in the QKD protocol [146]. In order to know the amount of information that can be gained by Eve, one has to measure photon arrival time. For measuring it, the attenuated pulses need to be sent to single photon detector and the output of that is taken from a time counter. The average time of arrival of the photons is almost same for the four laser diodes as seen in the Figure 4.5 which in this case is 41.34 $\pm$ 0.075 ns as derived from their peaks. The information leakage due to photon arrival time difference for four laser diodes calculated from the cross correlation between the sources is $I_{\{H,V\}}(T:E) = 3.2 \times 10^{-3}$ bits/pulse, $I_{\{D,A\}}(T:E) = 2.5 \times 10^{-3}$ bits/pulse with mutual information $I(W:E) \propto 10^{-3}$ bits/pulse.

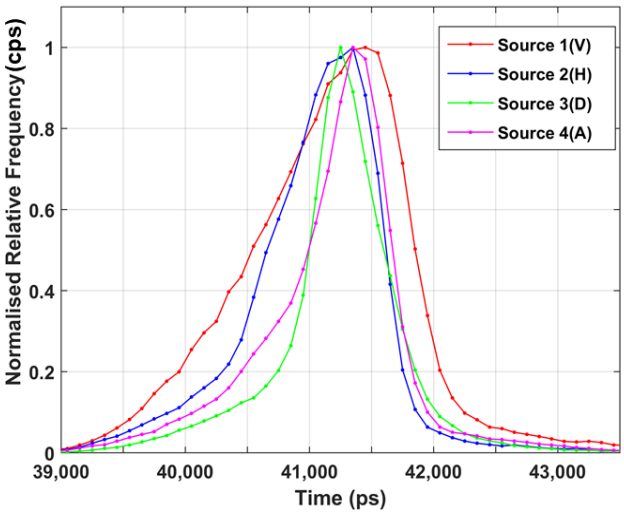



**Figure 4.5:** Graph showing arrival time of photons from four different laser diodes

### 4.4.4 Information Leakage due to Polarization Error at Source

The use of optical devices in the transmitter to combine the beams from four diodes into one may lead to many imperfections. These imperfections may occur either due to misalignment in the transmitter setup or due to imperfect optics. Therefore, the generated states are not perfect in terms of polarization and may contain error which may reflect in the polarization extinction ratio in H,V as well as D,A basis. This error may lead to information leakage to Eve. It gets further amplified in the final QBER after the states are sent to Bob. Figure 4.6 gives the errors in polarization. It shows that from mismatch in the basis dependent error (in non-compatible basis)

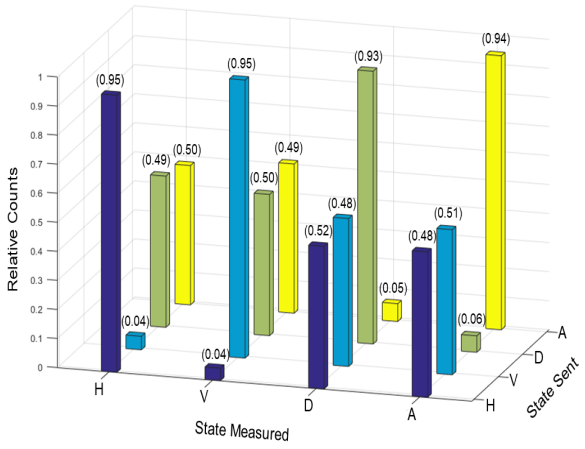



**Figure 4.6:** Polarization error at the source

Eve can extract information about the bits sent by Alice. Error in $H/V$ and $D/A$ basis are $e_{H/V} = 0.0341$ and $e_{D/A} = 0.0094$ respectively and their mismatch is $\Delta e = |e_{H/V} - e_{D/A}|$. While doing basis reconciliation in QKD Eve can guess the bits sent to Bob by the data she already had about this mismatch. So, information shared between Alice and Eve is $I(A:E) \propto \Delta e \propto 10^{-2}$ bits/pulse.

### 4.4.5 Information Leakage due to Spatial Mode Mismatch

While doing free space QKD it becomes very important to look at the modes of the signal that are propagating through the medium. The spatial mode may be responsible for creating vulnerability in the QKD source. If the modes do not perfectly overlap with each other it may hamper the indistinguishability of four quantum states. If the four beams enter the fiber with different injection angles then the output spot size distribution will be different for different beams and is evident while using shorter length fibre for mode cleaning. This mismatch in spatial modes can be measured by EMCCD camera. For making four spatial modes overlap with each other one needs to couple them into a short length single mode fiber. Earlier work has not given much emphasis on mismatch among spatial modes as they amounted to very less leakage [106] but here we show that if Eve has a very low pixel size camera then she could measure the mode mismatch in four laser diodes. Experimental scheme remains the same as in Figure 4.2 except that EMCCD camera is used instead of spectrometer. Images of spatial modes of four laser diodes are recorded in EMCCD camera. Figure 4.7 shows the spatial mode distribution of these four laser diodes. The information leakage due to spatial mode difference for the four laser diodes calculated from the cross correlation between them is $I_{\{H,V\}}(X:E) = 4.2 \times 10^{-3}$ bits/pulse, $I_{\{D,A\}}(X:E) = 4.5 \times 10^{-3}$ bits/pulse with mutual information $I(X:E) \propto 10^{-3}$ bits/pulse.

The highlight of the present work which makes it different from [106] is the consideration of new parameters that can also contribute to the information leakage. Pulse width variation is an important parameter in the source which gives rise to side channel information to the adversary. Our work quantifies this leakage of information to Eve due to pulse width mismatch between four laser diodes. Secondly, the polarization error in different bases at the source is also an important quantity which sets a bound

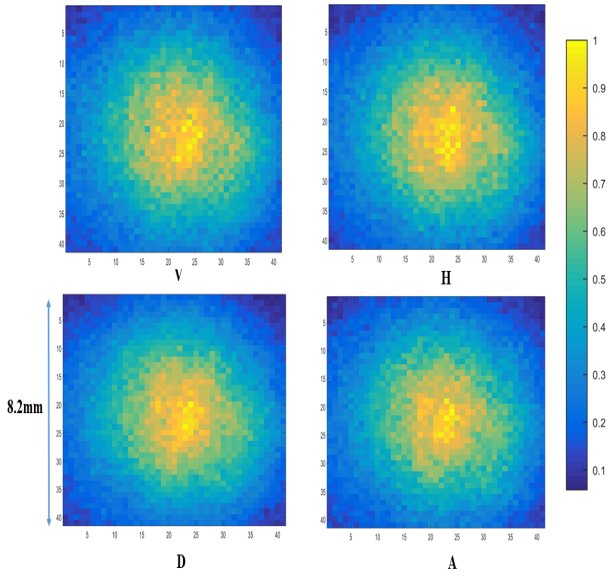



**Figure 4.7:** Images of beams taken at the out of the fiber which are coming from four laser diodes

in the side channel information to Eve. Lastly, it has been shown that leakage can take place if Eve uses detector with smaller pixel size to find the spatial mode distribution of four states. Smaller the pixel size, Eve will be able to discriminate four spatial modes with higher certainty. However, [106] concludes that spatial measurements leads to negligible information leakage.

In the given reference [106], to find out the information leakage, laborious way of calculating the conditional probabilities has been used. Instead we use the cross correlation technique, which is much more experiment friendly, simple and also gives a good estimation of the side channel leakage in the QKD source.

## 4.5 Conclusion

In the present work we have characterized the various source parameters that can lead to possible side channel attack. Using cross correlation function for calculating

mutual information between Alice and Eve gives quite good results. This method is simple which can be easily implemented in the field and gives real-time values for possible information leakage. In our setup parameters such as pulse width and spatial mode contribute less to side channel information to Eve. The information leakage once quantified can be crucial for extracting the secret key after privacy amplification. This mutual information can further be decreased by correcting the optical and the electronic elements in the source. To make a better BB84 source, one has to make sure that the states that are being created must be as indistinguishable as possible. This makes very difficult for Eve to guess the states correctly by knowing the parameters of the source. For wavelength mismatch one can put very narrow bandwidth filters which can decrease the the overall FWHM as well as the peak to peak mismatch between the four laser diodes. Using precise temperature control and stabilization methods one can reduce the wavelength mismatch between the four laser diodes. For making the pulse width of the laser diodes same, one can build a common laser driver circuit for them. For making arrival times same for all the four laser diodes one has to put fast delay generator in the driving circuit. For removing spatial mode mismatch, one can use long length fiber for mode cleaning. For reducing polarization error, one can use polarization maintaining fiber and broad-band optical elements in the setup. The parameters contributing to information leakage are mainly wavelength and polarization errors which need special attention while developing the QKD source. Earlier spatial mode was thought to be contributing less in information leakage [106, 147] but if Eve has good resolution camera, then she can guess the states with more confidence. Pulse width mismatch contributes less in this leakage and can be overlooked if the bit length of the secure key is not the matter of concern.

# Chapter 5

# Increasing Key rate of BB84 protocol with Coincidence Detection Method

## 5.1 Demand for QKD with Multi-Photons

BB84 is proven to be unconditionally secure, based solely on the validity of the laws of quantum mechanics [41, 72, 93]. It was later pointed out that imperfection in practical implementations seriously undermine the security of the QKD protocols [81]. This led to proposals for various types of attacks exploiting the imperfections in the components of the QKD system [106, 148–150]. One of them was the lack of ideal single photon sources. This led to the use of weak coherent pulses in which the number of photons in each pulse is governed by a Poissonian distribution. This leads to non-zero probability of pulses containing more than one photon. An eavesdropper can exploit this major vulnerability to extract information about the key during the transmission stage by using a photon number splitting attack [81]. This resulted in several innovative protocols [42, 51, 55–57, 136, 141, 151–153] and proof of security

with practical implementations [20, 47, 48]. Notable among the proposed protocols was the decoy state protocol [54, 56] for its efficient mitigation of the photon number splitting attack. On the other hand, entanglement based protocols [136, 141] suffered from very low key rates and problem of distributing entanglement over long distances reliably with high fidelity. As a result, the decoy state method emerged as the preferred method for long distance quantum key distribution [59, 154, 155] with a key rate that was substantially higher than the key rate for implementations with imperfect devices [48]. In this method, the sender, Alice, prepares a set of decoy pulses with varying intensities in addition to the standard BB84 states. The decoy pulses are inserted randomly within the actual signal pulse train unknown to the receiver, Bob, as well as any potential eavesdropper, Eve. Without any prior knowledge regarding the position of the decoy pulses, there is an equal probability of Eve attacking both the decoy as well as the BB84 signal pulses. By monitoring the quantum bit error rate (QBER) of the decoy pulses, Alice and Bob can reliably estimate a lower bound for the secret key rate. But the improved performance comes at a cost. Implementation of the decoy state protocol requires multiple intensities of the weak coherent pulses, its calibration and increased complexities in hardware and processing.

The major contribution of this work is to demonstrate that, an increased key rate can be achieved without using decoy pulses when communicating parties are in direct line of sight (LOS) channel which can be monitored by other methods, for example, using Lidars [156]. LOS channel are most commonly used in terrestrial communication between two towers in the same city or different cities and also in high altitudes [35, 157]. For small distance communication direct LOS channel can be realized using drones [158]. The protocol utilises the inherent randomness in the number of photons per pulse of the source itself. The presence of multi-photon pulses sent by Alice is tracked by coincidence detection at Bob's end and secure key is extracted using some of the

multi-photon pulses too. The difference in the number of actual recorded coincidences and expected number of coincidences for a given value of mean photon number for a given channel plays an important factor in this case. If the ratio of this difference with the actual number of coincidence falls below a threshold value, security is compromised and the protocol is aborted. Otherwise they form the key from the single as well as some of the multi-photon pulses followed by standard error correction and privacy amplification methods. We also use an additional figure of merit, the ratio of coincidences to singles to further monitor the security. Since we use coincidence measurements as a major tool, we call this the Coincidence Detection (CD) protocol.

We introduce a quantum key distribution protocol for the line of sight channels based on coincidence measurements. We present a proof-of-concept implementation of our protocol. We show that using coincidence measurements to monitor multi-photon pulses results in a higher secure key rate over longer distances for such channels. This key rate is higher than the decoy state protocol, the most popular practical implementation of quantum key distribution protocol based on BB84.

## 5.2 General Analysis of Key Rate for Poissonian QKD Sources

In this section, we will provide the mathematical derivation of the key rate for our protocol. But before proceeding with the derivation, let us first briefly outline the protocol as follows:

- Alice sends weak coherent pulses to Bob prepared in the standard way for polarization based implementations of BB84.
- Since the number of photons in each pulse is governed by poissonian statistics,

some of the pulses might contain more than one photon.

- Bob, while recording the measurement results, also records all the 2 and 3-fold coincidence events. The coincidence window is set according to the pulse width of the signal pulses.

- The total number of coincidences are matched with the expected number of coincidences which are calculated from the value of $\mu$.

- Any change in the number of 2 and 3-fold coincidences than the expected value for a specific channel will reveal the presence of eavesdropper in the system assuming that Eve is randomly attacking the pulse (no collective and coherent attack).

