On The Observables Analysis Of BB84 Photonic Encodings

By

Unish Subba
(067/MSICE/619)

Submitted To
The Department of Electronics and Computer Engineering
Institute of Engineering, Pulchowk Campus
Tribhuwan University
Pulchowk, Lalitpur, Nepal

April 2, 2014

On The Observables Analysis Of BB84 Photonic Encodings

By

Unish Subba
(067/MSICE/619)

A thesis proposal submitted in partial fulfillment of the requirements for the degree of
Master of Science in Information and Communication Engineering

Department of Electronics and Computer Engineering
Institute of Engineering, Pulchowk Campus
Tribhuwan University
Pulchowk, Lalitpur, Nepal

April 2, 2014

Dedications

To my Family

Acknowledgements

To my inspiration

Abstract

Information and communication theory studies and seeks justification to cause and effect of information creation, transformation and detection processes. Quantum Information Theory studies information and communication theory from the elementary particles known as of today using the quantum mechanics theory formalism. Akin to Shannon's entropy which quantifies information is a probabilistic measure in classical information theory, the Von Neumann entropy is defined as information in QIT. Over the years many new application have been developed from QIT awareness and QKD is perhaps the earliest and most matured application.

BB84 protocol is earliest QKD protocol which allows two parties to exchange secret key for secure communication. QKD BB84 protocol has gained growing interest primarily because everyday today we exchange valuable information. The security of communication relies on the fact of impossibility of creating exact copies of quantum states and measuring the quantum state without destroying it. The key is encoded in the states of photons and transmitted over the noisy channel. Many different kinds of researches have been conducted to check the security of the protocol.

The security of BB84 QKD protocol relies on QBER. It is desirable to posses QBER as a function of single observable. This thesis investigates polarization and phase shift encoding of BB84 protocol to answer the possibility of existence of such single observable. A photon source is assumed that emits single photons which are encoded in polarization and phase. A noisy channel acts on the encoded photons and are subsequently decoded. QBER is calculated for both encoding and results are compared to extract possible common observable that links to single observable.

List of Figures

List of Tables

Table of Contents

1. Introduction

1.1. Overview

Quantum information theory studies the information and communication theory from the microscopic particles point of view that are described by the law of quantum mechanics theory. The information and communication theory deals with the information creation, transmission, channel transformation, detection and studies cause and effect of these processes. Shannon notion of information as entropy [1] is accepted and has become central quantity in information theory and analogously, in quantum information theory Von Neumann entropy [2] is accepted as being an information quantity. Over the years quantum information theory and its applications have drawn numerous researchers into the field.

Although the application and availability of quantum computing and quantum computer is still infancy, one application has given constant hope and confidence to dwell into this newly emerging field. This application is called QKD(Quantum Key Distribution) which is a cryptography application. This application is not only important because it provides a test ground for quantum theory and communication but also it is important because privacy has also become an important and essential subject in the information technology society where we live in today. Secure communication is required in almost all sectors today, such as- mobile communication, email, web, bank electronics payment, to name a few. Classical cryptography is based on computational difficulty of decrypting the secret keys which is no longer secure with the computing power available today.

BB84 protocol is the first QKD application developed by Charles Bennett and Gilles

Brassard in 1984. It is one such early cryptography algorithm based on the quantum particle property. It allows two communicating parties to securely share key bits that can be used later as the encryption decryption key. The security comes from the inherent property of a quantum particle such that at the instant of any measurement the particle will be destroyed producing one time measurement result. Furthermore the No-Cloning theorem prohibits producing copies of the quantum particles state making it impossible for wire trappers to collect and resend the photonic state. To date, BB84 protocol has been successful both theoretically and practically to provide a secure communication. It has been formally implemented and tested in practice by number of academic institutions, researchers and commercial companies. Today the QKD has been successfully implemented by academic institutions and commercial companies [16] [17] with over 100km fiber optic cables and free space.

In this protocol [4], the sender generates random binary bits, the secret key, and encodes them into four polarized photonic states. These photonic states are then transmitted over the quantum channel and decoded with random basis of measurement at the receiver. Through the classical channel the receiver then tells the sender what measurement basis he/she used. The sender then compares his/her basis with the basis from the receiver, notes down the correct basis and sends this to the receiver. After receiving the basis compared information from the sender, the receiver corrects uses the correct basis to generate the secret key also called shifted key. Following this process of shifted key generation, error correction and privacy amplification are performed on the key to protect it from errors and to make it more secure. Any wire tappers will not be able to extract the key information without introducing error rate which will be known to sender and receiver. When the error rate is higher than a pre-defined threshold the protocol is aborted.

Polarization and phase encoding are two commonly used techniques for quantum communication in BB84 protocol. In polarization encoding, random classical bits are grouped into 2 bits and are converted into four types polarized photons- horizontal, vertical, +45 diagonal and -45 degree diagonal. These polarized states of photons are then transmitted over the communication channel to the receiver. Similarly, in phase encoding the random classical key bits are encoded into four phase photonic states (0, $\pi/2$, π, $3\pi/2$) and transmitted over the communication channel to the receiver.

The security of QKD relies on the fact that it is impossible to clone a quantum state and that when a quantum state is measured the state is destroyed giving only one time measurement chance. Various kinds of researches on the security of BB84 QKD has been conducted. Some of the well-known security analysis includes the intercept-resend attacks, Photon Number Splitting(PSN), .One of the security flaw comes from the problem of creating single photons because it allows attackers to steal photons. But ability to produce single photon is not a solution either because with increasing communication distance there is high probability that the single photons will be lost. The QBER(Quantum Bit Error Rate) which determines the number of qubits correctly detected and decoded is a parameter that gives extent of security. If QBER is high than it gives indication of eavesdropper and the protocol is aborted.

What is the ultimate relationship between QBER and the observables of information carrier like photon. Is there any concrete and perhaps singular relationship between QBER and information carrier observables? Less information regarding this question have been reported. This thesis seeks to answer this question by making a comparative study on photonic encoding as used in BB84 QKD protocol. The cause and effect of observables on the various photonic encodings is reported. This can help to understand more clearly the differences and similarities between any two photonic encoding techniques and justification into security issues.

1.2. Objective

This purpose of this thesis is to examine link between the observables of information carrier and QBER and hence security of BB84 QKD protocol. Another aim of this thesis is to seek answer on whether QBER can be expressed as a function of single observable. To achieve this goal this thesis makes a comparative theoretical analysis and simulation of polarization and phase shift encoding of BB84 protocol is conducted.

The objectives are be fragmented as below,

- To examine the link between observables and QBER
- To examine the existence of QBER as a function of single observable
- To make a comparative analysis and simulation of BB84 polarization and phase shift encoding algorithm

1.3. Scope

This thesis examines theory with comparative study through algorithm simulation in Matlab. From the algorithm point of view which has four major stages, only the first phase covering polarization and phase shift encoding are relevant to this thesis. From the physical implementation point of view assumption have been made on devices. A realistic photon sources generates pulses each of which contains arbitrary number of photons and not a single photon. However this thesis is based on the assumption that a single photon source is available. The QBER is dependent on source and

measurement device material their quantum efficiency. This thesis makes assumption that these are perfect material with no loss hence making the thesis more a theoretical study. Furthermore, communication distance factor is also dropped out. As such this thesis provides theoretical limits and any real physical implementation factors can be added suitably.

1.4. Application

Cryptography is essential integral part of communication. In the information technology society we live in today, the need for unbreakable secure encryption and decryption means has never been more than before. Voice communication over mobile network, email communication, secure web, online electronic payments such as bank and home utilities, online shopping are used every second every day worldwide and they can be compromised. They are based upon existing classical cryptography which is quit unreliable and breakable with todays computing technologies. The security provided by QKD protocol such as BB84 protocol looks very promising and in near future all information technology encryption and decryption may be based upon QKD. With the fast advancement of integrated electronics technology, fiber optics and reduction of manufacturing cost aided by the current theoretic and formal demonstration of the BB84 QKD protocol security strength, the reality of using QKD it is not far away. If QKD becomes reality on a wide scale this could change all existing information technology application and hence QKD is important and since this research touches the core of the underlying theory and engineering of QKD, this research is important.

2. Literature Review

The purpose of this thesis is to determine observables relation with QBER by making a comparative analysis of polarization and phase shift encoding as used in BB84

protocol. The core literature relevant to this thesis are the BB84 QKD algorithm, security and QBER. Thus these are covered in this chapter. First the BB84 protocol algorithm is described wherewith more emphasis is provided on polarization and phase shift encoding. Then researches conducted on security in the form of various kinds of attacks are described and finally QBER is covered.

2.1. BB84 Protocol and Photonic Encodings

BB84 protocol is a quantum key distribution protocol developed by Charles Bennett and Gilles Brassard in 1984 [3] which allows two communicating parties, Alice and Bob to create a secure and secret key that cannot be known to eavesdropper, Eve, that can be used to encrypt and decrypt messages. The protocol has four major stages- Encoding and Transmission, Shifted Key Generation, Information Reconciliation and Privacy Amplification. Although polarization encoding was implemented in the original BB84 protocol, phase encoding is also possible [4] which is also described in the encoding and transmission stage. These stages are explained below-

2.1.1. Encoding and Transmission

Encoding and transmission involves creating four different photonic states according to the random binary secret key bits and transmission of the photonic states to the receiver. Two widely used encoding method are polarization encoding and phase shift encoding which are described below.

2.1.1.1. Polarization Encoding

In polarization encoding the random key bits are encoded into four photonic polarized states- vertical and horizontal polarized photons and, +45 and -45 diagonally polarized photons. This table below illustrates the how random digital bits that forms the key are encoded into different polarized states of photons.

Random Bits	Polarized Encoded State	Quantum State
00	Horizontally Polarized	|0>
10	+45 Diagonally Polarized	|+>
01	Vertically Polarized	|1>
11	-45 Diagonally Polarized	|->

Table 1Polarization Encoding

The block diagram showing the implementation of polarization encoding is shown below.

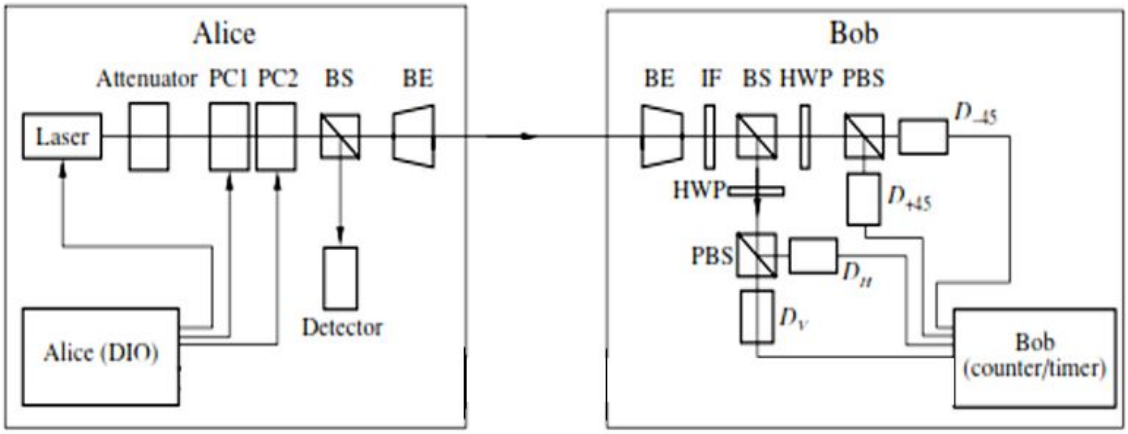

Figure 1: Polarization Encoding Block Diagram

In the figure above, the sender, Alice, creates random binary bits and also creates photons from the laser source. The binary bits are encoded into four polarization photonic states using the Pockel Cells(PC) according to the encoding table shown above. The encoded photons passes through the beam splitter(BS) that allows half of the produced photons to pass through and half of which are reflected to the sender detector. This is done to get statistics and keep track of the transmitted photons. The polarization encoded photons then enters the communication and are detected at the receiver. At the receiver the received photons converged and realigned for processing. The photons reach the BS where half of the photons are passed through and half of them are reflected. As shown, the photons that are passed through also passes a HWP and these together constitutes measurement in the X basis. Similarly, the photons that are reflected by the BS are incident on the HWP and this together constitute measurement in the Z basis. This measurements is random due to the fact that probability of transmission and reflection at the BS is random. The results are accordingly recorded by Bob.

2.1.1.2. Phase Shift Encoding

Phase shift Encoding is another method to encode the random bits into distinguishable photonic states. Here the bits are encoded into photonic states having 0, $\pi/2$, π and $3\pi/2$ phase. To achieve phase encoding Mach-Zehnder Interferometer (MZI) is used. In this implementation the photons enter the Mach-Zehnder Interferometer and random binary bits (the secret keys) controls the phase of photons in one of the path as shown in figure below such a way that the photons at the output have phase of 0, $\pi/2$, π or $3\pi/2$. The encoding table is for the conversion is shown below.