To estimate the number of 2 and 3-fold coincidence events, it is essential to consider how the pulses split at a balanced beam splitter (BS). The action of BS for single photon inputs in both the ports is given by

$$\begin{bmatrix} \hat{a}_2 \\ \hat{a}_3 \end{bmatrix} = \begin{bmatrix} t_{02} & r_{12} \\ t_{13} & r_{03} \end{bmatrix} \begin{bmatrix} \hat{a}_0 \\ \hat{a}_1 \end{bmatrix}, \tag{5.1}$$

where $\hat{a}_0$ and $\hat{a}_1$ are field operators at the input ports of the BS as shown in the Figure 5.1 and $\hat{a}_2, \hat{a}_3$ are the values at the output ports. Variables $t_{ij}$ and $r_{ij}$ are the transmission and reflection coefficients of the BS (Figure 5.1). For balanced beam splitter (50 : 50 BS) the $2 \times 2$ square matrix takes the value as

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}. \tag{5.2}$$

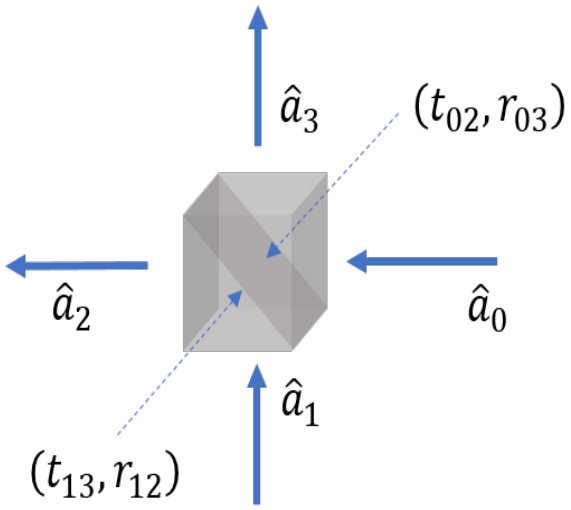



**Figure 5.1:** Schematics representing the action of beam splitter (BS) on single photon inputs.

By applying this value, the relation between input and output ports becomes

$$\begin{aligned} \hat{a}_2 &= \frac{1}{\sqrt{2}}(\hat{a}_0 + i\hat{a}_1) \\ \hat{a}_3 &= \frac{1}{\sqrt{2}}(i\hat{a}_0 + \hat{a}_1). \end{aligned} \tag{5.3}$$

Now, taking one port to be empty and injecting '$n$' photons on port $\hat{a}_0$, then the output photons are distributed between the reflected and transmitted ports as

$$|n\rangle \rightarrow \sum_{k=0}^{n} C_k^n |n-k\rangle_R |k\rangle_T, \tag{5.4}$$

where $R(T)$ corresponds to the reflected (transmitted) port. $|C_k^n|^2$ is the probability of getting $n$-$k$ ($k$) photons in the reflected (transmitted) port (Figure 5.2). The possible cases for 2 and 3 photon pulses are given below in the tables 5.1 and 5.2 respectively. We will take the coincidences arising out of this splitting of pulses into our consideration when deriving the final key rate.

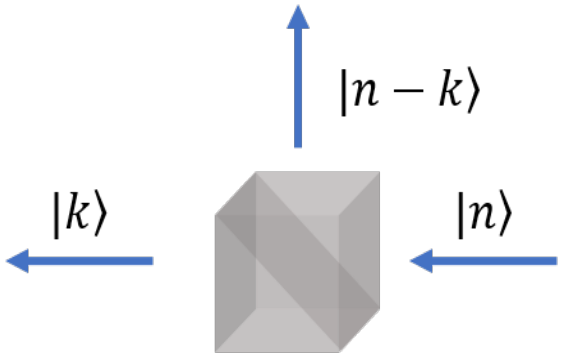



**Figure 5.2:** Output port photon distributions for $n$ photon input state

Table 5.1: Splitting of a two-photon pulse at a beam splitter.

| Possible Cases | Number of Photons at Transmitted Port | Number of Photons at Reflected Port | Probability |
|---|---|---|---|
| 1 | 2 | 0 | 1/4 |
| 2 | 0 | 2 | 1/4 |
| 3 | 1 | 1 | 1/2 |

Table 5.2: Splitting of a three-photon pulse at a beam splitter.

| Possible Cases | Number of Photons at Transmitted Port | Number of Photons at Reflected Port | Probability |
|---|---|---|---|
| 1 | 3 | 0 | 1/8 |
| 2 | 0 | 3 | 1/8 |
| 3 | 1 | 2 | 3/8 |
| 4 | 2 | 1 | 3/8 |

In order to derive the key rate, we follow the treatment of [56]. We denote phase randomized signal state of the weak coherent pulses as mixture of coherent states

$$\rho = \frac{1}{2\pi}\int_0^{2\pi} |\sqrt{\mu}e^{i\theta}\rangle\langle\sqrt{\mu}e^{i\theta}|d\theta. \tag{5.5}$$

Here, $\mu$ stands for average number of photons per pulse and the signal is assumed to be randomised over all $\theta$. The probability $P(n)$ of each pulse carrying $n$ photons is

derived from the Poissonian distribution as $p_n = e^{-\mu}\mu^n/n!$. Progressing onwards, the gain $Q_\mu$ of each pulse is defined as

$$Q_\mu = Y_0 e^{-\mu} + Y_1 e^{-\mu}\mu + Y_2 e^{-\mu}(\mu^2/2!) + ... + ... + Y_n e^{-\mu}(\mu^n/n!), \tag{5.6}$$

where $Y_n$ is the conditional probability that Bob detects an "n photon" signal state given that Alice has sent an "n photon" state. Then, $Q_n$ becomes the joint probability of Bob detecting "n photon" signal and Alice sending the same "n photon" signal state. For realistic cases, in the absence of an eavesdropper, the term $Y_0$ gives the background rate of the system including detector dark counts, $p_{dark}$. For $n \geq 1$ , yield $Y_n$ consists of two terms, the detection of signal photons travelling through the channel and the background rate. Assuming that the background rate and the signal events are independent, the expression of $Y_n$ is seen to be dependent on the channel [56] and approximated to

$$Y_n \approx [\eta_n + p_{dark}]/2. \tag{5.7}$$

The transmission efficiency $\eta_n$ of the channel is related to the number of photons as

$$\eta_n = 1 - (1-\eta)^n, \tag{5.8}$$

where $\eta$ is the overall channel transmissivity. Now, the quantum bit error rate (QBER) corresponding to each signal state, $E_\mu$, is defined as

$$E_\mu Q_\mu = \sum_{n=0}^{\infty} Q_n E_n, \tag{5.9}$$

where $E_n$ is the error corresponding to the signal containing $n$ photons. Even in the absence of any signal pulse, Bob might record a detection due to background photons or dark current of the detector. This error results in $E_0$ and is equal to 1/4 since all four

detectors have equal probability of registering a dark count. If the signal has $n \geq 1$ photons, then the error $E_n$ is given by

$$E_n = \left(\eta_n \frac{E_{detector}}{2} + (1-\eta_n)\frac{p_{dark}}{4}\right)/Y_n, \tag{5.10}$$

where $E_{detector}$ is independent of $n$ and the values of $E_n$ and $Y_n$ can be experimentally derived from the measured values of $Q_\mu$ and $E_\mu$. Major change in these values for a specific channel will reveal the presence of eavesdropper.

Having defined all the necessary terms and variables, let us briefly look at how the equations governing the secret key rate evolve. It was shown in [41] that secret key rate in an ideal implementation scenario with a perfect single photon source and perfect detectors has the form

$$R \geq [1 - 2H_2(E_b)], \tag{5.11}$$

where $H_2$ is the binary Shannon entropy defined as $H_2(x) = -xlog_2x - (1-x)log_2(1-x)$ and $E_b$ is the QBER. This formula was later modified by [48] for a more realisitic implementation with weak coherent pulses as

$$R \geq qQ_\mu \left\{ -f(E_\mu)H_2(E_\mu) + \frac{Q_1}{Q_\mu}\left[1 - H_2\left(\frac{Q_\mu E_\mu}{Q_1}\right)\right]\right\}, \tag{5.12}$$

where $q$ is an implementation dependent factor. In case of passive random basis selector, like balanced beam splitter, $q = 1/2$. $f(E_\mu)$ is the error correcting code efficiency. A severe shortcoming of the above approach was in estimating the maximal value of $\mu$. In order to minimise the number of pulses with 2 or above photons, $\mu$ had to be kept sufficiently small. This reduced the number of single photon pules thereby greatly limiting the secret key rate. At the same time, the protocol was vulnerable to PNS attacks since the absence of multi-photon pulses could not be ensured. In the decoy state

protocol [56], this was taken care of and the secret key rate was modified to

$$R \geq q\{-Q_\mu f(E_\mu)H_2(E_\mu) + Q_1[1 - H_2(E_1)]\}. \tag{5.13}$$

### 5.2.1 Key Rate Estimation for Coincidence Detection Method

It is seen in Eq. (5.13) that only single photons are contributing to the key. Now, instead of discarding all the multiphoton pulses, we systematically include a fraction of all such pulses in the final secret key rate as

$$\begin{aligned} R_{CD} \geq \{&-qQ_\mu f(E_\mu)H_2(E_\mu) + C_1Q_1[1 - H_2(E_1)] \\ &+ C_2Q_2[1 - H_2(E_2)] + C_3Q_3[1 - H_2(E_3)]\}, \end{aligned} \tag{5.14}$$

where $C_n$'s are the coefficients of the contributing single, double and triple photons pulses with the implementation dependent factor $q$ absorbed into them. This is the secret key rate of the CD protocol. In order to derive these coefficients, consider the following: a single photon pulse can only end in the correct basis with probability 1/2 in case of passive basis selector like a balanced beam spliter for which $q = 1/2$. This leads to to $C_1 = 1/2$. A two-photon pulse will give rise to three cases as in Table 5.1 of which case 3 and only one of case 1 or case 2 will contribute to the key. So, $C_2 = 1/2 + 1/4 = 3/4$. Similarly, from Table 5.2 we obtain $C_3 = 3/8 + 3/8 + 1/8 = 7/8$. In this case, both cases 3 and 4 will contribute to the key since in both cases at least one photon will be detected in the correct basis. Please note that the probabilities in Tables 5.1 and 5.2 are calculated for a balanced beam splitter. So the factor of $q = 1/2$ is already accounted for while calculating the probabilities justifying the absorption of $q$ into $C_n$. Substituting these values in Eq.(5.14) we arrive at the final form of the secret

key rate. The final secret key rate is as follows

$$\begin{aligned} R_{CD} \geq \{ & -\frac{1}{2} Q_\mu f(E_\mu) H_2(E_\mu) + \frac{1}{2} Q_1 [1 - H_2(E_1)] \\ & + \frac{3}{4} Q_2 [1 - H_2(E_2)] + \frac{7}{8} Q_3 [1 - H_2(E_3)] \}. \end{aligned} \tag{5.15}$$

It is evident that some of the pulses with multiple photons also contribute to the secret key rate, therefore, we can achieve a higher key rate compared to the decoy state protocol. This protocol, a modification of BB84 protocol, works best with four SPCMs (Single Photon Counting Modlues) as more number of multiphoton pulses can be tracked and the keys can be extracted from them. For two detector system Eq.(5.15) will be modified by omitting the last term as only two fold coincidences will be observed. For single detector setup only the first and second term will remain in Eq.(5.14).

### 5.2.2 Security Against Eavesdropper

The standard security analysis of a QKD protocol involves calculating the difference in mutual information between the communicating parties and the eavesdropper. For direct reconciliation (DR) the difference in mutual infromation between Alice-Bob and Alice-Eve while, it is Alice-Bob and Bob-Eve for reverse reconciliation (RR). If the mutual information between Alice-Bob exceeds that between Alice-Eve (DR) or Bob-Eve (RR), a secure key can be extracted and the channel is deemed secure. An additional parameter is the QBER. For BB84 based protocols using ideal source and detector, the QBER has an upper limit of 11% against collective attakcs [41, 73]. After the protocol is executed, if the estimated QBER exceeds that limit, the channel is discarded and the protocol is repeated again. For all those attacks that affect the QBER, it serves as a powerful tool at the hands of the communicating parties.

The security for our protocol is derived from monitoring the QBER as well as the total

number of coincidences for a *pre-characterised channel* within acceptable statistical fluctuations due to device and channel limitations. This means, that the channel transmittance is known and is trusted. This is ensured by actively monitoring the channel during the characterisation process. The total number of coincidences expected are

$$C = \frac{1}{2} Y_2 P_2(\mu) + \frac{3}{4} Y_3 P_3(\mu). \tag{5.16}$$

$P_n(\mu)$ is the Poissonian probability of a pulse containing $n$ photons for a given $\mu$. Since the yield $Y_n$ depends on $\eta$, the coincidences depend on both $\mu$ and $\eta$. The fractions $(1/2)$ and $(3/4)$ arise due to the use of a balanced (50:50) beam splitter as the basis selector. The equation (5.16) means that a two-photon pulse will produce a coincidence half of the times while a three-photon pulse will result in a coincidence 3 out of 4 times. Now, the yields are related as already seen in Eq.(5.7)

$$Y_2 = 2\eta; Y_3 = 3\eta = \frac{3}{2} Y_2. \tag{5.17}$$

Substituting these values and writing $P_3(\mu)$ in terms $P_2(\mu)$ in Eq.(5.16), we can write the total number of coincidences as

$$C = \left( \frac{4+3\mu}{8} \right) Y_2 P_2(\mu). \tag{5.18}$$

As the number of coincidences depend on $\eta$ and $\mu$, the statistical fluctuation $\Delta C_{stat}$ can be written as as

$$\Delta C_{stat} = \left| \frac{\partial C}{\partial \eta} \right| \Delta\eta + \left| \frac{\partial C}{\partial \mu} \right| \Delta\mu. \tag{5.19}$$

Both these terms can be rewritten in terms of the $Y_2$ and $P_2(\mu)$. This will help us to compare $\Delta C_{stat}$ with $C$. Making the necessary substitutions, we arrive at the form

$$\Delta C_{stat} = \frac{8+5\mu-3\mu^2}{8\mu} Y_2 P_2(\mu)\Delta\mu + \frac{4+3\mu}{8\eta} Y_2 P_2(\mu)\Delta\eta. \tag{5.20}$$

The factors $\Delta\mu$ and $\Delta\eta$ are implementation dependent factors. The fluctuation in $\mu$ can arise from imperfect attenuators while fluctuations in $\eta$ can arise due to atmospheric changes. Let us assume that $\mu$ varies by a factor of $\alpha$ over the duration for which the protocol is run i.e. $\Delta\mu = \alpha\mu$. For the same duration, let the transmissivity vary by a factor of $\beta$. So, $\Delta\eta = \beta\eta$. Under these conditions, Eq.(5.20) is given by

$$\Delta C_{stat} = \frac{\alpha\left(8+5\mu-3\mu^2\right)+\beta\left(4+3\mu\right)}{8} Y_2 P_2(\mu). \tag{5.21}$$

We can now define a figure of merit $\Xi_{stat} = \Delta C_{stat}/C$, which has the form

$$\Xi_{stat} = \frac{8\alpha+4\beta+(5\alpha+3\beta)\mu-3\alpha\mu^2}{4+3\mu}. \tag{5.22}$$

Assuming that the experimental conditions do not change much during the course of the runtime of the protocol, we can make the realistic assumption that the factors $\alpha$ and $\beta$ are quite small. This helps us to set a theoretical bound on $\Xi_{stat}$. Since the variations of mean photon number ($\mu$) and transmissivity ($\eta$) are well within 1% on an average in our experiment. Therefore, theoretically for setting up the bound we take the values of $\alpha$ and $\beta$ to be around 1%. Additionally, $\Xi_{stat}$ acts as an upper bound for the statistical fluctuations in the number of coincincidences recorded during the course of the protocol.

#### Additional Figure of Merit for Security and Optimal $\mu$

We also define an additional figure of merit, the ratio of coincidences to singles. The total number of single detection events can be written as

$$S = Y_1 P_1(\mu) + \frac{1}{2} Y_2 P_2(\mu) + \frac{1}{4} Y_3 P_3(\mu). \tag{5.23}$$

Using Eqs.(5.17) and (5.18), we arrive at the following expression for the ratio of coincidences to singles, $\zeta$, as follows

$$\zeta = \frac{C}{S} = \frac{3\mu^2 + 4\mu}{\mu^2 + 4\mu + 8}. \tag{5.24}$$

The above analysis derives parameters that give additional security bounds specific to our protocol. These parameters along with QBER estimation suffice to establish the security of our protocol.

## 5.3 Experimental Implementation and Results

We have performed the proof of principle demonstration of our protocol. The details of the experimental setup is shown in Figure 5.3. We have generated weak coherent pulses by using variable optical attenuator at the output of a pulsed laser (Coherent Vitara T (Ti-Sapphire)) with a repetition rate of 80 MHz. After that the encoded state is propagated in free space lossy medium in the laboratory with channel transmissivity estimated at 70%. At Bob's end we have usual polarization based BB84 detection setup: balanced beam splitter (passive random basis selector) with polarizing beam splitter (PBS) on the reflected arm (measurement in {H,V}) and a combination

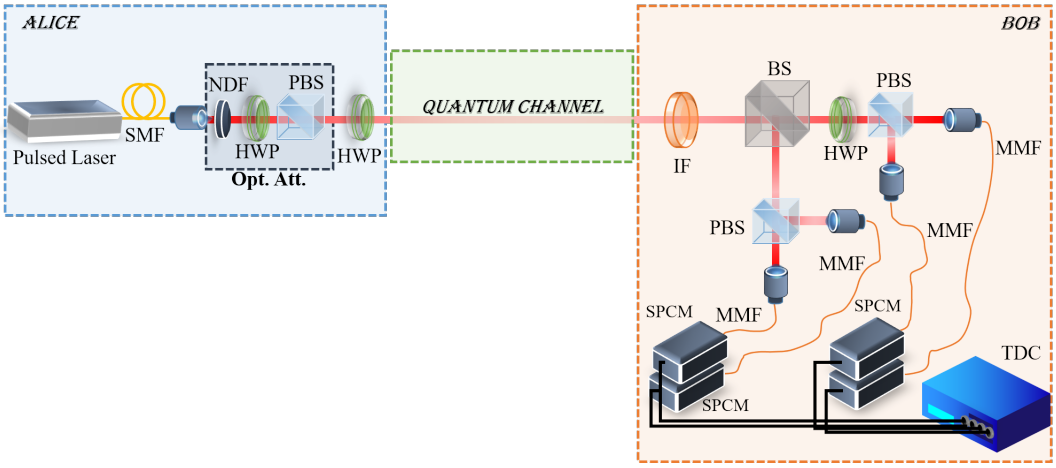



**Figure 5.3:** Experimental setup for coincident detection based quantum key distribution protocol. SMF: Single mode fiber; MMF: Multi-mode fiber; NDF: Neutral density filter; HWP: Half-wave plate; PBS: Polarizing beam splitter; BS: 50:50 beam splitter, IF: Interference filter; SPCM: Single photon counting module; TDC: Time to digital converter.

of half wave plate with PBS (measurement in {D, A}) at the transmitted arm. Photons at the output ports of the PBS are detected by fiber coupled avalanche photo diodes (Excelitas SPCM AQRH-14-FC). The avalanche photo diodes are connected to a 8 channel time to digital converter (IDQuantique ID-800) for recording the counts per integration time. It records singles, 2-fold and 3-fold coincidences between various detectors. The coincidence window should be less than or equal to the temporal pulse width of the signal pulse to minimize the probability of a coincidence being recorded between two successive signal pulses or between a signal pulse and any stray pulse. For field applications we can divide our protocol into two categories based on the available channel: I. LOS channel based implementation and II. non-LOS channel based implementation.

### 5.3.1 Direct LOS Channel

Here we propose to use the CD protocol for realistic atmospheric channels where the line of sight between Alice and Bob is under surveillance. This means, Eve's presence can be detected by monitoring the channel through other means and Eve is not allowed to alter the channel transmittance. From application point of view, these assumptions are realistic and give practical security.

Here the channel is pre-characterized so the amount of coincidences that Bob will

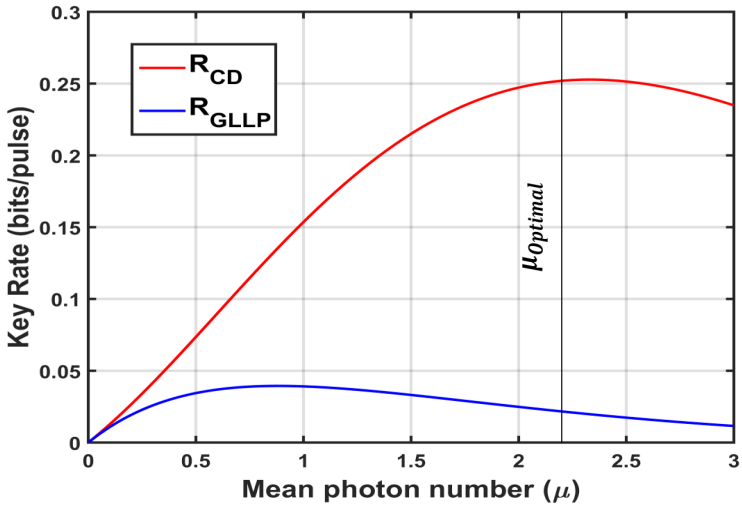



**Figure 5.4:** Variation of the secret key rate with mean photon number $\mu$ for decoy state and CD protocol with $\eta = 0.70$. As, is evident, the CD protocol has greater tolerance for higher values of $\mu$.

receive is known and is given by Eq.(5.16). The key rate for this can then be given by Eq.(5.15) and the security comes from observing the figure of merit $\Xi$ defined in Eq.(5.22). This results in increase in the optimal $\mu$ for the protocol as given in Figure 5.4, which results in increase in the key rate.

The channel transmissivity is calculated as the ratio of signals received to signals sent at the detector. This comes out to be $\eta_t = 0.70 \pm 0.028$. $\eta$ can be found from $\eta_t$ by dividing it with the efficiencies of detector and the fiber coupler. The yield $Y_n$ and $Q_\mu$

can then be calculated by using Eqs.(5.7) and (5.6) respectively. We use the calculated value of $\eta$ along with the value of $\mu$ to estimate the number of coincidence events. We list the number of coincidences $C$ alongwith $\Xi$ and $\frac{C}{S}$ in Table 5.3. It can be seen, the numbers agree within acceptable tolerance with the predicted values from theoretical simulation and as expected, higher values of $\mu$ lead to higher number of coincidences.

Table 5.3: List of values for all the security parameters. $C$ is the number of coincidences, $\Delta C_{stat}$ is the fluctuation in the number of the recorded coincidences, $\Xi_{stat}$ is the ratio between $\Delta C_{stat}$ and $C$ and $\zeta$ is the ratio between $C$ and the number of detected singles. The numbers in brackets for each of the parameteres are from the theoretical modelling of the protocol for a given channel attenuation. The values of $\alpha$ and $\beta$ are taken to be 0.01 corresponding to a 1 % variation in the values of $\mu$ and $\eta$ respectively.

| *Parameters* | *Values* | | | | |
|---|---|---|---|---|---|
| $\mu$ | 0.13 | 0.19 | 0.22 | 0.32 | 0.41 |
| $C$ | 3178 (3189) | 6249 (6414) | 8756 (8828) | 18367 (18657) | 30140 (30337) |
| $\Delta C_{stat}$ | 53 (64) | 69 (140) | 85 (200) | 111 (250) | 237 (340) |
| $\Xi_{stat}$ | 0.016 (0.020) | 0.011 (0.012) | 0.0097 (0.023) | 0.0065 (0.014) | 0.0079 (0.11) |
| $\zeta$ | 0.042 (0.066) | 0.059 (0.098) | 0.069 (0.115) | 0.102 (0.169) | 0.128 (218) |

By tracking the number of coincidences, $\Xi$, and $\frac{C}{S}$ we can monitor the presence of the eavesdropper. If the quantity $\Xi$ is below $\Xi_{stat}$, we can extract keys otherwise the protocol is aborted. Please note that we assume a passive eavesdropper who can only listen in on the communication channel between Alice and Bob and enjoys no control over the channel. In Figure 5.5, we study the secure key rate as a function of the channel length for different values of $\mu$. We see that the secure key rate increases with increasing values of $\mu$ due to increased presence of pulses containing photons. Next, we compare the secure key rates of our protocol with that calculated from the decoy state protocol for the same set of parameters, in Figure 5.6. The results show that we have higher key rate along with increase in the transmission distance. For the given channel and $\mu$ =0.41, we expected a key rate of 0.054 bits per pulse. From the experimental data, we obtained 0.053 $\pm$ 0.004. This matches very well with our

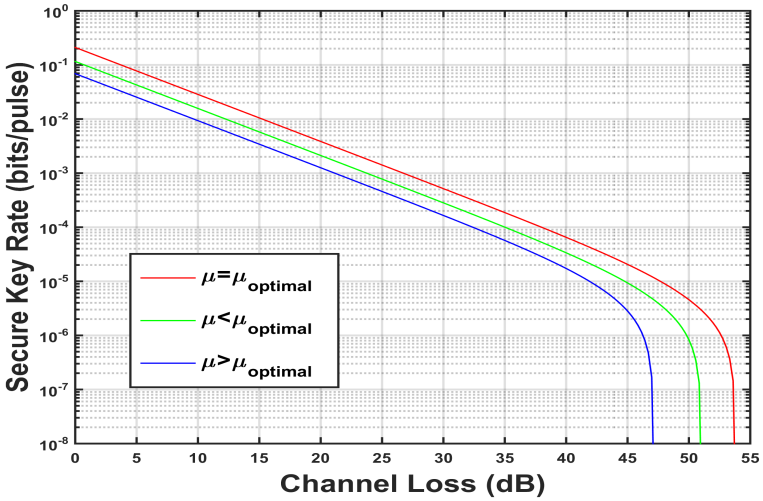



**Figure 5.5:** Secure key rate as function of the channel length with $\mu$ as a parameter. The value of $\mu_{optimal}$ is obtained from Figure 5.4 and is equal to 2.2. Two other values of $\mu$ used in the plot are 0.8 ($\mu < \mu_{optimal}$) and 2.9 ($\mu > \mu_{optimal}$)

.

theoretical model. For the same set of parameters, in case of the decoy state protocol, the expected key rate was 0.032 bits per pulse and the experimentally obtained key rate was $0.031 \pm 0.003$.