Random Bits	Phase Encoded State(φ_a)	Quantum State
00	0	|0>
01	$\pi/2$	|+>
10	π	|1>
11	$3\pi/2$	|->

Table 2:Phase Shift Encoding Table

The block diagram of the phase encoding is shown below.

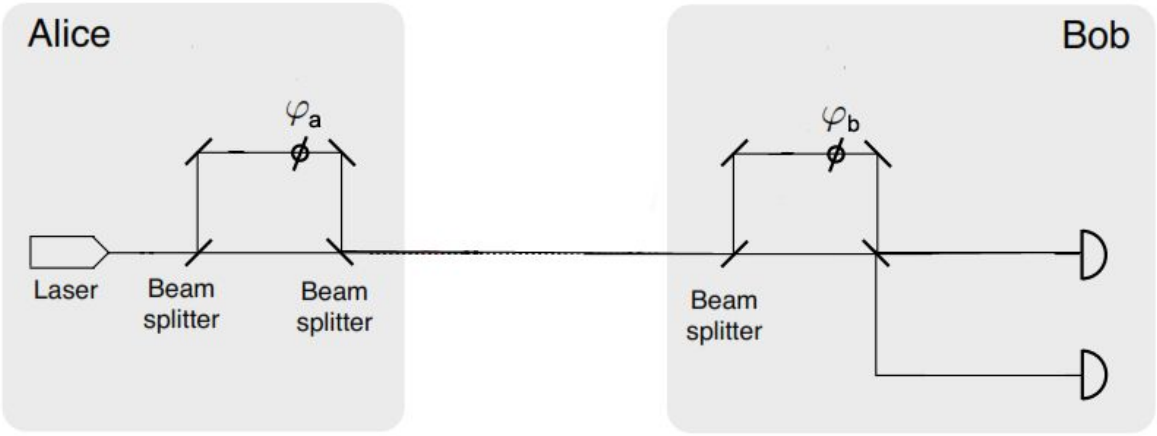

Figure 2: Phase Shift Encoding Block Diagram

In the above implementation,the combination of two beam splitter with two mirrors constitutes the Mach Zehnder interferometer(phase modulator)that produces a phase shift of φ_a and φ_b in the transmitter and receiver respectively.

2.1.2. Shifted Key Generation

After encoding and transmission of bits in photonic encoded form the next step is the detection and generation of shifted key which forms the secure core key to encrypt and decrypt messages. This step is explained next with polarization encoding and same approach is taken with phase shift encoding method.

When Bob receives the message encoded in quantum state of photon polarization, he performs decoding with random choice of arbitrary polarization gates(X or Z bases) and sends back to Alice the basis information which he used to decode the qubits but does not tell the result of the measurement. Alice compares the bases she used with the bases that Bob used and send Bob the basis which he got wrong. With this wrong bases information Bob can discard the incorrect bits and the correct bases corresponding to correct bit is used as the secure key.

Any middle eavesdropper, Eve, who is wire-tapping their photon communication link, cannot decode the key as it involves photon which is destroyed when she measures it. She may make photon measurement and retransmit an arbitrary photon state to Bob but in such case, Bob and Alice will know that someone is wire-tapping their link because she does not know which bases Alice used to encode the message having only a chance of 50% of getting right bases. When Bob makes his measurement sends the bases he used back to Alice, Alice will know that 25% of the total bases are only right and so will come to know that someone(Eve) has been trying to wire tap their link. The figure below illustrates the process of generation of shifted key or shared secret key with encoding and decoding that are involved.

Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

Table 3: Generation of Shifted Key

2.1.3. Information Reconciliation

The information reconciliation stage involves distillation and cleaning up the shared secret key by applying error corrections to the sifted key. Error correction is applied to the shared values X and Y between Alice and Bob to obtain some common shared values W. During the process of wire tapping suppose the eavesdropper obtains values Z then there might be some correlation between W and Z. Once Alice obtains the basis information, she compares her basis The information reconciliation stage

2.1.4. Privacy Amplification

The final stage is privacy amplification [5] a universal hash function unknown to potential wire trappers is applied to make the bits(W) from the information reconciliation stage more secure. From the information reconciliation stage, some values Z is obtained by the eavesdropper which night have some correlation between W and Z. Now in order to reduce correlation further between W and Z, some subset S of W is chosen using hash function [2]. That is a universal hash function G is applied that maps say n bits string in W to m bits string in S such that $g(w_1)=g(w_2)$ is at most

1/|S| where, w1,w2 ϵ W and g ϵ G. Now, the hash function is chosen in such a way that it maximizes the uncertainty about the secret key S obtainable by eavesdropper Eve.

2.2. Security

The security of QKD protocol stands on the fact that it is impossible to create a copy of a quantum state. However researches have been conducted to check the security of QKD that takes into account different work around. The researches that been conducted can be grouped into three major category- individual, joint attacks and quantum copying.

In individual attacks, each photon pulse in transit between legitimate sender and receiver are intercepted and measured separately by the eavesdropper. Within this, the photon pulses can be interacted instantly or at later time and with the help of the basis information that sender and receiver communicate over the classical channel extract the key information. In joint attacks, the eavesdropper prepares an ancilla state for each photons coming from the sender, interacts with the photon state and the prepared ancilla state, and then sends the photons to the receiver keeping the ancilla state. The eavesdropper later uses the basis information obtained from the public discussion to determine the ancilla state and hence the photonic state information.

The individual attacks includes the intercept-resend attack [6], Photon Number Splitting (PNS) attack [7] on weak coherent states, faked state attack, Trojan horse attack and time shift attack.

Intercept resend attack is simplest and one of the first studied form of attack. In this attack, the eavesdropper intercepts the transmitted photon signals, measures with

random basis, creates a new photons in the same detected state and resends them to the receiver. Photon Number Splitting attacks is based on the idea of stealing photons from pulses that are sent by the sender to the receiver. In other words, today's photon sources that are used for QKD produces weak coherent pulses attenuated from the laser sources and are therefore not true single photon source. Each attenuated pulse contains random number of photons- one, two, three or more photons and even zero photons on the statistical average. The number of photons has a Poissionian distribution as follows.

$$p(n, \mu) = \frac{\mu^n e^{-\mu}}{n!}$$

where, n is the number of photons and μ is the mean number of photons

Thus, in this attack, the mean number of photons μ directly determines security exploitation scope. A number of solutions have been reported to this form of attack. One solution is to reduce mean photon number(μ) which therefore prevents an eavesdropper to steal photons. In practice, μ value of 0.1 is used, which means that on average one photon is produced out of ten pulse. Another solution to this form of attack is to observe the photon number statistics at transmitter and receiver. If there is a mismatch in the probability distribution of photon numbers at the transmitter and receiver then it gives indication of possible eavesdropping. However this form of security check becomes inadequate when the eavesdropper is able to manipulate the photon number statistics so that the receiver sees the same photon number Possionian distribution. Another problem that arises if single photon is used and if probability distribution comparison is performed is that of distance. That is, if the communication link distance is increased then naturally there will be higher QBER due to higher probability that single photons will be lost and hence photon number probability distribution deviates leading to failure of the aforementioned security measure.

To cope with this kind of problem, another solution to PSN attack called the decoy state protocol has been reported. In this method, the sender intentionally creates decoy pulses, randomly, containing multiple photons and transmits them to receiver. The idea is to cope with the distance limitation problem using pulses having multiple photons with added security based on probability distribution known only to sender and receiver. More specifically, the photon number statistics are measured for transmitted signal pulse by the sender and receiver which then will give over some period of transmission an indication whether photons were lost or not.

The Trojan horse attack is somewhat different approach but realistic in which the attack is based on attack on the photon signals preparation and measurement devices. Here the eavesdropper targets the sender or receiver preparation or measurement device with light pulses and measures the reflected light pulses and performs phase modulation with some reference signal. The reflected light pulses gives information about the basis used by the sender to prepare the photons. A complete security breeze is possible if the eavesdropper can perform the aforementioned measurement quickly before the photons pulse reach the receiver. This is because if the eavesdropper is able to quickly get the basis information then the photons in transit between the sender and receiver can be measured with those acquired correct basis information and retransmitted to the receiver.

The faked state attack is another possible attack. In this attack, the eavesdropper intercepts the photon signals, measures it, creates and sends special photonic states to the receiver. The resend photons are special because they have the property that the receiver can only detect the photonic states if the receiver and eavesdropper have the same basis. Specifically, the special photons are created in such a way that their time shift is outside the receiver detector sensitivity curve. As such when such photons arrive at the receiver detectors only one detector can sense the photons while the other detector is blinded. This means that if the receiver uses different basis than the

eavesdropper nothing is measured. Thus if the eavesdropper measures the transmitted photons in wrong basis, the receiver will also measure in the wrong basis and vice versa. In this form of attack there are two indication of eavesdropper. First, there will be loss of signals at the detector and second, there will be time delays in the arrival of signals. For the first aspect, the eavesdropper might increase the brightness level of the resend signals. The second aspects is inherent to the attack technique. The possible solution for identifying eavesdropper is thus to use accurate timing between preparation and measurement of the signals.

Time shift attack is yet another attacking technique. It is similar to faked state attack in that it exploit the detection efficiency related to time shift. Meaning, here, the eavesdropper creates known time shift randomly to the photon signals in transmit between the communicating parties. Because of this time shifts in each photonic signals, the receiver detector produces measurement result known to the eavesdropper. As in case of faked state attack, there will be loss of signal detection and delay of arrival of signals.

Researches on possibility of cloning attack has also been reported [8]. A number of proofs of security have also been reported [9] [10].

2.3. QBER

Quantum Bit Error Rate (QBER) is one primary performance security measure quantity in QKD. It is the ratio of number of quantum qubits detected incorrectly to the total number of quantum qubits that were sent over the quantum channel, received and detected. In QKD, QBER gives signature of wiretappers when its value is higher than some predefined value. But QBER is not solely due to eavesdroppers but also on the channel environment, communication link distance and qubit detectors. In case of

photonic communication the channel environment are either optical fibers and free space [11]. It should also be noted that the noise due to channel environment increases with distance of the communication link.

In optical fiber communication channel [11][12], the effects that modifies the photonic state are chromatic dispersion and birefringence effects. The chromatic dispersion causes temporal spreading of light and is due to variation of velocities of pulses with frequencies. The birefringence effect causes depolarization or polarization mode dispersion wherein a pulse is split into its orthogonal components and this effect is due to optical fiber material factor. In free space channel, the loss of photonic state or decoherence is due to receiving device aperture and atmosphere [11][14]. The detectors used at the receiving end also has effect on QBER [11]. This QBER is due to the material used for detectors quantified by quantum efficiency and due to noise of the detector that sends out impulses in absence of actual signal.

If these various effects- transmission distance, detector inefficiency, dark count, faint light source with mean number of photons in a pulse, and uncorrelated photons in entanglement based encoding that can cause errors are considered then a general form of QBER [11] is as follows,

$$QBER = QBER_{wd} + QBER_{dc} + QBER_{ent}$$

Here $QBER_{wd}$ is the error due to wrong detection, $QBER_{dc}$ is error due to dark count and $QBER_{ent}$ is error due to uncorrelated photons which appears only in entanglement based encoding system.

3. Methodology

This research is both theoretical and simulation analysis oriented. Theoretical analysis is performed related to the thesis objective. The BB84 protocol algorithm using both polarization and phase shift encoding are implemented and stimulated in Matlab. In the test, random photon states are produced by the light source. Each random photon states are entered through the two encoders where they undergo polarization and phase shift. These encoded photon that exists from the transmitter are applied to the same noise channel operation. These noise coupled photons enters the receivers where uncorrelated random basis of measurement is applied. The QBER generated are recorded for each of the method. Then a comparative analysis is performed on the result. This result obtained are analyzed and compared with theoretical results obtained by researchers to draw conclusion.

The steps taken the research objective are summarized below,

- Theoretical examination of observables
- Construction of separate simulation model BB84 protocol Polarization encoding and Phase shift encoding
- Data testing, analysis and investigation obtained from the simulated models
- Interpretation of simulation result with theoretical examination

4. Analysis

5. Theoretical Preliminaries

The BB84 protocol, security and QBER was already described in details in the literature review. Here, other essential theoretical aspects relevant to this thesis objective are discussed. First classical theory of electromagnetic waves are described wherein, the polarization of waves and particles are described. Next, the theory of quantum information, the experimental apparatus and finally the measurement process are described.

5.1. Electromagnetic Waves and Polarization

Electromagnetic waves are energy waves which are generated as a result of transition of electrons from higher energy state to lower energy state. The transition of electrons between two energy states causes release of photons. The collection of photons emitted from the atoms constitutes the electromagnetic waves. Hence electromagnetic waves contain number of photons which are in motion. If the Power of the light source is P, and the frequency of the light is f, then the average number of photons per sec (<n>) is given by,

$$\langle n \rangle = P/hf$$

where, h is the plank constant

The emitted electromagnetic wave is made of electric and magnetic fields components which oscillates in two orthogonal directions in a plane which is perpendicular to the direction of the propagation of electromagnetic waves. Each electric and magnetic field can in turn be resolved into two components each having

its own phase. By convention the polarization state of of electromagnetic wave is described by the time varying direction and relative magnitude of the electric field. As such polarization is the curve traced by the end point of the vector arrow representing the instantaneous electric field. And the field is observed along the direction of propagation. The different phase relation of the two electric field components gives different polarization which can be classified into linear, circular or elliptical polarization. These different polarizations are described below.

Linear Polarization is the state of electric field vector of the electromagnetic wave at a point in space in which electric field is always directed along a line. For linearly polarized wave, the phase difference $\Delta\phi$ between the two electric field components is an integer multiple of π. That is, $\Delta\varphi = \varphi_y - \varphi_x = n\pi$ for n=0,1,2,3....Here we denote the horizontally x polarized electric field states by $|\leftrightarrow\rangle$and the vertically y polarized electric field states by $|\updownarrow\rangle$.

Circular polarization is the time harmonic variation of electric field in a given point in space if the electric field (or magnetic field) vector at that point traces a circle as a function of time. The condition for circular polarization is that magnitudes of the two components are equal and the phase difference between the two electric field components is an odd multiple of $\pi/2$. When the phase difference is $+\pi/2$ the direction of rotation of the electric field is clockwise (cw) and the wave is called left circularly polarized and when the phase difference is $-\pi/2$ the direction of rotation is counter clockwise (ccw). and the wave is called right circularly polarization. That is in general, the phase difference($\Delta\varphi$) is such that, $\Delta\varphi = \varphi_y - \varphi_x = (1/2+2n)\pi$ for clockwise direction and $\Delta\varphi = \varphi_y - \varphi_x = -(1/2+2n)\pi$ for counter clockwise direction with n taking integer values n=0,1,2,3 ...These two circular polarizations can be viewed as two orthogonal polarizations. The right and left circular polarization state is denoted here by $|R\rangle$ and $|L\rangle$.

Any state between the linear and circular polarization state is called elliptical polarization.

5.2. Quantum Information Theory

Here in this chapter, the theory of quantum states formalised by QM, the theory of quantum information theory, the entropy and the inequalities of QIT are described

5.2.1. Quantum States

In QIT the qubits is the elementary unit of information like bits in classical information theory. In QIT qubit are quantum state can be represented as a combination of its basis state. The linearly polarized electromagnetic waves- vertical, horizontal, +45 and -45 diagonal polarized electromagnetic waves are ultimately quantum states. We may represent horizontal and vertical linearly polarized states as $|0\rangle$ and $|1\rangle$ respectively in dirac notation of quantum state.

That is,

$|0\rangle = |\leftrightarrow\rangle$ is a horizontally polarized state

$|1\rangle = |\updownarrow\rangle$ is a vertically polarized state

Now, the +45 diagonally polarized(↗) and -45 anti-diagonally polarized states (↖) can be represented as the superposition of linearly horizontal and vertical polarized wave can be written as follows,

$$|+\rangle = |\nearrow\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$$

$$|-> = |↖> (|0> - |1>)/\sqrt{2}$$

Similarly the right circularly and left circularly polarized wave can be written as the superposition of linearly horizontal and vertical polarized wave as follows,

$$|R> = (|0> + i|1>)/\sqrt{2}$$

$$|L> = (|0> - i|1>)/\sqrt{2}$$

5.2.2. Entropies

Central to information theory is the concept of Entropy. As in classical information theory, there are various entropy quantities in QIT. The definition of measure of these entropies in QIT are provided below.

Von Neumann Entropy is defined as follows-

$$S(Q) = -Tr(QlogQ)$$

where, Q is the density matrix of a quantum state and Tr denotes the trace of matrix.

Quantum Relative Entropy is defined as follows,

$$S(Q_1||Q_2) = Tr(Q_1 log Q_1) – Tr(Q_1 log Q_2)$$

where Q_1 and Q_2 are two density of states of two system and Tr( ) denotes trace operation

Quantum Mutual Information is defined as follows,

$S(Q_1{:}Q_2) = S(Q_1) + S(Q_2) - S(Q_1Q_2)$

Quantum Conditional Entropy are defined as follows-

$S(Q_1|Q_2) = S(Q_1Q_2) - S(Q_2)$

and, $S(Q_2|Q_1) = S(Q_1Q_2) - S(Q_1)$

5.2.3. Inequalities of QIT

Here, the important inequalities results of QIT are provided. Any quantum state or system can be described with its density matrix. Given quantum states or sub-systems of a system described by density matrix Q_1, Q_2 and $Q_{12}$with corresponding Von Neumann entropies $S(Q_1)$, $S(Q_2)$ and $S(Q_1,Q_2)$then we have the following inequalities in QIT.

Klein Inequality states that the quantum relative entropy is non-negative and is expressed as below

$$S(Q_1||Q_2) \geq 0$$

with equality if and only if $Q_1 = Q_2$

Fano Inequality states that if Q_1 and Q_2 are density matrices such that the trace distance between them satisfies $Tr(Q_1,Q_2) \leq 1/e$, then

$$|S(Q_1)-S(Q_2)| \leq Tr(Q_1,Q_2)\ \log d + \eta(T(Q_1,Q_2))$$

Subadditivity Inequality states the following entropy inequality relation for sub-system 1, sub-system2 and joint system12.

$$S(Q_1,Q_2) \leq S(Q_1) + S(Q_2)$$

Similarly, the Triangular inequality states the following entropy inequalities for system consisting of of sub-system 1, sub-system2 and joint system12.

$$S(Q_1,Q_2) \geq |S(Q_1) + S(Q_2)|$$

5.3. Optical Instruments

Here optical components will be described as they are used produce, detect and manipulate different quantum states in experimental laboratory. First two forms of beam splitters(BM)- the 50:50 beam splitter and Polarization Beam Splitter (PBS) are described then two wave retarders- Quarter Wave Plate (QWP) and Half Wave Plates (HWP) which are light transparent birefringent crystal materials are described. A material is said to be birefringent if the speed of light through the material varies relative to the polarization orientation state of the incident light ray. The property of such material is that the speed of light is faster in one polarization direction called the fast axis and slower in the other polarization direction called the slow axis. Finally, the Mach Zehnder Interferometer(MZI) are described which is used for observing interference of two particles and is used in phase encoding.

5.3.1. Beam Splitter

A beam splitter is an optical device that splits light beam into two parts. Here the

effect of beam splitter and quantum nature of light is described. When electromagnetic wave of electric field intensity E, and power $P_{in}= |E|^2$ is incident on a 50:50 beam splitter then the beam will split into two beams of equal E-field amplitude $E/\sqrt{2}$. The two detectors placed in the path of the output beams will measure equal EM power of $P_{out}=P_{in}/2$. This is shown in the figure below.

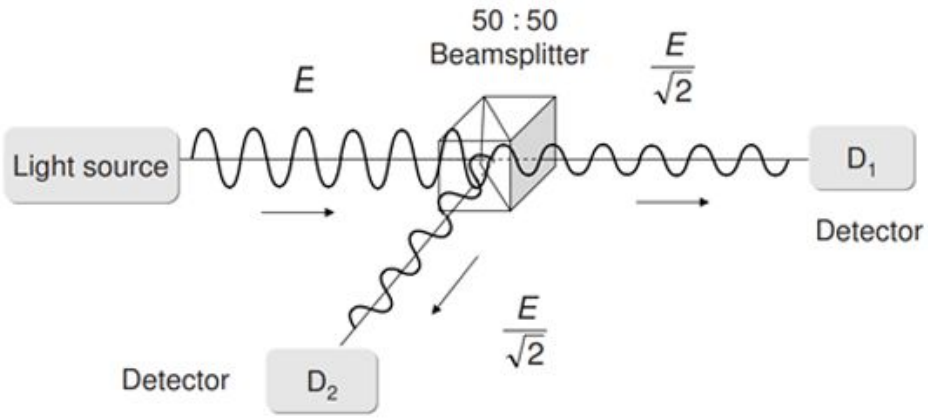

Figure 3: Dividing an EM light beam through a 50:50 beam splitter resulting in two beams of detected powers both equal to P/2

Now, when the power of the electromagnetic wave light source is reduced by proper amount then it is possible to emit single photon per unit time. When the emitted single photons are incident on the beam splitter then each of them will choose one of the two possible paths randomly. This is because photons cannot be split as they are elementary particles of quanta energy. The paths that these photons take are recorded in the single photon detectors (SPD). The numbers of pings generated at each of the single photon detectors over a period of time are equal. Thus, the probability of that each photon will take the straight path or the reflection path is equal to ½. This is illustrated in the picture below:

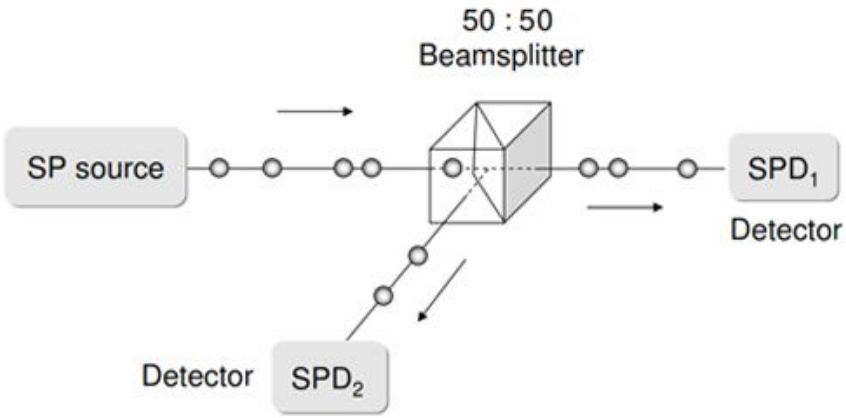

Figure 4: Same experimental setup with single photon (SP) being emitted and detected

5.3.2. Polarization Beam Splitter

The Polarization Beam Splitter (PBS) is a special assembly of birefringent crystal prism whose effect is to separate an incident polarized or unpolarized light beam into two orthogonally polarized components. This is used in polarization decoding to separate horizontal and vertical polarized photos as illustrated by the figure below.

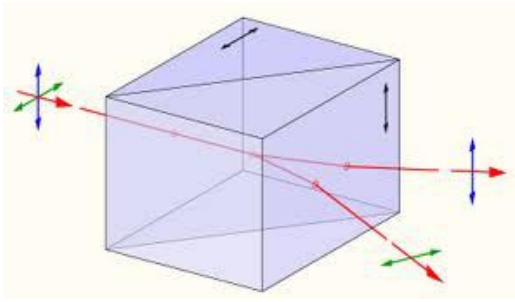

Figure 5: Polarization Beam Splitter

5.3.3. Quarter Wave Plates

A Quater Wave Plate(QWP) is a light transparent birefringent crystal materials which produces a relative phase change of $\Delta\phi = \pi/2$ between the components of the electric field. This can be obtained by controlling the thickness of the QWP. Thus QWP can be used to convert linearly polarized wave or photons into circularly polarized wave or photons and vice versa.

That is,

$$|+> \rightarrow |R>$$

$$|-> \rightarrow |L>$$

And,

$$|R> \rightarrow |+>$$

$$|L> \rightarrow |->$$

This transformation is equivalent to Hadamard gate action as follows:

$$H|0> = |+>$$

$$H|1> = |–>$$

$$H|+> = |0>$$

$H|-\rangle = |1\rangle$

The figure below illustrates this action of QWP,

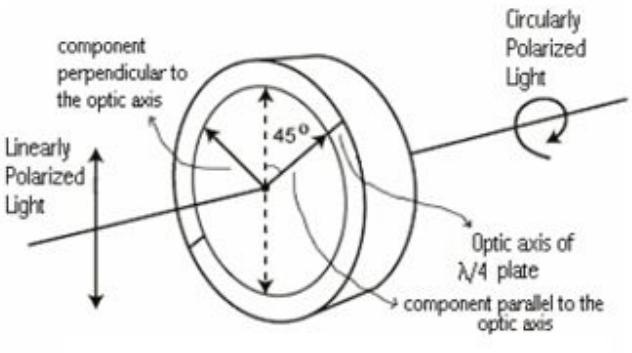

Figure 6: QWP Action

5.3.4. Half Wave Plates

Half wave plates (HWP) are light transparent birefringent crystal materials that produces a net phase delay between two orthogonal electric field components by π or one half of the wavelength. When the linearly polarized photons are incident on HWP the basis $\{\leftrightarrow, \updownarrow\}$ are interchanged. For this the fast axis of the plate must be oriented at 45° of the incident E-field polarization direction. Since this phase shift corresponds to a factor of $e^{i\pi} = -1$, the sign of one of the two polarization component is reversed and the result is a 90° rotation of the incident linear polarization. This HWP effect on linearly polarized photon is equivalent to action of Pauli matrix X on the $|0\rangle$ and $|1\rangle$.