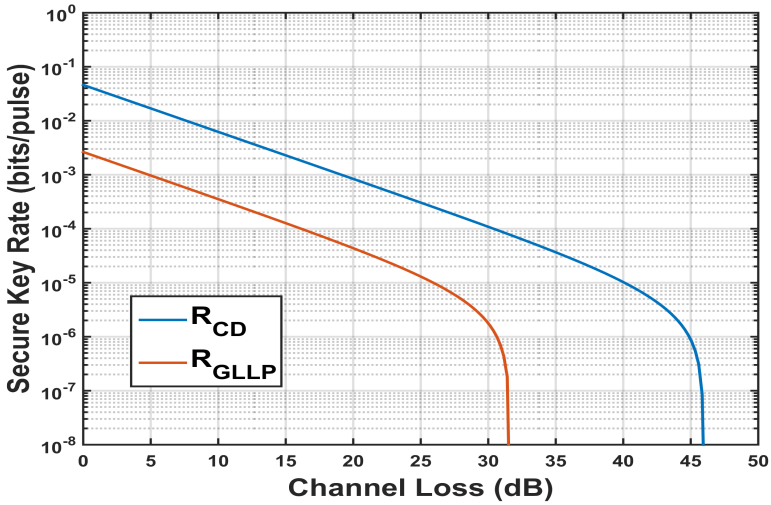



**Figure 5.6:** Comparison of secure key rates between decoy state protocol and CD protocol for the same set of parameters.

The increase in key rate is due to the fact that some of two and three photon pulses also contribute to the key. In addition, this protocol has greater tolerance to higher values of $\mu$ as compared to the decoy state protocol as shown in Figure 5.4. In general, the secure key rate starts decreasing when multiphoton pulses start dominating over single photon pulses. Since coincidence measurements alongwith the security parameters $\Xi$ and $C/S$ can successfully track and extract key from two-photon and three-photon pulses as well as from all the single photon pulses, this results in a much higher tolerance of mean photon number.

### 5.3.2 Non-direct LOS Channel Based Implementation

For the case when direct LOS is not available eavesdropping will be easier as regular channel monitoring will be a difficult task. Eve can take the advantage of this and can vary the losses accordingly (tamper the channel) to match with the original channel after extracting photons from each of the multi-photon pulses for gaining information of the key. This can be averted by incorporating the extra pulses with variable intensities randomly in between the signals akin to decoy state protocol. Lack of knowledge about the extra pulses makes Eve randomly attacking both the signal and extra pulses with equal possibility. The ratio is generally 70 (signal) : 30 (extra) so if Eve attacks them equally the relative loss in the detected number of photons for signal and extra pulses will be different. This change can be observed if the timing information is matched for the received signal and extra pulses with the transmitted. Checking the relative loss between the signal and extra pulses (i.e if the loss of signal is not equal to the extra pulses) can reveal the presence of eavesdropper, making the protocol secure. It must be noted that the introduction of extra pulses does not affect the higher key rate achieved through our protocol in comparison to decoy state protocol.The key rate formula will remain the same as it uses the optimal mean photon number ($\mu$) in which

the protocol must operate to achieve higher key rate.

In CV QKD, characterization of excess noise in the channel is done to track the presence of eavesdropper. This noise can be calculated from the total noise received at the detector which is

$$\xi_{exc} = \xi_{sys} + \xi_{ch} + \xi_{Eve}.$$

Where $\xi_{sys}$ consist of all kinds of noise due to system imperfections, $\xi_{ch}$ is the noise in the channel and $\xi_{Eve}$ is the noise contribution due to Eve while making the measurement. Characterizing the system and channel noise indicates the presence of Eve that can be calculated from total (excess) noise at Bob. The key rate in CV QKD for direct reconciliation in terms of noise can be written as

$$r = I_{A:B}(\xi_{sys+ch}) - I_{A:E}(\xi_{Eve})$$

Where $I_{A:B}(\xi_{sys+ch})$ is the mutual information shared between Alice and Bob, $I_{A:E}(\xi_{Eve})$ is the information gained by Eve. From the above expression if the noise imparted due to Eve ($\xi_{Eve}$) is large, making the key rate negative which results in aborting the protocol. The reviewer is right in pointing out CD protocol is similar to CV QKD protocol as both characterise the channel and system in terms of photon numbers received at Bob (CD protocol). The difference arrives from the fact that security in our protocol is derived from monitoring the QBER, as is done is typical BB84 implementations, as well as two additional security parameters. Qualitatively CD Protocol increases the key rate from standard BB84 protocol and can be comparable to CV QKD key rates for same driving laser frequency. However, the detailed quantification of the key rate comparison is beyond the scope of present study. The presented protocol will require a good spectral and temporal filtering mechanism. For spectral filtering, narrow bandwidth band pass filter has to be used. For accurate temporal filtering, a high speed

event timer has to be used with a resolution of picoseconds.

## 5.4 Conclusion

In this chapter we have proposed Coincidence Detection based BB84 quantum key distribution protocol with weak coherent pulse under restricted eavesdropping assumption set for LOS channel. We have proposed and derived an analytical expression for the secret key rate taking into account the contribution of pulses with more than one photon in the final key. We argue that by closely monitoring the number of coincidence events arising at the receiver end and matching it with the expected number of coincidences, any attempt at channel tampering can be monitored. We have also presented a security proof in support of our protocol and introduced two figures of merit to verify the security of our protocol. We have shown that this results in a higher key rate over longer distances compared to the much used decoy state protocol for the same set of parameters. We have also performed a proof-of-principle experiment to verify our predictions. The numbers obtained from the experiment agree quite well with the predicted results. One possible demerit might be the need for accurate characterization of the channel which might limit the implementation scenario to clear line of sight situations. Such a situation is mitigated by introducing extra pulses of variable intensities. Introduction of these pulses provide security like decoy state protocol [159]. The overall simpler setup is beneficial for free space lossy channel since it can achieve higher key rates over longer distances.

# Chapter 6

# Use of Non-Maximal Entangled State for Free Space BBM92 Protocol: Effect on QBER

Satellite based quantum communication for secure key distribution is becoming more demanding field due to its tight security [59, 160]. Prepare and measure protocols such as BB84 consider the satellite as a trusted device, which is fraught with danger looking at the current trend for satellite based optical communication. Therefore, entanglement based protocols must be a preferred choice since along with overcoming the distance limitation, one can take the satellite as an untrusted device [161]. E91 protocol is good candidate for satellite based quantum communication but, the key rate is very less [26, 73]. Maximum of the measured qubits are used up for checking Bell violation for security against Eve. Using entanglement based protocol requires to have maximal entangled state for more secure key distribution [162]. The current work discusses about how much non maximal entangled state one can use to have secure key distribution.

This will be more useful while using BBM92 protocol for key distribution as one can draw a straight connection between the extent of violation for Bell's inequality ($S$) and the quantum bit error rate (QBER) for a given setup.

## 6.1 Key Distribution with Non-Maximal Entangled Photon Source

With advancement in developing practical quantum computers, the demand for secure communication has increased. It has already been realized that by using Shor's quantum algorithm [13], one can break most of the encryptions used in key distribution between communicating parties [16]. Quantum Key Distribution (QKD) uses the principles of quantum mechanics to securely distribute keys between the two communicating parties [23, 26]. Moreover using QKD also ensures that the presence of Eavesdropper can be detected in real time just by observing the disturbance in the channel unlike conventional classical key distribution [41, 48, 57, 94].

Based on the usage and type of encryption there are many protocols, e.g. BB84 [23, 24], SARG04 [163], COW [131], E91 [26, 164] etc. BB84 protocol is widely used based on its ease of implementation in practice. And also the security is fool proof and theoretically robust against almost all the possible attacks by Eve [41, 73]. These protocols are robust and are easy to equip in real environment but are prone to side channel attacks [20, 96, 140] as the devices are not perfect. However, these protocols also have distance limitations as the disturbance in the channel increases with the transmission distance. To increase the transmission distance, Entanglement Based QKD (EB QKD) [94, 161] protocol can be used, one such example is Ekert Protocol (E91 protocol). The security of EB QKD protocol comes from the monogamy of entanglement [73], this tells if two parties (Alice and Bob) share maximally entangled state

then the third party has no correlation with the other two [71]. EB QKD are ideal for satellite based quantum communication as it can make two ground stations communicate securely. This can be done by sharing entangled state results as key between them that is received through satellite. There are several entangled photon sources that could be used in satellite based EB QKD [59, 160]. The only limitation of using EB QKD is the key rate, as mostly the entangled photon pairs produced are from spontaneous parametric down-conversion (SPDC) [111, 114] process that is not very efficient. In terms of security, EB QKD has advantage over prepare and measure (P&M) protocols with weak coherent pulse (WCP) used in practice. The security is ensured by checking Bell violation which makes the protocol inherently device independent. Even without checking for violation of Bell's inequality, one can still distribute secret keys if they share maximally entangled state like BBM92 protocol [34].

Even though the key rate of BB84 is higher but, it has distance and security limitation if done by WCP which is used in maximum setups. For carrying out long distance QKD, e.g., satellite communication, EB QKD protocol is more suitable as it does not require a trusted satellite. EB QKD e.g., E91 protocol is more secure compared to BB84, but for increasing the key rate most of the time one opts for BBM92 protocol. Key rate is higher in BBM92 protocol as it averts Bell's inequality measurements.

The current chapter investigates the relation between CHSH Bell's parameter $S$ and QBER including experimental imperfections in the field based QKD experiments. Here, we provide the optimum secret key rate that can be obtained from BBM92 protocol keeping the security offered by entangled photons.

## 6.2 Theoretical Background for Key Rate of EB QKD

The entanglement based QKD can be a good method for increasing the security and the distance of key distribution protocol. The standard Ekert protocol (E91) using the state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{6.1}$$

can be described as follows

- A common sender 'Charlie' sends a pair of entangled photon state $|\psi\rangle$ to Alice and Bob through quantum channel (fiber or free space).
- Alice and Bob independently make their measurements in random bases.
- The measurement bases of Alice are ({**22.5/-22.5**},{**67.5/-67.5**},{**0/90**}) where as Bob's bases are({**0/90**},{**45/-45**})
- After the measurement process both Alice and Bob declare their basis choices through the public channel.
- Alice and Bob will form the key when they choose same bases for their measurements (i.e when both of them measure in {**0/90**} basis).
- Rest of the measurement results will go for checking the CHSH Bell's parameter *S* for security of the protocol.

This protocol is secure against any eavesdropping strategy, as the security is based on the monogamy of entanglement. If maximal entangled state is used for key distribution then the Bell's parameter below $2\sqrt{2}$ (for ideal channel) will be considered as insecure for this protocol for a given channel [27, 28, 164, 165]. The drawback of this protocol

is that it has low key rate as maximum of the generated raw bits from the measurements are used for security check through violation of Bell's inequality. On practical ground, implementing this protocol can be challenging as the entanglement may degrade over the course of journey, thus reducing the Signal to Noise ratio (SNR). This might bring down the value of Bell's parameter ($S$) for a particular channel. Obtaining the value of Bell's parameter below that along with the associated QBER threshold will make the protocol abort. As even if both Alice and Bob shares entanglement, but still Eve has access to some information due to non-maximality of the source. This imperfect correlation results in information leakage to Eve for gaining access of the key.

BBM92 protocol says [34, 166] that if one has maximal entangled state then they can extract the key from it without going for Bell state analysis. The protocol is almost same as E91. The only difference is that the measuring bases of Alice and Bob are ({**0/90**},{**45/-45**}) and the key is generated when both of them measure in compatible (same) bases without checking Bell violation ($S$). The main advantage of BBM92 over E91 protocol is that the key rate becomes considerably higher as maximum number of detection results are used in building the key and very few are utilised for checking the error (QBER) and security (same as BB84 protocol). BBM92 is essentially the entangled version of BB84 protocol. The cut off error for (QBER) is same as that of BB84 protocol [94]. So, if one has maximally entangled state one can do EB QKD without using Bell's measurement [34]. We have created four entangled states using HOM (Hong Ou Mandel) interferometer [167] as show in the experiment (Figure 6.1). The aim of my work reported in this thesis work is to check the variation of $S$ with respect to QBER.

The generation of four entangled states (Bell states) using HOM has already been done [168, 169]. At the HOM dip region if one of the incoming arm is changed to

orthogonal polarization then we have the case of two distinguishable photons falling at the BS (as seen in Figure 5.1 of chapter 5). This will have four possibilities and the output state can be written as

$$|\Psi\rangle_{out} \propto \Big(\alpha_1 |H_1V_1\rangle + \alpha_2 |H_1V_2\rangle + \alpha_3 |H_2V_1\rangle + \alpha_4 |H_2V_2\rangle\Big), \tag{6.2}$$

where $\alpha_i$ are the complex amplitudes of the corresponding state. Keeping the HWP (polarization rotator) on one of the input and output arms of the HOM BS (BS in Figure 6.1(a) and 6.1(b)) one could get two possible Bell states ($|\phi\rangle^-$ & $|\psi\rangle^-$), that are

$$\begin{aligned} |\phi\rangle^- &= \frac{1}{\sqrt{2}}(|HH\rangle - |VV\rangle) \\ |\psi\rangle^- &= \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle). \end{aligned} \tag{6.3}$$

Where, $H$ & $V$ are the polarization states of the photon pairs. Creating $|\phi\rangle^+$ & $|\psi\rangle^+$ requires a $50:50$ BS (BS1 in Figure 6.1(c) and 6.1(d)) followed by a HWP on one of the output ports of it that is given by

$$\begin{aligned} |\phi\rangle^+ &= \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle) \\ |\psi\rangle^+ &= \frac{1}{\sqrt{2}}(|HV\rangle + |VH\rangle). \end{aligned} \tag{6.4}$$

The photons from the output ports of the two $50:50$ BS form the desired $|\phi\rangle^+$ or $|\psi\rangle^+$ according to the polarization rotation. Details of their preparation can be found in [169]. Figure (6.1) also shows the generation of 4 Bell sates from HOM in the Lab.

Now one gets the entangled photon source for QKD. The advantage of the following setup is that one can vary maximality of the entanglement by varying the HOM visibility. HOM Setup is also good source of producing single photon pairs. Therefore,

the multi-photon pairs generated through Spontaneous Parametric Down-conversion (SPDC) [111, 112, 114] is easily filtered out and pure two photon pairs are sent to Alice and Bob.

The standard error rate (QBER) that can be tolerated in BB84 protocol is 11% [41] against general and 14% against individual attacks [74]. Recently, it has been shown in [94] that the BBM92 protocol is bound by the same error rate for individual attacks. Therefore, by looking at the correlation between $S$ and QBER one can tell to which extent non-maximally entangled photons can be used for QKD. For perfectly secure QKD one needs maximally entangled source having maximum attainable value of $S$. As the increase in non-maximality of the system may leak information to Eve. So, by the entanglement monogamy, Eve then can have some correlation either with Alice or Bob [71]. This can also be checked directly with the formula given by [170, 171]

$$I(A:E) = H\left(\frac{1+\sqrt{S^2/4-1}}{2}\right), \tag{6.5}$$

where $I(A:E)$ is the mutual information between Alice and Eve, $H$ is the binary entropy and $S$ is the Bell's parameter. The maximum amount of information shared by Alice and Bob for BBM92 protocol is mutual information $I(A:B)$ between them, which is $I(A:B)$ between Alice and Bob that can be calculated using standard formula

$$I(A:B) = H(A) + \sum_{a\varepsilon A} p(a) \sum_{b\varepsilon B} p(b \mid a)\ Log\ p(b \mid a) \tag{6.6}$$

Where $H(A)$ is the entropy of Alice, $p(a)$ is the probability of getting a polarization (say $|H\rangle$) at Alice or Bob out of four polarization states. $p(b \mid a)$ is the probability of getting a polarization ($|V\rangle$) at Bob, given polarization ($|H\rangle$) is measured by Alice or vise versa. Experimentally This can be calculated from the coincidences detected at both ends normalised by the individual detector counts. Alternatively, one can calcu-

late $I(A:B)$ by the expression (Eq.(2.26)) already discussed in the section 2.1. Mutual information for $\{H,V\}$ and $\{D,A\}$ basis is given by

$$\begin{aligned} I(A:B)^{\{H,V\}} &= 1 - H(\delta_{HV}) \\ I(A:B)^{\{D,A\}} &= 1 - H(\delta_{DA}). \end{aligned} \tag{6.7}$$

Where $\delta_{HV}$ and $\delta_{DA}$ are QBER in $\{H,V\}$ and $\{D,A\}$ basis respectively. These values can be calculated from the experiment by looking at the coincidences between wrong photon pairs of the state. For example the coincidence between $|H\rangle$ and $|V\rangle$ polarization will give QBER for $\frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$ state. The average mutual information between Alice and Bob is then

$$I(A:B) = (I(A:B)^{\{H,V\}} + I(A:B)^{\{D,A\}})/2. \tag{6.8}$$

The final secure key rate of the protocol can be written as [43]

$$r = I(A:B) - I(A:E). \tag{6.9}$$

where $r$ is the secret key rate per symbol or bit. For extracting secure keys between Alice and Bob the key rate $(r)$ must have non zero value (i.e., $I(A:B) > I(A:E)$). $I(A:B)$ & $I(A:E)$ both vary with 'QBER' & '$S$' so, one could find out the range of '$S$' & 'QBER' which gives non zero '$r$' for secret key extraction in ideal condition. Proper modelling of free space channel can be done which helps in predicting QBER that can be matched with experimental result. Eavesdropper will use the non-maxiality to its benefit to gain the information about the key. Non maximal entangled states are generally not used for QKD as they pose threat to security. Recently, there have been several works done to show that non maximal entangled states are good for lossy channel QKD. These can serve as good candidate for EB QKD for satellite or free

space communication [162]. The effect of non maximality on QBER can be interesting to see for free space EB QKD.

## 6.3 Experimental Scheme for $S$ versus QBER Measurement

For generating entangled photon state we have used HOM interferometer [169] as this will give us good quality entangled photons. It uses two photon interference which can reduce the amount of multi-photons during entanglement generation. Figure 6.1 shows the schematics for proof of principal of the experiment.

The pump laser (coherent source) of 405nm with a non linear crystal (BBO Type-1) is used to simultaneously generate two photons by the process called spontaneous parametric down conversion (SPDC). These photon pairs with wavelength 810nm and emitted in non-colinear geometry are correlated. A Prism mirror is used to separate the pathways of signal and idler photons. They then interfere at a 50:50 BS to give $|0,2\rangle + |2,0\rangle$ state (in the number basis) at the output port of the BS. For creating the entangled state as stated in the section 6.2 the polarization of the two photons incoming at the BS is changed by placing a HWP in one of the arms after prism mirror. The two photons meeting at the BS have orthogonal polarization. The experimental scheme is shown in the Figure 6.1. In Figure 6.1 (a) and 6.1 (b) we take the case when the two photons are either transmitted or reflected from both the ports of the BS. This will give $|\psi^-\rangle$ state and $|\phi^-\rangle$ state as shown in Fig. (1b) that can be obtained by placing HWP after output port of the HOM BS.

Setup for producing $|\psi^+\rangle$ and $|\phi^+\rangle$ state is slightly different. If two photons coming out from the same output port of the BS of HOM interferometer are again

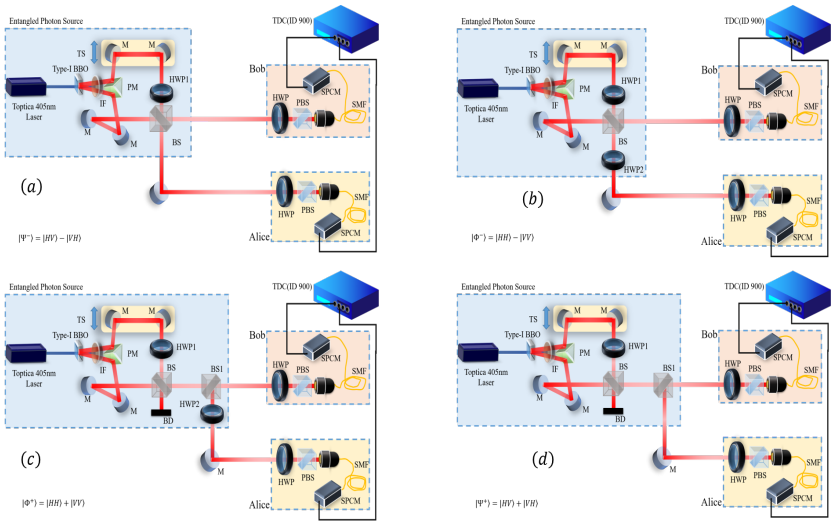



**Figure 6.1:** Experimental scheme for creating $|\psi^-\rangle$ Bell state (a) from HOM interferometer, all other states given in the rest of the figure.**BS**: Beam-Splitter, **PBS**: Polarizing Beam Splitter, **TS**: Translation Stage. **M**: Mirror, **HWP**: Half Wave Plate, **PM**: Prism mirror **SPCM**: Single Photon Counting Module, **SMF**: Single Mode Fiber **TDC**: Time to Digital-Converter.

sent to a 50:50 BS (BS1 in Fig.3). then the photons at the output ports of BS1 will give $|\psi^+\rangle$ state. If HWP is kept in one of the arms of the output ports of second BS (BS1) then $|\phi^+\rangle$ state is produced [169] which is shown in Figure 6.1(d). All the states are then measured by projecting them to different polarization states using combination of HWP and PBS which is then coupled to the single mode fiber with single photon counting module (SPCM). These can be thought as the detection setup for Alice and Bob. The coincidences from both the detectors are recorded for various polarization projections (by rotating the HWP). Coincidences in the same basis will give the key rate estimation in principle for BBM92 protocol. Coincidences in the same basis with different polarization projections in Alice and Bob's setup will give estimate for QBER. All the possible coincidences in specific HWP angle setting are recorded for Bell's violation ($S$) estimation and key rate estimation. We measured the Bell violation for each state and for different visibility settings. Visibility of HOM will give an indication of the amount of entanglement in the system which can be controlled

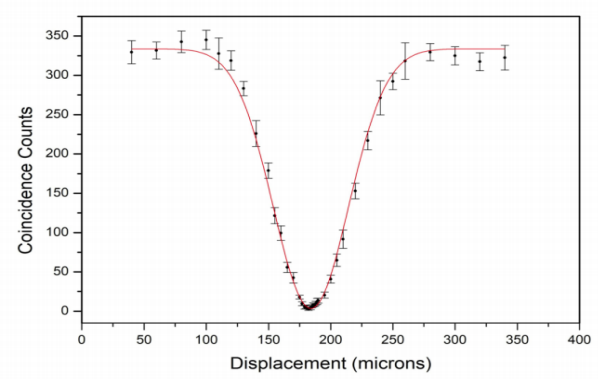



**Figure 6.2:** Graph for HOM Visibility. Coincidence counts with respect to delay of translation stage.

by the translation stage (TS). This visibility in HOM will change the coefficients of the corresponding states generated for EB QKD. With the change in the amount of entanglement (i.e change in $C_i, s$) we record the coincidences for key rate estimation. This will give indication of the variation of $S$ with QBER.

## 6.4 Results and Discussion

Experimental results show variation of Bell violation ($S$) with respect to QBER for different Bell states. It seems that Bell's parameter $S$ varies linearly with QBER with a negative slope, $S$ decreases with increase in QBER. The expression for this variation [74] for individual attacks, is known in the literature

$$S = 2\sqrt{2}(1-2\delta). \tag{6.10}$$

Considering EB QKD to be more secure in practical implementation than standard *P&M*, more general attacks can be considered, as Eq.(6.10) is valid for individual attacks and not for collective attacks. Also the error threshold for BBM92 is same as for BB84 considering only individual attacks [94]. Even though Eq.(6.10) says that the error limit is 14% but it is seen that for all the states, the value os $S$ falls below 2

for higher than 11% error. $\delta$ is the disturbance in the signal, in this case it is similar to QBER. $S$ is the most critical parameter for EB QKD. At each run if Alice and Bob have to go for Bell parameter check, then the key rate will be low. If the source is once calibrated for $S$ and the QBER at the beginning then for long run they can make sure about $S$ by observing QBER. This can be assumed for the case of satellite payload before launching into the orbit.

By the connection between $S$ and QBER one can have the indication about the purity of the source through the QBER generated instantaneously. This was earlier done only after sacrificing many key bits for finding $S$, then by looking at QBER secret key is extracted accordingly through post-processing. Therefore the present correlation between $S$ and QBER comes in handy in providing larger number of bits for same amount of raw key. This result becomes interesting as maximum of the EB QKD Protocols that have been done all assumed to have taken maximally entangled state. Maximal entanglement becomes crucial for the security of EB QKD as it ensures Eve has no data correlated to the key shared by Alice and Bob. Here, in the current work, looking at the QBER value one can tell about the value of $S$. This is crucial step to semi-device independency (measurement side) without sacrificing the key rate [73]. The results in the work can be used for doing QKD using non maximally entangled states. Which is more practical and easily implementable as during the course of time the entangled photon source may get worsen.

The graph in the Figure 6.3 shows the variation of $S$ with QBER. All the detector's inefficiencies have been taken into account while calculating QBER. The $(\eta_{det})$ (overall detector efficiency) is taken to be equal for Alice and Bob, as they are almost at the same distance to the source. The graph mainly shows how the $S$ is affected by the QBER (CHSH Bell parameter). This characterisation is important as the QBER in

the transmitting end directly indicates the condition of the entanglement. For satellite based QKD this relation can come in handy as one can verify the entanglement just by looking at the QBER, provided the initial calibration has been done.

Graph in Figure (6.3(a),(b),(c),(d)) shows that the relation is consistent with all the four types of Bell states. Through this method one can safely extract secret keys for BBM92 protocol even if the source is non-maximally entangled. As already the relation between $S$ and QBER is already known so by looking at the QBER one can make $S$ there by performing error correction and privacy amplification accordingly. Connection between $S$ and QBER gives a direct indication whether the source is being tampered or not! Earlier by looking at the QBER it was difficult to make out the value of $S$ at the same time. Therefore, separate bit string needed for Bell's parameter estimation, results in declining key rate. Use of non maximal entangled state can be useful for long distance QKD [169] For others states $|\psi\rangle^{+} = \left(C_1 |H_1V_2\rangle + C_2 |H_2V_1\rangle\right)$

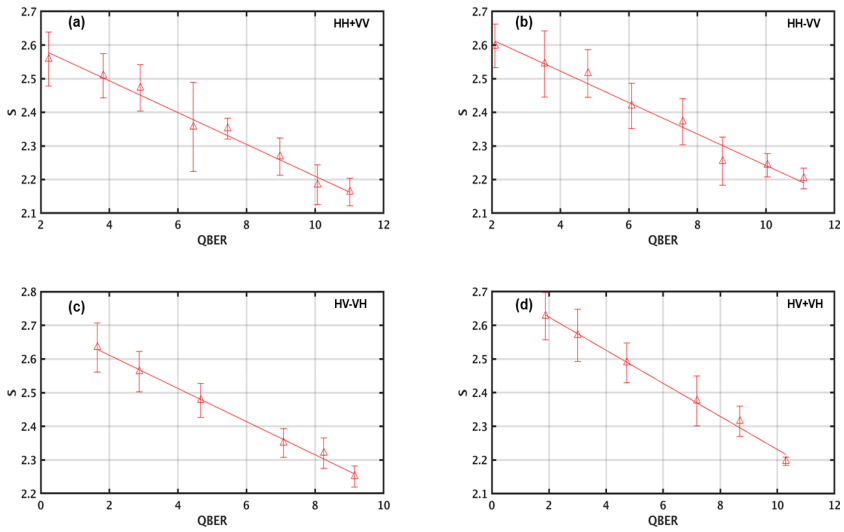



**Figure 6.3:** Variation of Bell's inequality ($S$) with QBER for all four Bell's state.

and $|\psi\rangle^{-} = \left(C_1 |H_1V_2\rangle - C_2 |H_2V_1\rangle\right)$ the variation of $S$ with QBER is shown in Figure 6.3(c) and 6.3(d) respectively. Irrespective of any Bell state, BBM92 protocol results in same error bound as BB84 protocol including implementation discrepancies. This

is interesting in a way that the result of measurement is independent of the state that we have prepared. So, for making a source for EB QKD, ease of state preparations can be thought to increase the robustness. This will not affect the variation of $S$ with QBER for a given system in the protocol.