That is,

$X|0\rangle = |1\rangle$

$$X|1> = |0>$$

Similarly, when +45 diagonally and -45 anti-diagonally polarized photons are incident on HWP the basis {↗,↖} are interchanged. However, unlike in case of HWP the fast axis of the plate is not changed that is 0°. This causes the change in direction of rotation of the incident circularly polarized waves. This HWP effect on circularly polarized photon is equivalent to action of Pauli matrix Z on the |+> and |->quantum states.

That is,

$$X|+> = |->$$

$$X|-> = |+>$$

The action of HWP is illustrated below,

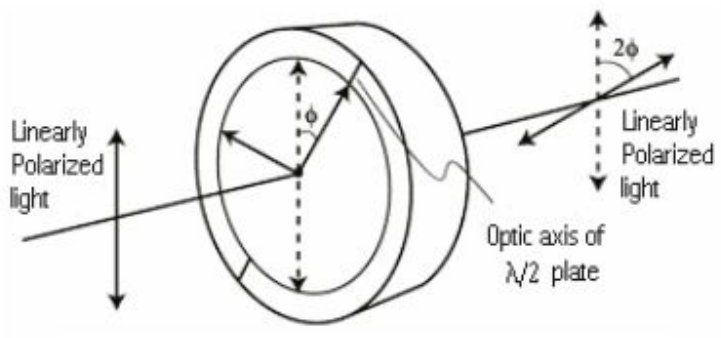

Figure 7: HWP Action

5.3.5. Mach Zehnder Interferometer

Mach Zehnder Interferometer is an apparatus set up and also a device that can be used to measure the interference pattern produced by constructive and destructive interference of light. In this a light is first split by a beam splitter into two parts, then one part is phase shifted by controlling the distance it travels or by using phase shifter in that path while the other part is allowed to travel without phase shift. Then the two beams of particles which undergoes phase shift and no phase shift are recombined by a second beam splitter. Depending upon the phase shift acquired by one part constructive and destructive interference is observed at the detector A and B.

The principle of operation of Mach Zehnder Interferometer is illustrated below.

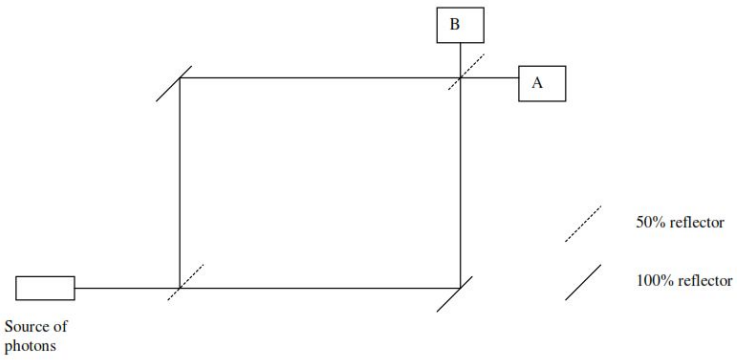

Figure 8: Mach Zehnder Interferometer

In the picture above, the dotted line 50% reflectors are beam splitters and the solid 100% reflectors are mirrors and A and B are detectors.

5.4. Measurement of Polarized States

Here the measurement and detection of linearly polarized photons and circularly polarized photons will be described next.

5.4.1. Measurement of Linearly Polarized Photons

The linearly polarized photons can be detected and measured by using one polarization beam splitter (PBS) and two single photon detectors (SPD) as shown in the figure below.

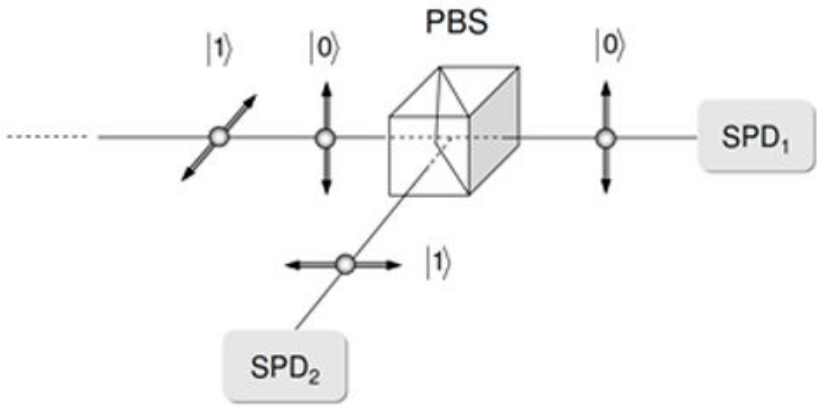

Figure 9: Splitting of light beam of single, linearly polarized photons through a PBS

SPD1 placed in the straight through path only detects vertically polarized or |0> photons, while the SPD2 placed in the reflection path detects only horizontally polarized or |1> photons. If a count is obtained from SPD1 or SPD2 we can attribute +1 or -1 respectively to these possible measurements.

This corresponds to measurement in the Z-basis in quantum mechanics. The eigenvectors and eigenvalues of Z operators are |0>, |1> and ±1. The transformation is,

$$Z|0\rangle = |0\rangle$$

or,

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

and,

$$Z|1\rangle = - |1\rangle$$

or,

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

5.4.2. Measurement of Circularly Polarized Photons

Similarly, to measure circular polarization state of photons, the circularly polarized photons are transformed into linearly polarized states first by QWP and then detected by the PBS-SPD1-SPD2 combination as in figure below.

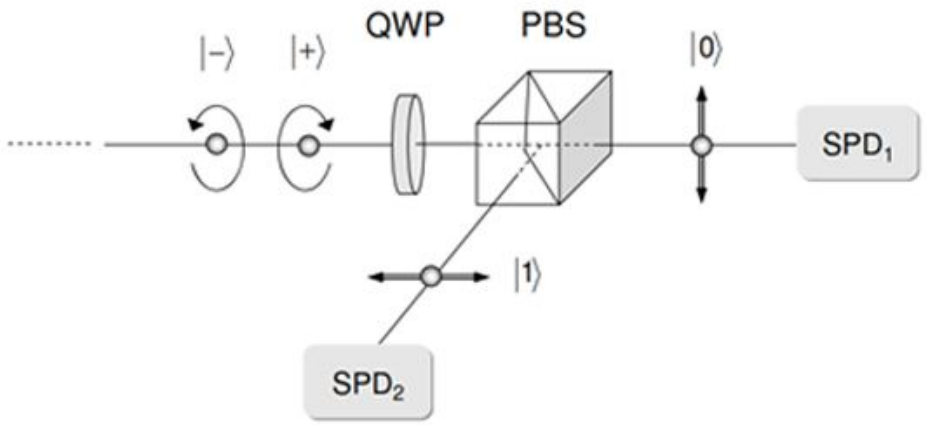

Figure 10: : Measurement and Detection for Circularly Polarized Photons

Thus, QWP-PBS-SPD1-SPD2 constitutes a quantum measurement apparatus to determine the state of circularly polarized photons. If a count is obtained in the SPD1 then we can attribute +1 and if a count is obtained in SPD2 then we can attribute -1 value. This corresponds to measurement in the X-basis as the eigenvector and eigenvalue of X are |+>,|-> and ±1.

That is,

$X|+> = |+>$

or $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

And,

$X|-> = |->$

or, $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = -\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$

6. Analysis and Simulation

Here theoretical and simulation analysis are provided.

Let us consider the transmitter section. In the transmitter, the sender, Alice generates photons and quantum state of a single photon can be described by the following equivalent Jones vector notation,

$$|\psi\rangle = \begin{bmatrix} \cos\theta \\ \sin\theta e^{i\varphi} \end{bmatrix}$$

where, θ is the angle made by electric field vector with the x-axis and φ is the phase difference between the x and y component. Both θ and φ are assumed to have random uniform distribution.

Such state can also be represented in density matrix form as,

$$Q_\psi = \begin{pmatrix} \cos^2\theta & \cos\theta \sin\theta e^{-i\varphi} \\ \cos\theta \sin\theta e^{i\varphi} & \sin^2\theta \end{pmatrix}$$

The sender also generates N uniformly distributed random binary bits according to which the photons(Q_Ψ) are encoded into polarization and phase shifted photonic states. The corresponding encoding lookup table are as follows.

Alice Random Bits	Polarized Encoded State	Encoded Quantum State	State Vector
00	Horizontally Polarized	|0>	$\begin{pmatrix}1\\0\end{pmatrix}$
10	+45 Diagonally Polarized	|+>	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$
01	Vertically Polarized	|1>	$\begin{pmatrix}0\\1\end{pmatrix}$
11	-45 Diagonally Polarized	|->	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$

Alice Random Bits	Phase Encoded State	Quantum State	State Vector
00	0	|0>	$\begin{pmatrix}\cos\theta\\ \sin\theta e^{i\varphi}\end{pmatrix}$
01	$\pi/2$	|+>	$i\begin{pmatrix}\cos\theta\\ \sin\theta e^{i\varphi}\end{pmatrix}$

10	π	|1>	$-\begin{pmatrix}\cos\theta \\ \sin\theta e^{i\varphi}\end{pmatrix}$
11	3π/2	|->	$-i\begin{pmatrix}\cos\theta \\ \sin\theta\end{pmatrix}$

Now, lets look at the communication channel. The photonic encoded states enters the quantum communication channel. It is described by a unitary operator Ɛ that acts on the transmitted quantum states. The quantum channels is modeled as a depolarizing channel that acts on the transmitted qubits, equivalently its density matrix(Q_Ψ) as follows-

$$Q\gamma = \mathcal{E}(Q_\Psi) = p_c I/2 Q_\Psi + (1-p_c)Q_\Psi$$

where, p_c is the probability that the channel input state described by Q_Ψ is transformed into a mixed state and $(1-p_c)$ is the probability that the input state is remains unaffected by the channel noise. Also I is the unit matrix.

Here, p_c is modeled as a uniformly distributed random probabilities.

Finally, the noise coupled signal are detected and measured at the receiver. Here each Qγ received is measured with N randomly generated X and Z basis operator in case of polarization encoding or 0 and π/2 basis in case of phase shift encoding which correspond.

These measurements are described by the following relation,

If Z was generated then the expected value of Z is,

$$\langle Z \rangle = Tr(ZQ\gamma)$$

And if X was generated then the expected value of X is,

$$\langle X \rangle = Tr(XQ\gamma)$$

Thus we get the expected value of the Z and X operators. These also represents the probability of correctly identifying the state $Q\gamma$.

Then the probability of wrong detection or probability of errors for the Z and X measurements as follows-

$$Pe(z) = 1-\langle Z \rangle$$

$$Pe(x) = 1-\langle X \rangle$$

The total probability of error is given by,

$$Pe = \frac{1}{2^{nR}} \sum_{j=X,Z} Pe(j)$$

As previously described in the QBER literature chapter, the QBER can be expressed as,

$$QBER = QBER_{wd} + QBER_{dc} + QBER_{ent}$$

However, this thesis is not concerned with detector efficiency, dark counts and entanglement based encoding implementation, the two factors $QBER_{dc}$, $QBER_{ent}$ are not essential and can be dropped out. The QBER that is of interest here is the $QBER_{wd}$ which is only concerned with the wrong detection of photons due to channel noise and wrong basis selection. This term then can be expressed as follows,

$$QBER = QBER_{wd} = p_{wd}$$

where, p_{wd} is the probability of wrong detection

This probability(Pe) is provided above.

7. Results and Discussions

A simulation model for the BB84 protocol was constructed with polarization and phase encoding. A photon source is considered that produced photons with random polar and azimuthal angles (θ,φ), which is then subsequently encoded in polarized and phase encoded form. These encoded photon was acted by channel noise and decoded with random basis. QBER was finally calculated for both the encoding methods.

Shown below are results of the simulation for N=32 , 64 and 128 key bits.

For N=32

Alice Basis: 1 1 1 0 0 0 0 0 1 1 0 0 1 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 1 1 0 1

Bob Basis: 1 0 0 0 1 1 1 0 0 0 0 1 0 1 0 1 0 1 0 0 1 0 0 1 0 0 0 0 0 1 0 0

Bob Result: 1 1 1 0 0 1 0 1 0 0 1 0 1 1 1 1 1 0 1 0 0 0 1 1 0 1 0 0 1 0 0 1

Basis Compared Result: 1 0 0 1 0 0 0 1 0 0 1 0 0 0 1 0 1 0 1 1 1 1 1 0 1 1 1 1 0 1 1 0

Shifted Key: 1 0 1 1 1 1 1 0 0 0 1 0 1 0 0 0 0

Polarization Shifted Key Length: 17

QBER: 0.46875

Alice Basis: 0 1 1 0 1 1 1 1 1 0 0 0 0 0 0 0 1 0 0 0 0 0 1 1 1 0 1 0 0 0 1 0

bob Basis: 0 0 0 0 0 0 1 1 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0

Result: 1 9 9 1 9 9 0 1 9 9 1 9 0 9 1 0 9 1 1 0 0 0 9 9 9 0 9 1 9 1 0 1

Basis Compared Result: 1 0 0 1 0 0 1 1 0 0 1 0 1 0 1 1 0 1 1 1 1 1 0 0 0 1 0 1 0 1 1 1

Shifted Key: 1 1 0 1 1 0 1 0 1 1 0 0 0 0 1 1 0 1

Phase Shifted Key Length: 18

QBER: 0.4375

For N=64

Alice Basis: 1 1 1 0 1 1 0 1 0 0 1 0 1 0 1 0 1 1 1 1 0 1 0 0 1 1 0 1 1 1 0 0 1 0 1 0 0 0 1 1 0 1 0 0 1 0 0 0 0 1 0 1 1 1 1 1 1 1 0 1 0 0 0 0

Bob Basis: 1 1 0 0 1 1 1 1 0 0 1 1 1 0 1 1 0 0 0 1 0 1 0
0 0 1 1 1 1 0 0 1 1 1 0 0 1 1 1 1 0 1 1 1 1 1 0 1 1 0
1 1 0 0 0 1 0 0 1 0 0 0 0 1

Bob Result: 0 1 0 0 0 0 1 1 1 0 0 1 1 0 0 0 1 1 0 1 0 1 0
1 1 0 0 1 1 1 0 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 1 0
1 0 0 0 1 1 0 1 0 0 1 0 0 1

Basis Compared Result: 1 1 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 0
1 1 1 1 1 0 1 0 1 1 0 1 0 1 0 0 1 0 0 1 1 1 1 0 0 1 0
1 0 0 0 0 1 0 0 0 1 0 0 0 0 1 1 1 0

Shifted Key: 0 1 0 0 0 1 1 0 0 1 0 0 1 0 1 0 1 0 1 1 0 0 1
0 0 0 0 0 1 0 1 1 0 0

Polarization Shifted Key Length: 34

QBER: 0.46875

Alice Basis: 1 0 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 1
0 0 1 0 0 0 0 0 1 1 0 1 0 0 0 0 0 0 1 1 0 0 0 0 0 1 0
0 0 1 0 0 0 0 0 0 0 0 1 0 1

bob Basis: 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0 0 0
0 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0
1 0 0 0 1 0 0 0 0 0 0 1 1 0

Result: 9 9 1 1 1 9 1 1 9 0 0 1 1 1 0 1 0 9 1 0 1 1 9 1

0 9 1 0 0 9 1 9 9 1 9 1 9 1 1 0 1 0 9 9 1 1 1 0 9 1 9 1 9 1 1 0 1 1 1 0 9 9

Basis Compared Result: 0 0 1 1 1 0 1 1 0 1 1 1 1 1 1 1 1 0 1 1 1 1 0 1 1 1 0 1 1 0 1 1 1 0 1 0 0 1 0 1 0 1 1 1 1 1 0 0 1 1 1 1 0 1 0 1 0 1 0 1 1 1 1 1 1 1 0 0

Shifted Key: 1 1 1 1 1 0 0 1 1 1 0 1 0 1 0 1 1 1 0 1 0 0 1 1 1 1 1 0 1 0 1 1 1 0 1 1 1 1 1 0 1 1 1 0

Phase Shifted Key Length: 44

QBER: 0.3125

For N=128

Alice Basis: 0 0 0 0 0 1 0 1 1 1 1 0 0 1 1 1 0 0 1 0 1 1 1 0 0 1 0 1 0 1 0 0 1 1 1 0 1 0 0 1 1 1 1 0 0 1 1 0 0 1 0 0 0 0 1 1 1 1 1 1 1 0 1 1 1 0 0 0 0 0 1 0 1 0 1 1 0 1 0 1 1 0 1 0 0 0 1 0 1 0 1 0 0 1 1 1 0 1 1 1 0 0 0 1 1 0 1 1 0 0 0 0 0 1 0 0 1 1 0 0 0 1 0 1 1 0 1

Bob Basis: 0 0 1 0 1 0 0 0 0 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 1 1 0 0 0 1 0 1 1 1 0 1 0 1 1 0 0 1 1 1 1 1 0 0 1 0 1 0 0 0 0 1 1 1 1 1 1 1 0 1 0 1 1 0 0 1 0 1 1 0 1 1 1 1 0 0 0 0 0 1 0 1 1 1 1 1 1 0 1 0 0 1 1 1 1 0 1 1 0 1 1 0 0 0 1 1 0 0 1 1 1 0 1 1 1 0 0 0 1 1

Bob Result: 0 1 1 0 0 0 1 1 0 0 0 1 1 0 1 1 1 1 1 0 1 1 0
0 0 1 1 1 0 1 0 1 0 1 1 1 1 1 1 0 0 1 1 0 1 0 0 0 0 0
1 0 1 0 0 0 1 1 0 1 0 1 0 1 1 1 1 0 1 1 1 1 0 0 1 1 1
0 1 0 0 1 1 1 1 0 1 0 1 0 0 0 0 0 0 1 0 0 0 0 1 1 1 0
0 0 0 0 1 0 1 1 1 1 1 0 1 1 1 1 0 1 0 1 0 1 1 1

Basis Compared Result: 1 1 0 1 0 0 1 0 0 0 1 1 1 0 0 0 1 1 1
0 0 0 1 1 0 1 1 0 1 1 1 0 1 1 0 0 0 0 0 0 0 1 1 1 0 0
0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 0 1 1 0 1 1 0
0 0 1 1 0 0 1 1 1 0 1 0 1 1 0 1 0 0 0 0 0 1 1 1 0 0 1
0 1 0 0 1 1 1 1 1 1 1 1 0 0 0 1 0 1 1 1 0 0 1 1 0 0 0
1

Shifted Key: 0 1 0 1 0 1 1 1 1 1 0 0 1 1 0 1 0 0 1 1 1 0 0
1 0 1 0 0 0 1 1 0 1 0 1 0 1 1 0 1 1 1 1 1 0 0 1 1 0 1
1 0 1 0 0 1 0 0 0 0 1 0 1 1 0 1 1 1 0 1 1

Polarization Shifted Key Length: 71

QBER: 0.44531

Alice Basis: 0 1 0 1 0 0 1 0 0 0 0 0 1 0 0 1 1 1 0 0 0 0 0
0 1 0 1 0 0 0 1 0 1 1 0 0 0 0 0 1 0 0 0 0 1 1 0 1 0 1
0 0 0 1 0 0 0 0 0 1 0 1 0 0 1 0 1 0 0 0 0 1 0 1 0 1 1
0 0 0 1 1 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1
0 0 0 1 0 1 0 0 1 0 0 0 1 1 0 0 1 1 1 0 0 0 0 0

bob Basis: 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

1 1 0 0 0 1 0 0 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 1 1
0 0 0 0 0 0 0 0 0 0 0 1 1 1 0 0 0 1 0 0 0 1 0 1 0 0 0
0 1 0 1 0 0 0 0 0 0 0 0 0 1 1 0 0 0 0 1 0 1 0 1 0 0 0
0 1 1 0 0 1 0 1 0 0 0 1 1 1 1 0 0 0 0 0 0 0 1 0

Result: 9 0 0 9 0 1 9 1 1 0 1 1 9 0 0 9 9 9 0 1 0 1 1 9
1 0 9 0 9 0 9 1 9 9 1 9 0 9 1 9 0 1 0 0 9 9 1 9 9 1 1
1 1 9 1 1 0 1 1 9 1 0 9 9 9 1 9 9 1 1 1 1 0 1 0 9 9 1
9 1 1 9 1 9 1 1 1 1 1 0 9 9 9 1 1 1 9 1 9 0 9 1 1 9 1
9 9 9 1 0 0 9 9 1 0 9 0 1 9 0 9 9 9 1 1 1 9 1

Basis Compared Result: 0 1 1 0 1 1 0 1 1 1 1 1 0 1 1 0 0 0 1
1 1 1 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 1 1 1 0 0
1 0 0 1 1 1 1 0 1 1 1 1 1 0 1 1 0 0 0 1 0 0 1 1 1 1 1
1 1 0 0 1 0 1 1 0 1 0 1 1 1 1 1 1 0 0 0 1 1 1 0 1 0 1
0 1 1 0 1 0 0 0 1 1 1 0 0 1 1 0 1 1 0 1 0 0 0 1 1 1 0
1

Shifted Key: 0 0 0 1 1 1 0 1 1 0 0 0 1 0 1 1 1 0 0 0 1 1 0
1 0 1 0 0 1 1 1 1 1 1 1 0 1 1 1 0 1 1 1 1 1 0 1 0 1 1
1 1 1 1 1 1 1 0 1 1 1 1 0 1 1 1 1 0 0 1 0 0 1 0 1 1 1
1

Phase Shifted Key Length: 78

QBER: 0.39063

8. Conclusion

From the foregoing result, we see that both polarization and phase shift encoding protocols produces almost half bits as shifted key for input N bits. The result also shows that the phase shift encoding produced more shifted key resulting less QBER. We can say that phase shift encoding on arbitrary quantum state of photons produces less error.

9. References

[1] C.E. Shannon. "*A Mathematical Theory Of Communication*" Bell Syst.Tech.J, 1948

[2] M.A Nielsen and I.L.Chuang, *Quantum Computation and Quantum Information*. Cambridge Univ. Press, 2000

[3] C. H. Bennett and G. Brassard. "Quantum Cryptography: Public key distribution and coin tossing," in Proc. IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, 1984, pp. 175

[4] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," Phys.Rev.Lett. 68. 3121, May. 1992.

[5] C. H. Bennett, G. Brassard, C. Cr´epeau, and U. M. Maurer,"Generalized Privacy Amplification," IEEE Trans. Inf. Theo. 41, 1915 (1995).

[6] C. H. Bennett, "Intercept-resend attacks in the Bennett-Brassard 1984 quantum-key-distribution protocol with weak coherent pulses," Phys. Rev. A 71, 062301, Jun. 2005.

[7] Fabio Grazioso, Frédéric Grosshans, "Photon-Number-Splitting-attack resistant Quantum Key Distribution Protocols without sifting", Laboratoire de Photonique Quantique et Moléculaire, France, Université de Montréal, Canada Laboratoire Aimé, France, September, 2013

[8] Mustapha Dehmani, Hamid Ez-Zahraouy, Abdelilah Benyoussef, "Quantum Cryptography with Several Cloning Attacks", Laboratory of Magnetism and High

Energy Physics, Journal of Computer Science 6 (7): 684-688, 2010, ISSN 1549-3636, 2010 Science Publications.

[9] Cyril Branciard, Nicolas Gisin, Barbara Kraus, Valerio Scarani, "Security of two quantum cryptography protocols using the same four qubit states", Group of Applied Physics, University of Geneva, February 1, 2008

[10] Agnes Ferenczi, Varun Narasimhachar, and Norbert Lutkenhaus, "Security proof of the unbalanced phase-encoded BB84 protocol", Institute for Quantum Computing & Department for Physics and Astronomy, University of Waterloo, 200 University Avenue West, N2L 3G1, Waterloo, Ontario, Canada, Jun, 2012.

[11] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, Quantum cryptography, *Rev. Mod. Phys.,* 2002, 74**,** 145.