For calculating secure key rate the difference between mutual information of Alice-Bob ($I(A:B)$) and Alice-Eve ($I(A:E)$) is taken. The key rate can be calculated from Eq.(6.9) The Plot for MI between Alice-Bob and Alice-Eve is given in Figure 6.4 This shows that non zero secure key rates are only possible for error bounds upto $\sim 4\%$. Above which even though the one has entanglement but still the secure key rate extraction won't be possible. Attack strategy by Eve is taken to be general as she uses the weakness in entanglement to gain the information about the key. In the above expression (Eq.(6.9)) for key rate $r$, it is assumed that Eve can perform any kind of attack. Eve can get the advantage as Alice and Bob are using non maximal entanglement. The information leakage is due to the fact that the states in the QKD are not perfectly entangled. Figure 6.4 (a),(b),(c) and (d) shows the secret key rate for the different Bell states in practical conditions.

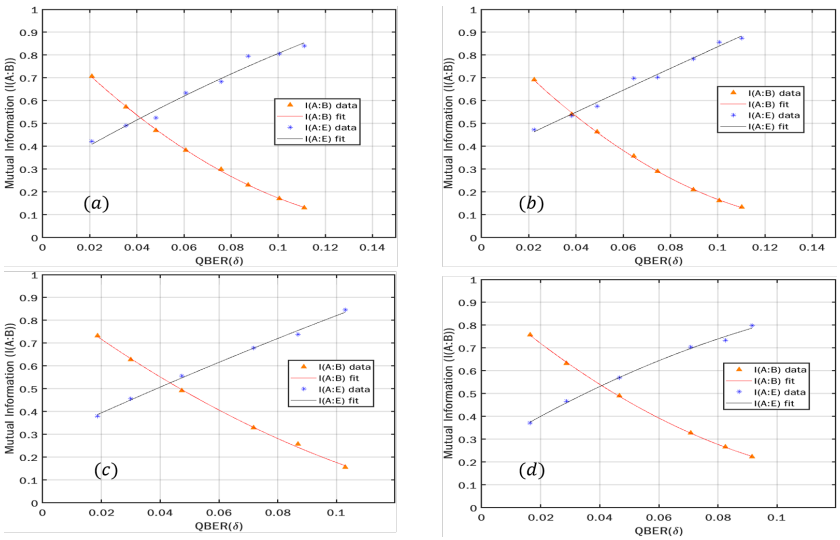



**Figure 6.4:** Secret key rate with variation in QBER and in entanglement for Bell state.

In all the figures for secure key rate, it is seen that the error bounds for getting secure key rate in BBM92 protocol is independent of the Bell states created. Practically the sender can transmit any of these states to Alice and Bob. This also gives an advantage in implementing the protocol in terms of state creation. For secure key distribution one has to go below 5% of QBER such that the protocol becomes independent of measurement apparatus. For long distance key distribution one can check the presence of Eve by monitoring QBER. This must be less than 5% for semi device independent operation which can give more security.

## 6.5 Conclusion

In the present work, we discuss about the method to improve the key rate of EB QKD protocol keeping the security intact. This can be done by using BBM92 protocol for key distribution and matching the QBER with pre-calibrated value of $S$ of the source. Thus by averting the testing of Bell's inequality violation and sacrificing the bits for ensuring secure key distribution, our method will help in increasing the key rate, since QBER itself could provide the value of CHSH parameter $S$. For the same channel transmissivity, the number of photons received at the detectors are same for both the protocols (E91 and BBM92). For BBM92 protocol, nearly 50% of the received photons will contribute to the sifted key whereas for E91 less than 50% of them will contribute to sifted key. It signifies the use of BBM92 over E91 for achieving higher key rates. If one uses highly efficient detectors or detectors with efficiency 65% or more with zero background photons, then both the protocols will have same security (detector loophole is closed). In [172] it has been shown that for low detector efficiency one can do DI QKD using non maximally entangled states, also they are more robust against atmospheric turbulence which can be beneficial for free space QKD [173]. The only assumption is that the source (entangled photon source)

is trusted, properly characterised for Bell-CHSH parameter and possible errors of the system. This assumption is valid as for satellite to ground QKD, one can do this before launching the source into the orbit. Requirement of highly efficient detectors to perform DI-QKD using non maximally entangled states is essential as it closes the detection loophole for Bell's inequality violation. In practical scenario, one can reduce the overall background (1%) and can use detector efficiency of 75% to perform DI QKD using non maximally entangled states.

Earlier works generally talk about the use of maximal entangled state for secure key distribution. The present work brings out an ease in performing satellite based QKD or free space QKD over long time without further characterizations at each run. It is seen that with change in the entanglement of the source the QBER also changes. Using the results from this study, one can derive secure key without going to Bell's inequality violation. It is also been observed in our study that having entanglement will not ensure that secure key can be extracted. The present study can be useful for doing long term QKD without routinely characterizations of the entangled source system.

# Chapter 7

# Summary

Information processing using photonic systems for quantum communication has gained massive popularity over the past few decades due to the two most unique characteristics of quantum mechanics used for cryptography - the no cloning theorem and entanglement. These properties help to ensure security of the information transfer between the communicating parties. QKD is the future of modern secret communication with the assistance of classical communication. QKD not only provides unconditional security [17, 38] but also helps in tracking the presence of eavesdropper in real time. QKD works better against conventional cryptography as it provides information theoretic security rather than being based on computational hardness of the system [11, 23]. This point is crucial to prevent any attack or information leakage during communication. For performing QKD one has to either build an ideal single photon source or bright entangled photon source. Both of which are still are subjects of research work [96]. Alternatively, one can use WCP but, it opens up several security loopholes in terms of implementation for free space QKD [48, 81]. Some of which has been discussed in this thesis with possible remedies to close them. Similarly, for entanglement based

QKD one requires maximally entangled source for secure communication. Possible methods have been suggested for secure communication with non maximal entangled source in this thesis work.

In chapter 2 and 3 we have mainly discussed about the standard techniques used for finding out secret key rates and QBER for practical scenarios. Chapter 2 deals with the theoretical frame work for proving security of BB84 and BBM92 protocols in ideal and real situations. How the key rate gets modified due to physical imperfections in the source and the detectors have also been elaborated in detail. These expressions can be used for calculating the key rate for QKD setup while implementing in the field. Chapter 3 discusses about the experimental techniques starting from developing the laser driver circuits and making RNG from FPGA to the optical design. This chapter talks about the various challenges one can face during building the setup for field experiments and to counter them through various post processing techniques.

While implementing the BB84 protocol, unavailability of ideal single photon source (SPS), can lead to security loophole. The possible parameters at the source end which can lead to information leakage to the third party is discussed in chapter 4. The information leakage due to these parameters occurs mainly due to experimental imperfections. We have characterized the various source parameters that can lead to possible side channel attack. Using cross correlation function for calculating mutual information between Alice and Eve gives quite good results. The mutual information for most of the parameters comes to be in the order of ($\sim 10^{-3}$ bits/pulse).

In chapter 5, we have discussed the method to increase the key rate using WCP with multi-photons. Previously, all the key extraction procedures used to include the contribution due to the single photons only, for removing the possibility of PNS attack [48, 54]. We have proposed Coincidence Detection based BB84 quantum key distribu-

tion protocol with weak coherent pulses under restricted eavesdropping assumption set for LOS channel. We have derived an analytical expression for the secret key rate taking into account the contribution of pulses with more than one photon in the final key. We argue that by closely monitoring the number of coincidence events arising at the receiver end and matching it with the expected number of coincidences, any attempt at channel tampering can be monitored.

In chapter 6, possible method to increase the key rate without compromising the security of EB QKD has been talked about. We have discussed the method to improve the key rate of EB QKD protocol keeping the security intact. This is done by using BBM92 protocol for key distribution and matching the QBER with pre-calibrated value of Bell parametr $S$ of the source. Involving Bell's inequality violation $S$ for checking security decreases the key rate. For our work, it is seen that for a given channel, one can get the hint of $S$ from QBER once they calibrate the source. This method can be used for semi-DI QKD which are more secure than standard BB84 and BBM92 protocol where both source and detector need to be characterized. The connection between $S$ and QBER also ensures that one can use non maximal entangled photon source for EB QKD. Non maximal states are good when it comes to free space communication in turbulent atmosphere.

## Scope for Future Work

In my thesis, we have studied mainly two protocols, BB84, and BBM92 QKD protocols. With BB84, we have characterized the source on different parameters e.g., wavelength, pulse width, spatial mode, polarization error, etc. Mismatch in these parameters gives Eve the advantage of gaining information about the source. This mismatch can be rectified if one properly characterizes the source for the errors due to

imperfections. Later they can be filtered out in the EC and PA part of the key extraction protocol. For robust security against side-channel attacks, one has to do detector characterizations similar to source characterization. For long-distance transmission, one has to look for the information leakage due to spatial mode at the detector end [174]. We will see that whether information leakage due to spatial mode can be decreased by using beam structures other than Gaussian.

In chapter 5, we have investigated how we can increase the key rate of BB84 protocol for free space QKD. The full rigorous security proof in terms of mutual information is required to relax some of the assumptions for LOS and use it in fiber-based QKD. Recently there has been studies on finding countermeasures against detector blinding attack [64]. The coincidence detection method can come into help by providing a way to check detector blinding attack [175, 176]. This can be interesting as it can be done within the existing setup unlike in [175] which requires multi-pixel detectors.

Increasing the key rate for entanglement-based (EB) protocols has been a topic of modern research [73]. BBM92 protocol can be a good candidate for this but using polarization degree of freedom has its own limitations.The orbital angular momentum (OAM) degree of freedom could be more robust and a higher key rate with EB QKD. OAM can be useful against turbulent atmosphere for free space communication [ref-shashi]. Though there has been work done in the field of OAM based QKD [52] but, the key rate is limited by the refresh rate of SLMs (Spatial Light Modulators). One can increase this key rate through OAM sorting technique [177] which we will be using for OAM based EB QKD.

# Bibliography


[1] S. Aaronson, *Quantum computing since Democritus* (Cambridge University Press, 2013).

[2] S. Singh, *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography* (Doubleday, USA, 1999), 1st ed.

[3] C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners* (Springer Publishing Company, Incorporated, 2009), 1st ed.

[4] D. R. Stinson, *Cryptography: theory and practice* (Chapman and Hall/CRC, 2005).

[5] D. Boneh and V. Shoup, *A graduate course in applied cryptography,* (2020).

[6] H. Feistel, W. Notz, and J. Smith, *Some cryptographic techniques for machine-to-machine data communications,* Proceedings of the IEEE **63**, 1545–1554 (1975).

[7] C. E. Shannon, *Communication theory of secrecy systems,* The Bell System Technical Journal **28**, 656–715 (1949).

[8] A. Biryukov and D. Khovratovich, *Related-key cryptanalysis of the full aes-192 and aes-256,* Cryptology ePrint Archive, Report 2009/317 (2009). https://ia.cr/2009/317.

[9] W. Diffie and M. Hellman, *New directions in cryptography,* IEEE Transactions on Information Theory **22**, 644–654 (1976).

[10] R. L. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems,* Commun. ACM **21**, 120–126 (1978).

[11] M. A. Nielsen and I. Chuang, *Quantum computation and quantum information,* (2002).

[12] A. Calderbank, E. Rains, P. Shor, and N. Sloane, *Quantum error correction via codes over gf(4),* IEEE Transactions on Information Theory **44**, 1369–1387 (1998).

[13] P. W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,* SIAM Journal on Computing **26**, 1484–1509 (1997).

[14] C.-Y. Lu, D. E. Browne, T. Yang, and J.-W. Pan, *Demonstration of a compiled version of shor's quantum factoring algorithm using photonic qubits,* Phys. Rev. Lett. **99**, 250504 (2007).

[15] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, *Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance,* Nature **414**, 883–887 (2001).

[16] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Quantum cryptography,* Rev. Mod. Phys. **74**, 145–195 (2002).

[17] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, *Secure quantum key distribution with realistic devices,* Rev. Mod. Phys. **92**, 025002 (2020).

[18] S. Wiesner, *Conjugate coding,* ACM Sigact News **15**, 78–88 (1983).

[19] A. Molina, T. Vidick, and J. Watrous, *Optimal counterfeiting attacks and generalizations for wiesner's quantum money,* in "Theory of Quantum Computation, Communication, and Cryptography," , K. Iwama, Y. Kawano, and M. Murao, eds. (Springer Berlin Heidelberg, Berlin, Heidelberg, 2013), pp. 45–64.

[20] N. Lütkenhaus, *Security against individual attacks for realistic quantum key distribution,* Physical Review A **61**, 052304 (2000).