[12] Muhammad Mubashir Khan, Salahuddin Hyder, Mahmood K Pathan, Kashif H Sheikh, "A Quantum Key Distribution Network Through Single Mode Optical Fiber", International Symposium on Collaborative Technologies and Systems, May 14-17, 2006 Las Vegas, Nevada, USA

[13] Muhammad Mubashir Khan, Michael Murphy, Almut Beige, "High error-rate quantum key distribution for long distance communication", arxiv.org/abs/0901.3909v4

[14] N. Antonietti, M. Mondin, F. Daneshgaran, G. Giovanelli, I. Kostadinov, B. Lunelli, "Quantum bit error rate in modeled atmospheres" International Journal of Quantum Information, World Scientific Publishing Company, Aug, 2008

[15] Y.-S. Kim, Y.-C. Jeong, and Y.-H. Kim, "Implementation of Polarization-Coded Free-Space BB84 Quantum Key Distribution" ISSN 1054-660X, Laser Physics, 2008, Vol. 18, No. 6, pp. 810–814

[16] Id Quantique, URL: http://www.idquantique.com

[17] QuintessenceLabs, URL: http://qlabsusa.com

10. Appendices

10.1. BB84 Algorithm Code

```
clc
clear all

N = input('Enter the number of input bits(N)=');

% ----- Parameter Initialization----------------

% ------Polarization Encoding Initialization & preallocation ----------

Pol=zeros(2,N);                    % : zeros(no. of rows, no. of columns)
alice_basis=zeros(1,N);
bob_basis=zeros(1,N);
basis=zeros(2,2);
bob_result_state=zeros(2,2);
bob_state=zeros(1,N);
bob_result=zeros(1,N);
compare=zeros(1,N);
basis_pol_info=zeros(1,N);
shifted_key_pol=zeros(1,N);

n=zeros(1,N);
m=zeros(1,N);

X=[0 1;1 0];
Z=[1 0;0 -1];

% ------Polarization Encoding Initialization ----------

% Phase Shift at the Transmitter

alpha1 = exp(1i*cos(0));                    % basis 0
alpha2 = exp(1i*cos(pi/2));                 % basis 1
alpha3 = exp(1i*cos(pi));                   % basis 0
alpha4 = exp(1i*cos(3*pi/2));               % basis 0

% Phase Shift at the Receiver

beta1 = exp(1i*cos(0));                     % basis 0
beta2 = exp(1i*cos(pi/2));                  % basis 1
beta3 = exp(1i*cos(pi));                    % basis 0
```

```
beta4 = exp(1i*cos(3*pi/2));                    % basis 1

path = zeros(1,N);
Out = zeros(2,N);
result =zeros(1,N);

a = zeros(1,N);
b = zeros(1,N);
c = zeros(1,N);
d = zeros(1,N);
e = zeros(1,N);
f = zeros(1,N);
g = zeros(1,N);
h = zeros(1,N);

alice_basis_phase = zeros(1,N);
bob_basis_phase = zeros(1,N);
basis_phase_info = zeros(1,N);

% ----- Start of Loop ---------------------------------------

for k=1:N;

    % ---------------- Input State Initialization ------------------------

    theta(k) = 180 * rand;
    phi(k) =   360 * rand;

    P(:,k) = [cos(theta(k)) sin(theta(k))*exp(1i*phi(k))]';

    % --------------- Polarization Encoding Starts ----------------------

    %---------------- Alice produces random polarized states----------------

            n(k)=randi([0,1]);
            m(k)=randi([0,1]);

                    if ((n(k)==0)&&(m(k)==0))
                        Pol(:,k) = [1 0;0 0]*P(:,k);
                        alice_basis(k)=0;
                    elseif ((n(k)==0)&&(m(k)==1)),
                        Pol(:,k) = 1/2*[1 1;1 1]*P(:,k);
                        alice_basis(k)=1;
                    elseif ((n(k)==1)&&(m(k)==0)),
```

```
            Pol(:,k) = [0 0;0 1]*P(:,k);
            alice_basis(k)=0;
        elseif ((n(k)==1)&&(m(k)==1)),
            Pol(:,k) = 1/2*[1 -1;-1 1]*P(:,k);
            alice_basis(k)=1;
        end

%   ---------------- Bob generates random Z,X basis -------------------

        B(k)=randi([0,1]);
            if(B(k)==0)
                basis(:,:,k) = Z;      % Z
                bob_basis(k)=0;
            else
                basis(:,:,k) = X;      % X
                bob_basis(k)=1;
            end

% -------------- Bob generated basis acts on received photons --------

        if(bob_basis(k)==0)
            bob_result_state(:,k)=Z*Pol(:,k);
        else
            bob_result_state(:,k)=X*Pol(:,k);
        end

% ------------- To calculate the bits corresponding to decoded bob state

            if(bob_result_state(:,k)==([1 0;0 0]*P(:,k)))
                bob_state(k)=1;
            elseif(bob_result_state(:,k)==((1/2)*[1 1;1 1]*P(:,k)))
                bob_state(k)=2;
            elseif(bob_result_state(:,k)==(-[0 0;0 1]*P(:,k)))
                bob_state(k)=3;
            elseif(bob_result_state(:,k)==((-1/2)*[1 -1;-1 1]*P(:,k)))
                bob_state(k)=4;
            else
                bob_state(k)=5;
            end

% ------------ Bob measurement result ---------------------

        if(bob_basis(k)==0 && bob_state(k)==1)          % Z basis and H
            bob_result(k) = 1;
```

```
elseif(bob_basis(k)==0 && bob_state(k)==2)       % Z basis and D
    bob_result(k) = randi([0,1]);

elseif(bob_basis(k)==0 && bob_state(k)==3)       % Z basis and V
    bob_result(k) = 0;

elseif(bob_basis(k)==0 && bob_state(k)==4)       % Z basis and A
    bob_result(k) = randi([0,1]);

elseif(bob_basis(k)==1 && bob_state(k)==1)       % X basis and H
    bob_result(k) = randi([0,1]);

elseif(bob_basis(k)==1 && bob_state(k)==2)       % X basis and D
    bob_result(k) = 1;

elseif(bob_basis(k)==1 && bob_state(k)==3)       % X basis and V
    bob_result(k) = randi([0,1]);

elseif(bob_basis(k)==1 && bob_state(k)==4)       %X basis and A
    bob_result(k) = 0;

elseif((bob_basis(k)==0 || bob_basis(k)==1) && bob_state(k) == 5)
    bob_result(k) = randi([0,1]);
end

% --------- Polarization Basis Comparision -------------------------------

                                compare(k)=xor(alice_basis(k),bob_basis(k));

                                    if(compare(k)==0)
                                        basis_pol_info(k) = 1;
                                    else
                                        basis_pol_info(k) = 0;
                                    end

                                    if(basis_pol_info(k)== 1)
                                       shifted_key_pol(k)=bob_result(k);
                                    else
                                       shifted_key_pol(k)= 5;
                                    end
                                    ind_pol(k) = (shifted_key_pol(k)==5);

%--------Polarization Encoding Ends-----------------
```

```
% -----------Phase Encoding Starts ----------------

mod1(:,k) = alpha1*P(:,k);                                  % Phase Shift
Modulated State
mod2(:,k) = alpha2*P(:,k);
mod3(:,k) = alpha3*P(:,k);
mod4(:,k) = alpha4*P(:,k);

demod1(:,k) = beta1*P(:,k);                                 % Phase Shift
demodulated State
demod2(:,k) = beta2*P(:,k);
demod3(:,k) = beta3*P(:,k);
demod4(:,k) = beta4*P(:,k);

% --------- Random Path Generation --------------

path(k)=rand;

% -------- Path 1 -----------------------------

if (0<path(k) && path(k)<=0.25)
    Out(:,k) = P(:,k);
    alice_basis_phase(k) = 0;
    bob_basis_phase(k) = 0;
    result(k) = 1;

% -------- Path 2 -----------------------------

elseif (0.25<path(k) && path(k)<=0.5),     % Path 2 is chosen: Photon travels
through the transmitter Phase shifter but not through the receiver phase shifter

                a(k)=randi([0,1]);
                b(k)=randi([0,1]);


                    if (a(k)==0&&b(k)==0)              %a(0)b(0) = 00 => 0
phase shift
                        Out(:,k) = mod1(:,k);
                        alice_basis_phase(k) = 0;
                        bob_basis_phase(k) = 0;
                        result(k) = 1;
                    elseif (a(k)==0&&b(k)==1),        %a(0)b(1) = 00 => pi/2
phase shift
```

```
                    Out(:,k) = mod2(:,k);
                    alice_basis_phase(k) = 1;
                    bob_basis_phase(k) = 0;
                    result(k) = 9;
                elseif (a(k)==1&&b(k)==0),        %a(1)b(0) = 00 => pi
phase shift
                    Out(:,k) = mod3(:,k);
                    alice_basis_phase(k) = 0;
                    bob_basis_phase(k) = 0;
                    result(k) = 0;
                elseif  (a(k)==1&&b(k)==1),        %a(1)b(1) = 00 =>
3pi/2 phase shift
                    Out(:,k) = mod4(:,k);
                    alice_basis_phase(k) = 1;
                    bob_basis_phase(k) = 0;
                    result(k) = 9;
                end

    % -------- Path 3 ------------------------------

   elseif (0.5<path(k) && path(k)<=0.75),                % Third Path is Chosen-
Photon travels through the straight path at the transmitter

        c(k)=randi([0,1]);
        d(k)=randi([0,1]);

                if (c(k)==0&&d(k)==0)
                    Out(:,k) = demod1(:,k);
                    alice_basis_phase(k) = 0;
                    bob_basis_phase(k) = 0;
                    result(k) = 1;

                elseif (c(k)==0&&d(k)==1),
                    Out(:,k) = demod2(:,k);
                    alice_basis_phase(k) = 0;
                    bob_basis_phase(k) = 1;
                    result(k) = 9;

                elseif (c(k)==1&&d(k)==0),
                    Out(:,k) = demod3(:,k);
                    alice_basis_phase(k) = 0;
                    bob_basis_phase(k) = 0;
                    result(k) = 0;
```

```
                elseif (c(k)==1&&d(k)==1),
                    Out(:,k) = demod4(:,k);
                    alice_basis_phase(k) = 0;
                    bob_basis_phase(k) = 1;
                    result(k) = 9;
                end

% -------- Path 4 -----------------------------

elseif(0.75<path(k) && path(k)<1),

                e(k)=randi([0,1]);
                f(k)=randi([0,1]);

                    if (e(k)==0&&f(k)==0)

                            g(k)=randi([0,1]);
                            h(k)=randi([0,1]);

                                        if (g(k)==0&&h(k)==0)
                                            Out(:,k) = (alpha1+beta1)*P(:,k);
                                            alice_basis_phase(k) = 0;
                                            bob_basis_phase(k) = 0;
                                            result(k) = 1;

                                        elseif (g(k)==0&&h(k)==1),
                                            Out(:,k) = (alpha1+beta2)*P(:,k);
                                            alice_basis_phase(k) = 0;
                                            bob_basis_phase(k) = 1;
                                            result(k) = 9;

                                        elseif (g(k)==1&&h(k)==0),
                                            Out(:,k) = (alpha1+beta3)*P(:,k);
                                            alice_basis_phase(k) = 0;
                                            bob_basis_phase(k) = 0;
                                            result(k) = 0;

                                        elseif (g(k)==1&&h(k)==1),
                                            Out(:,k) = (alpha1+beta4)*P(:,k);
                                            alice_basis_phase(k) = 0;
                                            bob_basis_phase(k) = 1;
                                            result(k) = 9;
                                        end
```

```
elseif (e(k)==0&&f(k)==1),

        g(k)=randi([0,1]);
        h(k)=randi([0,1]);

                if (g(k)==0&&h(k)==0)
                    Out(:,k) = (alpha2+beta1)*P(:,k);
                    alice_basis_phase(k) = 1;
                    bob_basis_phase(k) = 0;
                    result(k) = 9;
                elseif (g(k)==0&&h(k)==1),
                    Out(:,k) = (alpha2+beta2)*P(:,k);
                    alice_basis_phase(k) = 1;
                    bob_basis_phase(k) = 1;
                    result(k) = 1;
                elseif (g(k)==1&&h(k)==0),
                    Out(:,k) = (alpha2+beta3)*P(:,k);
                    alice_basis_phase(k) = 1;
                    bob_basis_phase(k) = 0;
                    result(k) = 9;
                elseif (g(k)==1&&h(k)==1),
                    Out(:,k) = (alpha2+beta4)*P(:,k);
                    alice_basis_phase(k) = 1;
                    bob_basis_phase(k) = 1;
                    result(k) = 0;
                end

elseif (e(k)==1&&f(k)==0),

        g(k)=randi([0,1]);
        h(k)=randi([0,1]);

                if (g(k)==0&&h(k)==0)
                    Out(:,k) = (alpha3+beta1)*P(:,k);
                    alice_basis_phase(k) = 0;
                    bob_basis_phase(k) = 0;
                    result(k) = 0;
                elseif (g(k)==0&&h(k)==1),
                    Out(:,k) = (alpha3+beta2)*P(:,k);
                    alice_basis_phase(k) = 0;
                    bob_basis_phase(k) = 1;
                    result(k) = 9;
                elseif (g(k)==1&&h(k)==0),
                    Out(:,k) = (alpha3+beta3)*P(:,k);
```

```
                                        alice_basis_phase(k) = 0;
                                        bob_basis_phase(k) = 0;
                                        result(k) = 1;
                                    elseif (g(k)==1&&h(k)==1),
                                        Out(:,k) = (alpha3+beta4)*P(:,k);
                                        alice_basis_phase(k) = 0;
                                        bob_basis_phase(k) = 1;
                                        result(k) = 9;
                                    end


            elseif (e(k)==1&&f(k)==1),

                    g(k)=randi([0,1]);
                    h(k)=randi([0,1]);

                                    if (g(k)==0&&h(k)==0)
                                        Out(:,k) = (alpha4+beta1)*P(:,k);
                                        alice_basis_phase(k) = 1;
                                        bob_basis_phase(k) = 0;
                                        result(k) = 9;
                                    elseif (g(k)==0&&h(k)==1),
                                        Out(:,k) = (alpha4+beta2)*P(:,k);
                                        alice_basis_phase(k) = 1;
                                        bob_basis_phase(k) = 1;
                                        result(k) = 0;
                                    elseif (g(k)==1&&h(k)==0),
                                        Out(:,k) = (alpha4+beta3)*P(:,k);
                                        alice_basis_phase(k) = 1;
                                        bob_basis_phase(k) = 0;
                                        result(k) = 9;
                                    elseif (g(k)==1&&h(k)==1),
                                        Out(:,k) = (alpha4+beta4)*P(:,k);
                                        alice_basis_phase(k) = 1;
                                        bob_basis_phase(k) = 1;
                                        result(k) = 1;
                                    end

                    end
end

% --------- Phase Basis Comparision -------------------------------
```

```
compare(k)=xor(alice_basis_phase(k),bob_basis_phase(k));

                                        if(compare(k)==0)
                                              basis_phase_info(k)= 1;
                                        else
                                              basis_phase_info(k)= 0;
                                        end

                                        if(basis_phase_info(k)== 1)
                                           shifted_key_phase(k)=result(k);
                                        else
                                           shifted_key_phase(k)= 5;
                                        end
                                        ind_ph(k) = (shifted_key_phase(k)==5);

end

%--------Polarization Encoding Calculation & Output-----

shifted_key_pol(ind_pol) = [] ;
M_pol= length(shifted_key_pol);
QBER_pol = (N-M_pol)/N;

disp(['Alice Basis: ', num2str(alice_basis)]);
disp(['Bob Basis: ', num2str(bob_basis)]);
disp(['Bob Result: ', num2str(bob_result)]);
disp(['Basis Compared Result: ', num2str(basis_pol_info)]);
disp(['Shifted Key: ', num2str(shifted_key_pol)]);
disp(['Polarization Shifted Key Length: ', num2str(M_pol)]);
disp(['QBER: ', num2str(QBER_pol)]);

%--------Phase Encoding Calculation & Output -----

shifted_key_phase(ind_ph) = [] ;
M_ph= length(shifted_key_phase);
QBER_ph = (N-M_ph)/N;

disp(['Alice Basis: ', num2str(alice_basis_phase)]);
disp(['bob Basis: ', num2str(bob_basis_phase)]);
disp(['Result: ', num2str(result)]);
disp(['Basis Compared Result: ', num2str(basis_phase_info)]);
disp(['Shifted Key: ', num2str(shifted_key_phase)]);
disp(['Phase Shifted Key Length: ', num2str(M_ph)]);
disp(['QBER: ', num2str(QBER_ph)]);
```

On The Observables Analysis Of BB84 Photonic Encodings

By

Unish Subba
(067/MSICE/619)

Submitted To
The Department of Electronics and Computer Engineering
Institute of Engineering, Pulchowk Campus
Tribhuwan University
Pulchowk, Lalitpur, Nepal

April 2, 2014

On The Observables Analysis Of BB84 Photonic Encodings

By

Unish Subba
(067/MSICE/619)

A thesis proposal submitted in partial fulfillment of the requirements for the degree of
Master of Science in Information and Communication Engineering

Department of Electronics and Computer Engineering
Institute of Engineering, Pulchowk Campus
Tribhuwan University
Pulchowk, Lalitpur, Nepal

April 2, 2014

Dedications

To my Family

Acknowledgements

To my inspiration

Abstract

Information and communication theory studies and seeks justification to cause and effect of information creation, transformation and detection processes. Quantum Information Theory studies information and communication theory from the elementary particles known as of today using the quantum mechanics theory formalism. Akin to Shannon's entropy which quantifies information is a probabilistic measure in classical information theory, the Von Neumann entropy is defined as information in QIT. Over the years many new application have been developed from QIT awareness and QKD is perhaps the earliest and most matured application.

BB84 protocol is earliest QKD protocol which allows two parties to exchange secret key for secure communication. QKD BB84 protocol has gained growing interest primarily because everyday today we exchange valuable information. The security of communication relies on the fact of impossibility of creating exact copies of quantum states and measuring the quantum state without destroying it. The key is encoded in the states of photons and transmitted over the noisy channel. Many different kinds of researches have been conducted to check the security of the protocol.

The security of BB84 QKD protocol relies on QBER. It is desirable to posses QBER as a function of single observable. This thesis investigates polarization and phase shift encoding of BB84 protocol to answer the possibility of existence of such single observable. A photon source is assumed that emits single photons which are encoded in polarization and phase. A noisy channel acts on the encoded photons and are subsequently decoded. QBER is calculated for both encoding and results are compared to extract possible common observable that links to single observable.

List of Figures

List of Tables

Table of Contents

1. Introduction

1.1. Overview

Quantum information theory studies the information and communication theory from the microscopic particles point of view that are described by the law of quantum mechanics theory. The information and communication theory deals with the information creation, transmission, channel transformation, detection and studies cause and effect of these processes. Shannon notion of information as entropy [1] is accepted and has become central quantity in information theory and analogously, in quantum information theory Von Neumann entropy [2] is accepted as being an information quantity. Over the years quantum information theory and its applications have drawn numerous researchers into the field.

Although the application and availability of quantum computing and quantum computer is still infancy, one application has given constant hope and confidence to dwell into this newly emerging field. This application is called QKD(Quantum Key Distribution) which is a cryptography application. This application is not only important because it provides a test ground for quantum theory and communication but also it is important because privacy has also become an important and essential subject in the information technology society where we live in today. Secure communication is required in almost all sectors today, such as- mobile communication, email, web, bank electronics payment, to name a few. Classical cryptography is based on computational difficulty of decrypting the secret keys which is no longer secure with the computing power available today.

BB84 protocol is the first QKD application developed by Charles Bennett and Gilles

Brassard in 1984. It is one such early cryptography algorithm based on the quantum particle property. It allows two communicating parties to securely share key bits that can be used later as the encryption decryption key. The security comes from the inherent property of a quantum particle such that at the instant of any measurement the particle will be destroyed producing one time measurement result. Furthermore the No-Cloning theorem prohibits producing copies of the quantum particles state making it impossible for wire trappers to collect and resend the photonic state. To date, BB84 protocol has been successful both theoretically and practically to provide a secure communication. It has been formally implemented and tested in practice by number of academic institutions, researchers and commercial companies. Today the QKD has been successfully implemented by academic institutions and commercial companies [16] [17] with over 100km fiber optic cables and free space.

In this protocol [4], the sender generates random binary bits, the secret key, and encodes them into four polarized photonic states. These photonic states are then transmitted over the quantum channel and decoded with random basis of measurement at the receiver. Through the classical channel the receiver then tells the sender what measurement basis he/she used. The sender then compares his/her basis with the basis from the receiver, notes down the correct basis and sends this to the receiver. After receiving the basis compared information from the sender, the receiver corrects uses the correct basis to generate the secret key also called shifted key. Following this process of shifted key generation, error correction and privacy amplification are performed on the key to protect it from errors and to make it more secure. Any wire tappers will not be able to extract the key information without introducing error rate which will be known to sender and receiver. When the error rate is higher than a pre-defined threshold the protocol is aborted.

Polarization and phase encoding are two commonly used techniques for quantum communication in BB84 protocol. In polarization encoding, random classical bits are grouped into 2 bits and are converted into four types polarized photons- horizontal, vertical, +45 diagonal and -45 degree diagonal. These polarized states of photons are then transmitted over the communication channel to the receiver. Similarly, in phase encoding the random classical key bits are encoded into four phase photonic states (0, $\pi/2$, π, $3\pi/2$) and transmitted over the communication channel to the receiver.

The security of QKD relies on the fact that it is impossible to clone a quantum state and that when a quantum state is measured the state is destroyed giving only one time measurement chance. Various kinds of researches on the security of BB84 QKD has been conducted. Some of the well-known security analysis includes the intercept-resend attacks, Photon Number Splitting(PSN), .One of the security flaw comes from the problem of creating single photons because it allows attackers to steal photons. But ability to produce single photon is not a solution either because with increasing communication distance there is high probability that the single photons will be lost. The QBER(Quantum Bit Error Rate) which determines the number of qubits correctly detected and decoded is a parameter that gives extent of security. If QBER is high than it gives indication of eavesdropper and the protocol is aborted.

What is the ultimate relationship between QBER and the observables of information carrier like photon. Is there any concrete and perhaps singular relationship between QBER and information carrier observables? Less information regarding this question have been reported. This thesis seeks to answer this question by making a comparative study on photonic encoding as used in BB84 QKD protocol. The cause and effect of observables on the various photonic encodings is reported. This can help to understand more clearly the differences and similarities between any two photonic encoding techniques and justification into security issues.

1.2. Objective

This purpose of this thesis is to examine link between the observables of information carrier and QBER and hence security of BB84 QKD protocol. Another aim of this thesis is to seek answer on whether QBER can be expressed as a function of single observable. To achieve this goal this thesis makes a comparative theoretical analysis and simulation of polarization and phase shift encoding of BB84 protocol is conducted.

The objectives are be fragmented as below,

- To examine the link between observables and QBER
- To examine the existence of QBER as a function of single observable
- To make a comparative analysis and simulation of BB84 polarization and phase shift encoding algorithm

1.3. Scope

This thesis examines theory with comparative study through algorithm simulation in Matlab. From the algorithm point of view which has four major stages, only the first phase covering polarization and phase shift encoding are relevant to this thesis. From the physical implementation point of view assumption have been made on devices. A realistic photon sources generates pulses each of which contains arbitrary number of photons and not a single photon. However this thesis is based on the assumption that a single photon source is available. The QBER is dependent on source and

measurement device material their quantum efficiency. This thesis makes assumption that these are perfect material with no loss hence making the thesis more a theoretical study. Furthermore, communication distance factor is also dropped out. As such this thesis provides theoretical limits and any real physical implementation factors can be added suitably.

1.4. Application

Cryptography is essential integral part of communication. In the information technology society we live in today, the need for unbreakable secure encryption and decryption means has never been more than before. Voice communication over mobile network, email communication, secure web, online electronic payments such as bank and home utilities, online shopping are used every second every day worldwide and they can be compromised. They are based upon existing classical cryptography which is quit unreliable and breakable with todays computing technologies. The security provided by QKD protocol such as BB84 protocol looks very promising and in near future all information technology encryption and decryption may be based upon QKD. With the fast advancement of integrated electronics technology, fiber optics and reduction of manufacturing cost aided by the current theoretic and formal demonstration of the BB84 QKD protocol security strength, the reality of using QKD it is not far away. If QKD becomes reality on a wide scale this could change all existing information technology application and hence QKD is important and since this research touches the core of the underlying theory and engineering of QKD, this research is important.

2. Literature Review

The purpose of this thesis is to determine observables relation with QBER by making a comparative analysis of polarization and phase shift encoding as used in BB84

protocol. The core literature relevant to this thesis are the BB84 QKD algorithm, security and QBER. Thus these are covered in this chapter. First the BB84 protocol algorithm is described wherewith more emphasis is provided on polarization and phase shift encoding. Then researches conducted on security in the form of various kinds of attacks are described and finally QBER is covered.

2.1. BB84 Protocol and Photonic Encodings

BB84 protocol is a quantum key distribution protocol developed by Charles Bennett and Gilles Brassard in 1984 [3] which allows two communicating parties, Alice and Bob to create a secure and secret key that cannot be known to eavesdropper, Eve, that can be used to encrypt and decrypt messages. The protocol has four major stages- Encoding and Transmission, Shifted Key Generation, Information Reconciliation and Privacy Amplification. Although polarization encoding was implemented in the original BB84 protocol, phase encoding is also possible [4] which is also described in the encoding and transmission stage. These stages are explained below-

2.1.1. Encoding and Transmission

Encoding and transmission involves creating four different photonic states according to the random binary secret key bits and transmission of the photonic states to the receiver. Two widely used encoding method are polarization encoding and phase shift encoding which are described below.

2.1.1.1. Polarization Encoding

In polarization encoding the random key bits are encoded into four photonic polarized states- vertical and horizontal polarized photons and, +45 and -45 diagonally polarized photons. This table below illustrates the how random digital bits that forms the key are encoded into different polarized states of photons.

Random Bits	Polarized Encoded State	Quantum State
00	Horizontally Polarized	|0>
10	+45 Diagonally Polarized	|+>
01	Vertically Polarized	|1>
11	-45 Diagonally Polarized	|->

Table 1Polarization Encoding

The block diagram showing the implementation of polarization encoding is shown below.