[21] M. HAYASHI, *QUANTUM INFORMATION THEORY: Mathematical Foundation* (SPRINGER, 2018).

[22] C. Kollmitzer and M. Pivk, *Applied quantum cryptography*, vol. 797 (Springer, 2010).

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

[24] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, *Experimental quantum cryptography,* Journal of cryptology **5**, 3–28 (1992).

[25] C. H. Bennett, *Quantum cryptography using any two nonorthogonal states,* Phys. Rev. Lett. **68**, 3121–3124 (1992).

[26] A. K. Ekert, *Quantum cryptography based on bell's theorem,* Phys. Rev. Lett. **67**, 661–663 (1991).

[27] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Proposed experiment to test local hidden-variable theories,* Physical review letters **23**, 880 (1969).

[28] J. F. Clauser and M. A. Horne, *Experimental consequences of objective local theories,* Physical review D **10**, 526 (1974).

[29] J. S. Bell, *On the einstein podolsky rosen paradox,* Physics Physique Fizika **1**, 195 (1964).

[30] A. Aspect, J. Dalibard, and G. Roger, *Experimental test of bell's inequalities using time-varying analyzers,* Physical review letters **49**, 1804 (1982).

[31] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, *Quantum privacy amplification and the security of quantum cryptography over noisy channels,* Phys. Rev. Lett. **77**, 2818–2821 (1996).

[32] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, *Concentrating partial entanglement by local operations,* Phys. Rev. A **53**, 2046–2052 (1996).

[33] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, *Mixed-state entanglement and quantum error correction,* Phys. Rev. A **54**, 3824–3851 (1996).

[34] C. H. Bennett, *Quantum cryptography using any two nonorthogonal states,* Physical review letters **68**, 3121 (1992).

[35] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, *Air-to-ground quantum communication,* Nature Photonics **7**, 382–386 (2013).

[36] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan, *Satellite-relayed intercontinental quantum network,* Phys. Rev. Lett. **120**, 030501 (2018).

[37] R. RENNER, *Security of quantum key distribution,* International Journal of Quantum Information **06**, 1–127 (2008).

[38] N. Lütkenhaus, *Estimates for practical quantum cryptography,* Physical Review A **59**, 3301 (1999).

[39] D. Mayers, *Quantum key distribution and string oblivious transfer in noisy channels,* in "Annual International Cryptology Conference," (Springer, 1996), pp. 343–357.

[40] H.-K. Lo and H. F. Chau, *Unconditional security of quantum key distribution over arbitrarily long distances,* Science **283**, 2050–2056 (1999).

[41] P. W. Shor and J. Preskill, *Simple proof of security of the bb84 quantum key distribution protocol,* Phys. Rev. Lett. **85**, 441–444 (2000).

[42] M. Koashi and J. Preskill, *Secure quantum key distribution with an uncharacterized source,* Phys. Rev. Lett. **90**, 057902 (2003).

[43] I. Devetak and A. Winter, *Distillation of secret key and entanglement from quantum states,* Proceedings of the Royal Society A: Mathematical, Physical and engineering sciences **461**, 207–235 (2005).

[44] R. König, R. Renner, A. Bariska, and U. Maurer, *Small accessible quantum information does not imply security,* Phys. Rev. Lett. **98**, 140502 (2007).

[45] R. Renner and R. König, *Universally composable privacy amplification against quantum adversaries,* in "Theory of Cryptography," , J. Kilian, ed. (Springer Berlin Heidelberg, Berlin, Heidelberg, 2005), pp. 407–425.

[46] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, *Tight finite-key analysis for quantum cryptography,* Nature Communications **3**, 634 (2012).

[47] H. Inamori, N. Lütkenhaus, and D. Mayers, *Unconditional security of practical quantum key distribution,* The European Physical Journal D **41**, 599–627 (2007).

[48] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, *Security of quantum key distribution with imperfect devices,* in "International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.", (IEEE, 2004), p. 136.

[49] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, *Fast and simple one-way quantum key distribution,* Applied Physics Letters **87**, 194108 (2005).

[50] K. Inoue, E. Waks, and Y. Yamamoto, *Differential phase shift quantum key distribution,* Phys. Rev. Lett. **89**, 037902 (2002).

[51] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, *Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations,* Phys. Rev. Lett. **92**, 057901 (2004).

[52] A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B. Heim *et al.*, *High-dimensional intracity quantum cryptography with structured photons,* Optica **4**, 1006–1010 (2017).

[53] N. Walenta, A. Burg, D. Caselunghe, J. Constantin, N. Gisin, O. Guinnard, R. Houlmann, P. Junod, B. Korzh, N. Kulesza *et al.*, *A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing,* New Journal of Physics **16**, 013047 (2014).

[54] W.-Y. Hwang, *Quantum key distribution with high loss: toward global secure communication,* Physical Review Letters **91**, 057901 (2003).

[55] X.-B. Wang, *Beating the photon-number-splitting attack in practical quantum cryptography,* Physical review letters **94**, 230503 (2005).

[56] H.-K. Lo, X. Ma, and K. Chen, *Decoy state quantum key distribution,* Physical review letters **94**, 230504 (2005).

[57] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, *Overcoming the rate–distance limit of quantum key distribution without quantum repeaters,* Nature **557**, 400–403 (2018).

[58] H.-K. Lo, M. Curty, and K. Tamaki, *Secure quantum key distribution,* Nature Photonics **8**, 595–604 (2014).

[59] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li *et al.*, *Satellite-to-ground quantum key distribution,* Nature **549**, 43–47 (2017).

[60] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity *et al.*, *Experimental demonstration of free-space decoy-state quantum key distribution over 144 km,* Physical Review Letters **98**, 010504 (2007).

[61] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, M.-J. Li, H. Chen, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, *Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km,* Phys. Rev. Lett. **124**, 070501 (2020).

[62] M. Lucamarini, K. Patel, J. Dynes, B. Fröhlich, A. Sharpe, A. Dixon, Z. Yuan, R. Penty, and A. Shields, *Efficient decoy-state quantum key distribution with quantified security,* Optics express **21**, 24550–24565 (2013).

[63] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, *Provably secure*

*and high-rate quantum key distribution with time-bin qudits,* Science advances **3**, e1701491 (2017).

[64] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, *Hacking commercial quantum cryptography systems by tailored bright illumination,* Nature photonics **4**, 686–689 (2010).

[65] N. Lütkenhaus and M. Jahma, *Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack,* New Journal of Physics **4**, 44 (2002).

[66] C. E. Shannon, *A mathematical theory of communication,* The Bell System Technical Journal **27**, 379–423 (1948).

[67] G. S. Vernam, *Cipher printing telegraph systems: For secret wire and radio telegraphic communications,* Journal of the AIEE **45**, 109–115 (1926).

[68] N. Lütkenhaus, *Security against eavesdropping in quantum cryptography,* Physical Review A **54**, 97 (1996).

[69] W. K. Wootters and W. H. Zurek, *A single quantum cannot be cloned,* Nature **299**, 802–803 (1982).

[70] W. Heisenberg, *Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik,* in "Original Scientific Papers Wissenschaftliche Originalarbeiten," (Springer, 1985), pp. 478–504.

[71] V. Coffman, J. Kundu, and W. K. Wootters, *Distributed entanglement,* Phys. Rev. A **61**, 052306 (2000).

[72] D. Mayers, *Unconditional security in quantum cryptography,* Journal of the ACM (JACM) **48**, 351–406 (2001).

[73] 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. **12**, 1012–1236 (2020).

[74] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, *Optimal eavesdropping in quantum cryptography. i. information bound and optimal strategy,* Physical Review A **56**, 1163 (1997).

[75] S. Pirandola, *Symmetric collective attacks for the eavesdropping of symmetric quantum key distribution,* International Journal of Quantum Information **6**, 765–771 (2008).

[76] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, *Quantum cryptography, or unforgeable subway tokens,* in "Advances in Cryptology," (Springer, 1983), pp. 267–275.

[77] T. M. Cover and J. A. Thomas, *Elements of information theory second edition solutions to problems,* Internet Access pp. 19–20 (2006).

[78] S. M. Moser and P.-N. Chen, *A student's guide to coding and information theory* (Cambridge University Press, 2012).

[79] D. J. MacKay and D. J. Mac Kay, *Information theory, inference and learning algorithms* (Cambridge university press, 2003).

[80] A. S. Holevo, *Bounds for the quantity of information transmitted by a quantum communication channel,* Problemy Peredachi Informatsii **9**, 3–11 (1973).

[81] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, *Limitations on practical quantum cryptography,* Physical review letters **85**, 1330 (2000).

[82] C. A. Fuchs and A. Peres, *Quantum-state disturbance versus information gain: Uncertainty relations for quantum information,* Physical Review A **53**, 2038 (1996).

[83] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *The security of practical quantum key distribution,* Reviews of modern physics **81**, 1301 (2009).

[84] A. Peres, *Quantum theory: concepts and methods*, vol. 57 (Springer Science & Business Media, 2006).

[85] R. J. Glauber, *The quantum theory of optical coherence,* Physical Review **130**, 2529 (1963).

[86] R. J. Glauber, *Photon correlations,* Physical Review Letters **10**, 84 (1963).

[87] E. Sudarshan, *Equivalence of semiclassical and quantum mechanical descriptions of statistical light beams,* Physical Review Letters **10**, 277 (1963).

[88] R. J. Glauber, *Coherent and incoherent states of the radiation field,* Physical Review **131**, 2766 (1963).

[89] H.-K. Lo and J. Preskill, *Security of quantum key distribution using weak coherent states with nonrandom phases,* Quantum Info. Comput. **7**, 431–458 (2007).

[90] R. W. Hamming, *Error detecting and error correcting codes,* The Bell System Technical Journal **29**, 147–160 (1950).

[91] S. Roman, *Coding and Information Theory* (Springer-Verlag, Berlin, Heidelberg, 1992).

[92] C. H. Bennett, G. Brassard, and J.-M. Robert, *Privacy amplification by public discussion,* SIAM journal on Computing **17**, 210–229 (1988).

[93] D. Mayers, *Shor and preskill's and mayers's security proof for the bb84 quantum key distribution protocol,* The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics **18**, 161–170 (2002).

[94] E. Waks, A. Zeevi, and Y. Yamamoto, *Security of quantum key distribution with entangled photons against individual attacks,* Phys. Rev. A **65**, 052310 (2002).

[95] K. Takemoto, Y. Nambu, T. Miyazawa, K. Wakui, S. Hirose, T. Usuki, M. Takatsu, N. Yokoyama, K. Yoshino, A. Tomita *et al.*, *Transmission experiment of quantum keys over 50 km using high-performance quantum-dot single-photon source at 1.5 $\mu m$ wavelength,* Applied Physics Express **3**, 092802 (2010).

[96] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, *Practical challenges in quantum key distribution,* npj Quantum Information **2**, 1–12 (2016).

[97] N. Lal, A. Banerji, A. Biswas, A. Anwar, and R. Singh, *Photon statistics of twisted heralded single photons,* Journal of Modern Optics **67**, 126–132 (2020).

[98] A. Divochiy, F. Marsili, D. Bitauld, A. Gaggero, R. Leoni, F. Mattioli, A. Korneev, V. Seleznev, N. Kaurova, O. Minaeva *et al.*, *Superconducting nanowire photon-number-resolving detector at telecommunication wavelengths,* Nature Photonics **2**, 302–306 (2008).

[99] N. Lütkenhaus and A. Shields, *Focus on quantum cryptography: theory and practice,* New Journal of Physics **11**, 045005 (2009).

[100] S. D. Brown, R. J. Francis, J. Rose, and Z. G. Vranesic, *Field-programmable gate arrays*, vol. 180 (Springer Science & Business Media, 1992).

[101] U. Jetzek, *Galois Fields, Linear Feedback Shift Registers and Their Applications* (Carl Hanser Verlag GmbH Co KG, 2018).

[102] A. Poorghanad, A. Sadr, and A. Kashanipour, *Generating high quality pseudo random number using evolutionary methods,* in "2008 International Conference on Computational Intelligence and Security," , vol. 1 (IEEE, 2008), vol. 1, pp. 331–335.

[103] E. Barkan, E. Biham, and N. Keller, *Instant ciphertext-only cryptanalysis of gsm encrypted communication,* in "Annual international cryptology conference," (Springer, 2003), pp. 600–616.

[104] W. Uhring, C.-V. Zint, and J. Bartringer, *A low-cost high-repetition-rate picosecond laser diode pulse generator,* in "Semiconductor lasers and laser dynamics," , vol. 5452 (International Society for Optics and Photonics, 2004), vol. 5452, pp. 583–590.

[105] A. Biswas, A. Banerji, P. Chandravanshi, R. Kumar, and R. P. Singh, *Experimental side channel analysis of bb84 qkd source,* IEEE Journal of Quantum Electronics **57**, 1–7 (2021).

[106] 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 **11**, 065001 (2009).

[107] M. Curty, X. Ma, H.-K. Lo, and N. Lütkenhaus, *Passive sources for the bennett-brassard 1984 quantum-key-distribution protocol with practical signals,* Physical Review A **82**, 052325 (2010).

[108] C. Gerry and P. Knight, *Quantum optics,* (2000).

[109] *Quantum key distribution (qkd); component characterization: characterizing optical components for qkd systems,* ETSI GS QKD 011 V1.1.1 (2016-05) (2016).

[110] M. Kumazawa, T. Sasaki, and M. Koashi, *Rigorous characterization method for photon-number statistics,* Optics express **27**, 5297–5313 (2019).

[111] L. Mandel and E. Wolf, *Optical coherence and quantum optics* (Cambridge university press, 1995).

[112] S. E. Harris, M. K. Oshman, and R. L. Byer, *Observation of tunable optical parametric fluorescence,* Phys. Rev. Lett. **18**, 732–734 (1967).

[113] B. Mollow and R. Glauber, *Quantum theory of parametric amplification. i,* Physical Review **160**, 1076 (1967).

[114] G. S. Agarwal, *Quantum optics* (Cambridge University Press, 2012).

[115] S. Karan, S. Aarav, H. Bharadhwaj, L. Taneja, A. De, G. Kulkarni, N. Meher, and A. K. Jha, *Phase matching in $\beta$-barium borate crystals for spontaneous parametric down-conversion,* Journal of Optics **22**, 083501 (2020).

[116] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, *New high-intensity source of polarization-entangled photon pairs,* Phys. Rev. Lett. **75**, 4337–4341 (1995).

[117] M. Jabir and G. Samanta, *Robust, high brightness, degenerate entangled photon source at room temperature,* Scientific Reports **7**, 1–8 (2017).

[118] M. M. Wilde, *Quantum information theory* (Cambridge University Press, 2013).

[119] J. Goodman, *Introduction to Fourier Optics* (MaGraw-Hill, 1996), 2nd ed.

[120] E. Hecht, *Optics* (Addison-Wesley, 1998), 4th ed.

[121] E. Knill, R. Laflamme, and G. J. Milburn, *A scheme for efficient quantum computation with linear optics,* nature **409**, 46–52 (2001).

[122] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, *A fast and compact quantum random number generator,* Review of Scientific Instruments **71**, 1675–1680 (2000).

[123] T. F. Da Silva, G. B. Xavier, and J. P. Von Der Weid, *Real-time characterization of gated-mode single-photon detectors,* IEEE Journal of Quantum Electronics **47**, 1251–1256 (2011).

[124] A. Yoshizawa, R. Kaji, and H. Tsuchida, *Quantum efficiency evaluation method for gated-mode single-photon detector,* Electronics Letters **38**, 1468–1469 (2002).

[125] J. Millman and C. C. Halkias, *Integrated electronics: analog and digital circuits and systems,* Tata McGraw-Hill Education: New Delhi **44**, 45 (1972).

[126] B. P. Lathi and R. A. Green, *Signal processing and linear systems* (Oxford University Press New York, 1998).

[127] A. Shokrollahi, *Ldpc codes: An introduction,* in "Coding, cryptography and combinatorics," (Springer, 2004), pp. 85–110.

[128] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, *Generalized privacy amplification,* IEEE Transactions on Information theory **41**, 1915–1923 (1995).

[129] W. H. Press, S. A. Teukolsky, W. T. Vetterling, and B. P. Flannery, *Numerical Recipes 3rd Edition: The Art of Scientific Computing* (Cambridge University Press, USA, 2007), 3rd ed.

[130] M. Stewart, *A superfast toeplitz solver with improved numerical stability,* SIAM journal on matrix analysis and applications **25**, 669–693 (2003).

[131] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. Towery, and S. Ten, *High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres,* New Journal of Physics **11**, 075003 (2009).

[132] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, *Risk analysis of trojan-horse attacks on practical quantum key distribution systems,* IEEE Journal of Selected Topics in Quantum Electronics **21**, 168–177 (2014).

[133] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, *Trojan-horse attacks threaten the security of practical quantum cryptography,* New Journal of Physics **16**, 123030 (2014).

[134] A. Huang, S. Barz, E. Andersson, and V. Makarov, *Implementation vulnerabilities in general quantum cryptography,* New Journal of Physics **20**, 103016 (2018).

[135] A. Shenoy-Hejamadi, A. Pathak, and S. Radhakrishna, *Quantum cryptography: key distribution and beyond,* Quanta **6**, 1–47 (2017).

[136] H.-K. Lo, M. Curty, and B. Qi, *Measurement-device-independent quantum key distribution,* Physical review letters **108**, 130503 (2012).

[137] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You *et al.*, *Measurement-device-independent quantum key distribution over untrustful metropolitan network,* Physical Review X **6**, 011024 (2016).

[138] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang *et al.*, *Measurement-device-independent quantum key distribution over a 404 km optical fiber,* Physical review letters **117**, 190501 (2016).

[139] H.-L. Yin and Z.-B. Chen, *Coherent-state-based twin-field quantum key distribution,* Scientific reports **9**, 1–7 (2019).

[140] H. Ko, B.-S. Choi, J.-S. Choe, K.-J. Kim, J.-H. Kim, and C. J. Youn, *Critical side channel effects in random bit generation with multiple semiconductor lasers in a polarization-based quantum key distribution system,* Optics express **25**, 20045–20055 (2017).

[141] U. Vazirani and T. Vidick, *Erratum: Fully device-independent quantum key distribution [phys. rev. lett. 113, 140501 (2014)],* Physical review letters **116**, 089901 (2016).

[142] 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 **57**, 366–387 (2016).

[143] S. Sajeed, P. Chaiwongkhot, A. Huang, H. Qin, V. Egorov, A. Kozubov, A. Gaidash, V. Chistiakov, A. Vasiliev, A. Gleim *et al.*, *An approach for security evaluation and certification of a complete quantum communication system,* Scientific Reports **11**, 1–16 (2021).

[144] L. Rabiner and R. Schafer, *Theory and applications of digital speech processing* (Prentice Hall Press, 2010).

[145] S. G. Reddy, S. Prabhakar, A. Aadhi, A. Kumar, M. Shah, R. Singh, and R. Simon, *Measuring the mueller matrix of an arbitrary optical element with a universal su (2) polarization gadget,* JOSA A **31**, 610–615 (2014).

[146] A. Lamas-Linares and C. Kurtsiefer, *Breaking a quantum key distribution system through a timing side channel,* Optics express **15**, 9388–9393 (2007).

[147] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, *Air-to-ground quantum communication,* Nature Photonics **7**, 382–386 (2013).

[148] 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 **48**, 2023–2038 (2001).

[149] F. Xu, B. Qi, and H.-K. Lo, *Experimental demonstration of phase-remapping attack in a practical quantum key distribution system,* New Journal of Physics **12**, 113026 (2010).

[150] S. Félix, N. Gisin, A. Stefanov, and H. Zbinden, *Faint laser quantum key distribution: Eavesdropping exploiting multiphoton pulses,* Journal of Modern Optics **48**, 2009–2021 (2001).

[151] K. Tamaki and H.-K. Lo, *Unconditionally secure key distillation from multiphotons,* Physical Review A **73**, 010302 (2006).

[152] M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M. J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, and A. Forbes, *Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases,* Physical Review A **88**, 032305 (2013).

[153] A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, *High-dimensional intracity quantum cryptography with structured photons,* Optica **4**, 1006–1010 (2017).

[154] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li *et al.*, *Secure quantum key distribution over 421 km of optical fiber,* Physical review letters **121**, 190502 (2018).

[155] A. Dixon, J. Dynes, M. Lucamarini, B. Fröhlich, A. Sharpe, A. Plews, S. Tam, Z. Yuan, Y. Tanizawa, H. Sato *et al.*, *High speed prototype quantum key distribution system and long term field trial,* Optics express **23**, 7583–7592 (2015).

[156] H. Endo, M. Fujiwara, M. Kitamura, O. Tsuzuki, R. Shimizu, M. Takeoka, and M. Sasaki, *Group key agreement over free-space optical links,* OSA Continuum **3**, 2525–2543 (2020).

[157] Y. Chu, R. Donaldson, R. Kumar, and D. Grace, *Feasibility of quantum key distribution from high altitude platforms,* Quantum Science and Technology (2021).

[158] S. Isaac, A. Conrad, T. Rezaei, D. Sanchez-Rosales, R. Cochran, A. Gutha, D. Gauthier, and P. Kwiat, *Drone-based quantum key distribution,* in "2021 Conference on Lasers and Electro-Optics (CLEO)," (IEEE, 2021), pp. 1–2.

[159] M. Lucamarini, J. F. Dynes, B. Fröhlich, Z. Yuan, and A. J. Shields, *Security bounds for efficient decoy-state quantum key distribution,* IEEE Journal of Selected Topics in Quantum Electronics **21**, 197–204 (2015).

[160] A. Villar, A. Lohrmann, X. Bai, T. Vergoossen, R. Bedington, C. Perumangatt, H. Y. Lim, T. Islam, A. Reezwana, Z. Tang *et al.*, *Entanglement demonstration on board a nano-satellite,* Optica **7**, 734–737 (2020).

[161] A. Khalique and B. C. Sanders, *Long-distance quantum communication through any number of entanglement-swapping operations,* Physical Review A **90**, 032304 (2014).

[162] P. Xue, C.-F. Li, and G.-C. Guo, *Efficient quantum-key-distribution scheme with nonmaximally entangled states,* Physical Review A **64**, 032305 (2001).

[163] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, *Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations,* Physical review letters **92**, 057901 (2004).

[164] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, *Quantum cryptography with entangled photons,* Physical review letters **84**, 4729 (2000).

[165] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek *et al.*, *Entanglement-based quantum communication over 144 km,* Nature physics **3**, 481–486 (2007).

[166] M. P. Peloso, I. Gerhardt, C. Ho, A. Lamas-Linares, and C. Kurtsiefer, *Daylight operation of a free space, entanglement-based quantum key distribution system,* New Journal of Physics **11**, 045007 (2009).

[167] C. K. Hong, Z. Y. Ou, and L. Mandel, *Measurement of subpicosecond time intervals between two photons by interference,* Phys. Rev. Lett. **59**, 2044–2046 (1987).

[168] S. Prabhakar, T. Shields, A. C. Dada, M. Ebrahim, G. G. Taylor, D. Morozov, K. Erotokritou, S. Miki, M. Yabuno, H. Terai *et al.*, *Two-photon quantum interference and entanglement at 2.1 $\mu$m,* Science advances **6**, eaay5195 (2020).

[169] F. Bouchard, A. Sit, Y. Zhang, R. Fickler, F. M. Miatto, Y. Yao, F. Sciarrino, and E. Karimi, *Two photon interference: the hong-ou-mandel effect,* Reports on Progress in Physics (2020).

[170] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, *Device-independent security of quantum cryptography against collective attacks,* Physical Review Letters **98**, 230501 (2007).

[171] M. Fujiwara, K.-i. Yoshino, Y. Nambu, T. Yamashita, S. Miki, H. Terai, Z. Wang, M. Toyoshima, A. Tomita, and M. Sasaki, *Modified e91 protocol demonstration with hybrid entanglement photon source,* Optics express **22**, 13616–13624 (2014).

[172] P. H. Eberhard, *Background level and counter efficiencies required for a loophole-free einstein-podolsky-rosen experiment,* Physical Review A **47**, R747 (1993).

[173] T. Brünner and F. S. Roux, *Robust entangled qutrit states in atmospheric turbulence,* New Journal of Physics **15**, 063005 (2013).

[174] 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,* Physical Review A **91**, 062301 (2015).

[175] G. Gras, D. Rusca, H. Zbinden, and F. Bussières, *Countermeasure against quantum hacking using detection statistics,* Physical Review Applied **15**, 034052 (2021).

[176] A. Biswas, A. Banerji, N. Lal, P. Chandravanshi, R. Kumar, and R. P. Singh, *Quantum key distribution with multiphoton pulses: An advantage,* arXiv preprint arXiv:2008.07166 (2020).

[177] C. Perumangatt, N. Lal, A. Anwar, S. G. Reddy, and R. Singh, *Quantum information with even and odd states of orbital angular momentum of light,* Physics Letters A **381**, 1858–1865 (2017).

# List of Publications

## Thesis related Publications

1. **Ayan Biswas**, Anindya Banerji, Pooja Chandravanshi, Rupesh 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, Dec. 2021*, Art no. 8000207, doi: 10.1109/JQE.2021.3111332.

2. **Ayan Biswas**, Anindya Banerji, Pooja Chandravanshi, Rupesh Kumar and R. P. Singh, "Quantum key distribution with multiphoton pulses: An advantage", *OSA Continuum 2021 (accepted).*

3. **Ayan Biswas**, Sarika Mishra, Satyajeet Patil, Anindya Banerji and R. P. Singh,"Use of Non Maximal entangled state for free space BBM92 quantum key distribution protocol" *(under preparation)*.

## Conference Papers

4. **Ayan Biswas**, Nijil Lal, Anindya Banerji, and R. P. Singh, "Entanglement Duality Assisted Secure Key Distribution", *Frontiers in Optics/Laser Science 2020 (online)*, paper **JTu1A. 48**.

5. **Ayan Biswas**, Anindya Banerji, Nijil Lal, Pooja Chandravanshi, and R. P. Singh, "Coincidence detection based quantum key distribution protocol", *OSA Quantum 2.0 Con- ference 2020 (online)*, paper **QTu8B. 17**.

## Other Publications

6. Nijil Lal, Anindya Banerji, **Ayan Biswas**, Ali Anwar and R. P. Singh, "Photon statistics of twisted heralded single photons", *Journal of Modern Optics,vol. 67, no. 2, pp. 126-132, (2020).*

7. Sarika Mishra, **Ayan Biswas**, Satyajeet Patil, Pooja Chandravanshi, Vardaan Mongia, Tanya Sharma, Anju Rani, Shashi Prabhakar, Ravindra P. Singh, "BBM92 quantum key distribution over a free space dusty channel of 200 meters", *arXiv:2112.11961.*