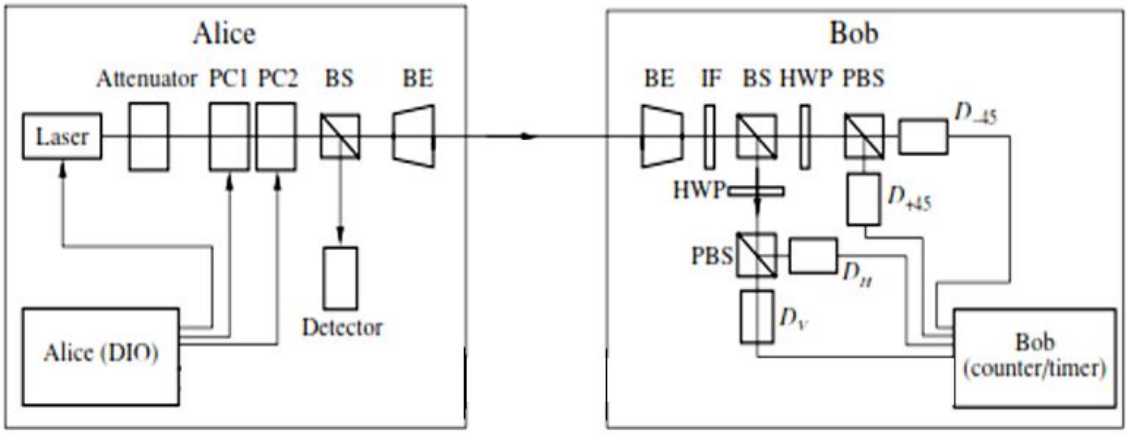

Figure 1: Polarization Encoding Block Diagram

In the figure above, the sender, Alice, creates random binary bits and also creates photons from the laser source. The binary bits are encoded into four polarization photonic states using the Pockel Cells(PC) according to the encoding table shown above. The encoded photons passes through the beam splitter(BS) that allows half of the produced photons to pass through and half of which are reflected to the sender detector. This is done to get statistics and keep track of the transmitted photons. The polarization encoded photons then enters the communication and are detected at the receiver. At the receiver the received photons converged and realigned for processing. The photons reach the BS where half of the photons are passed through and half of them are reflected. As shown, the photons that are passed through also passes a HWP and these together constitutes measurement in the X basis. Similarly, the photons that are reflected by the BS are incident on the HWP and this together constitute measurement in the Z basis. This measurements is random due to the fact that probability of transmission and reflection at the BS is random. The results are accordingly recorded by Bob.

2.1.1.2. Phase Shift Encoding

Phase shift Encoding is another method to encode the random bits into distinguishable photonic states. Here the bits are encoded into photonic states having 0, $\pi/2$, π and $3\pi/2$ phase. To achieve phase encoding Mach-Zehnder Interferometer (MZI) is used. In this implementation the photons enter the Mach-Zehnder Interferometer and random binary bits (the secret keys) controls the phase of photons in one of the path as shown in figure below such a way that the photons at the output have phase of 0, $\pi/2$, π or $3\pi/2$. The encoding table is for the conversion is shown below.

Random Bits	Phase Encoded State(φ_a)	Quantum State
00	0	|0>
01	$\pi/2$	|+>
10	π	|1>
11	$3\pi/2$	|->

Table 2:Phase Shift Encoding Table

The block diagram of the phase encoding is shown below.

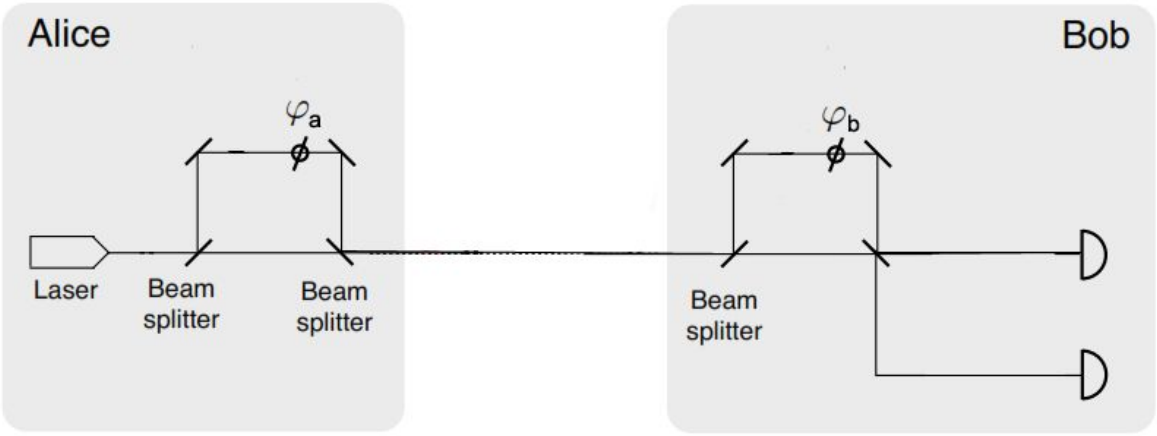

Figure 2: Phase Shift Encoding Block Diagram

In the above implementation,the combination of two beam splitter with two mirrors constitutes the Mach Zehnder interferometer(phase modulator)that produces a phase shift of φ_a and φ_b in the transmitter and receiver respectively.

2.1.2. Shifted Key Generation

After encoding and transmission of bits in photonic encoded form the next step is the detection and generation of shifted key which forms the secure core key to encrypt and decrypt messages. This step is explained next with polarization encoding and same approach is taken with phase shift encoding method.

When Bob receives the message encoded in quantum state of photon polarization, he performs decoding with random choice of arbitrary polarization gates(X or Z bases) and sends back to Alice the basis information which he used to decode the qubits but does not tell the result of the measurement. Alice compares the bases she used with the bases that Bob used and send Bob the basis which he got wrong. With this wrong bases information Bob can discard the incorrect bits and the correct bases corresponding to correct bit is used as the secure key.

Any middle eavesdropper, Eve, who is wire-tapping their photon communication link, cannot decode the key as it involves photon which is destroyed when she measures it. She may make photon measurement and retransmit an arbitrary photon state to Bob but in such case, Bob and Alice will know that someone is wire-tapping their link because she does not know which bases Alice used to encode the message having only a chance of 50% of getting right bases. When Bob makes his measurement sends the bases he used back to Alice, Alice will know that 25% of the total bases are only right and so will come to know that someone(Eve) has been trying to wire tap their link. The figure below illustrates the process of generation of shifted key or shared secret key with encoding and decoding that are involved.

Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

Table 3: Generation of Shifted Key

2.1.3. Information Reconciliation

The information reconciliation stage involves distillation and cleaning up the shared secret key by applying error corrections to the sifted key. Error correction is applied to the shared values X and Y between Alice and Bob to obtain some common shared values W. During the process of wire tapping suppose the eavesdropper obtains values Z then there might be some correlation between W and Z. Once Alice obtains the basis information, she compares her basis The information reconciliation stage

2.1.4. Privacy Amplification

The final stage is privacy amplification [5] a universal hash function unknown to potential wire trappers is applied to make the bits(W) from the information reconciliation stage more secure. From the information reconciliation stage, some values Z is obtained by the eavesdropper which night have some correlation between W and Z. Now in order to reduce correlation further between W and Z, some subset S of W is chosen using hash function [2]. That is a universal hash function G is applied that maps say n bits string in W to m bits string in S such that $g(w_1)=g(w_2)$ is at most

1/|S| where, w1,w2 ϵ W and g ϵ G. Now, the hash function is chosen in such a way that it maximizes the uncertainty about the secret key S obtainable by eavesdropper Eve.

2.2. Security

The security of QKD protocol stands on the fact that it is impossible to create a copy of a quantum state. However researches have been conducted to check the security of QKD that takes into account different work around. The researches that been conducted can be grouped into three major category- individual, joint attacks and quantum copying.

In individual attacks, each photon pulse in transit between legitimate sender and receiver are intercepted and measured separately by the eavesdropper. Within this, the photon pulses can be interacted instantly or at later time and with the help of the basis information that sender and receiver communicate over the classical channel extract the key information. In joint attacks, the eavesdropper prepares an ancilla state for each photons coming from the sender, interacts with the photon state and the prepared ancilla state, and then sends the photons to the receiver keeping the ancilla state. The eavesdropper later uses the basis information obtained from the public discussion to determine the ancilla state and hence the photonic state information.

The individual attacks includes the intercept-resend attack [6], Photon Number Splitting (PNS) attack [7] on weak coherent states, faked state attack, Trojan horse attack and time shift attack.

Intercept resend attack is simplest and one of the first studied form of attack. In this attack, the eavesdropper intercepts the transmitted photon signals, measures with

random basis, creates a new photons in the same detected state and resends them to the receiver. Photon Number Splitting attacks is based on the idea of stealing photons from pulses that are sent by the sender to the receiver. In other words, today's photon sources that are used for QKD produces weak coherent pulses attenuated from the laser sources and are therefore not true single photon source. Each attenuated pulse contains random number of photons- one, two, three or more photons and even zero photons on the statistical average. The number of photons has a Poissionian distribution as follows.

$$p(n, \mu) = \frac{\mu^n e^{-\mu}}{n!}$$

where, n is the number of photons and μ is the mean number of photons

Thus, in this attack, the mean number of photons μ directly determines security exploitation scope. A number of solutions have been reported to this form of attack. One solution is to reduce mean photon number(μ) which therefore prevents an eavesdropper to steal photons. In practice, μ value of 0.1 is used, which means that on average one photon is produced out of ten pulse. Another solution to this form of attack is to observe the photon number statistics at transmitter and receiver. If there is a mismatch in the probability distribution of photon numbers at the transmitter and receiver then it gives indication of possible eavesdropping. However this form of security check becomes inadequate when the eavesdropper is able to manipulate the photon number statistics so that the receiver sees the same photon number Possionian distribution. Another problem that arises if single photon is used and if probability distribution comparison is performed is that of distance. That is, if the communication link distance is increased then naturally there will be higher QBER due to higher probability that single photons will be lost and hence photon number probability distribution deviates leading to failure of the aforementioned security measure.

To cope with this kind of problem, another solution to PSN attack called the decoy state protocol has been reported. In this method, the sender intentionally creates decoy pulses, randomly, containing multiple photons and transmits them to receiver. The idea is to cope with the distance limitation problem using pulses having multiple photons with added security based on probability distribution known only to sender and receiver. More specifically, the photon number statistics are measured for transmitted signal pulse by the sender and receiver which then will give over some period of transmission an indication whether photons were lost or not.

The Trojan horse attack is somewhat different approach but realistic in which the attack is based on attack on the photon signals preparation and measurement devices. Here the eavesdropper targets the sender or receiver preparation or measurement device with light pulses and measures the reflected light pulses and performs phase modulation with some reference signal. The reflected light pulses gives information about the basis used by the sender to prepare the photons. A complete security breeze is possible if the eavesdropper can perform the aforementioned measurement quickly before the photons pulse reach the receiver. This is because if the eavesdropper is able to quickly get the basis information then the photons in transit between the sender and receiver can be measured with those acquired correct basis information and retransmitted to the receiver.

The faked state attack is another possible attack. In this attack, the eavesdropper intercepts the photon signals, measures it, creates and sends special photonic states to the receiver. The resend photons are special because they have the property that the receiver can only detect the photonic states if the receiver and eavesdropper have the same basis. Specifically, the special photons are created in such a way that their time shift is outside the receiver detector sensitivity curve. As such when such photons arrive at the receiver detectors only one detector can sense the photons while the other detector is blinded. This means that if the receiver uses different basis than the

eavesdropper nothing is measured. Thus if the eavesdropper measures the transmitted photons in wrong basis, the receiver will also measure in the wrong basis and vice versa. In this form of attack there are two indication of eavesdropper. First, there will be loss of signals at the detector and second, there will be time delays in the arrival of signals. For the first aspect, the eavesdropper might increase the brightness level of the resend signals. The second aspects is inherent to the attack technique. The possible solution for identifying eavesdropper is thus to use accurate timing between preparation and measurement of the signals.

Time shift attack is yet another attacking technique. It is similar to faked state attack in that it exploit the detection efficiency related to time shift. Meaning, here, the eavesdropper creates known time shift randomly to the photon signals in transmit between the communicating parties. Because of this time shifts in each photonic signals, the receiver detector produces measurement result known to the eavesdropper. As in case of faked state attack, there will be loss of signal detection and delay of arrival of signals.

Researches on possibility of cloning attack has also been reported [8]. A number of proofs of security have also been reported [9] [10].

2.3. QBER

Quantum Bit Error Rate (QBER) is one primary performance security measure quantity in QKD. It is the ratio of number of quantum qubits detected incorrectly to the total number of quantum qubits that were sent over the quantum channel, received and detected. In QKD, QBER gives signature of wiretappers when its value is higher than some predefined value. But QBER is not solely due to eavesdroppers but also on the channel environment, communication link distance and qubit detectors. In case of

photonic communication the channel environment are either optical fibers and free space [11]. It should also be noted that the noise due to channel environment increases with distance of the communication link.

In optical fiber communication channel [11][12], the effects that modifies the photonic state are chromatic dispersion and birefringence effects. The chromatic dispersion causes temporal spreading of light and is due to variation of velocities of pulses with frequencies. The birefringence effect causes depolarization or polarization mode dispersion wherein a pulse is split into its orthogonal components and this effect is due to optical fiber material factor. In free space channel, the loss of photonic state or decoherence is due to receiving device aperture and atmosphere [11][14]. The detectors used at the receiving end also has effect on QBER [11]. This QBER is due to the material used for detectors quantified by quantum efficiency and due to noise of the detector that sends out impulses in absence of actual signal.

If these various effects- transmission distance, detector inefficiency, dark count, faint light source with mean number of photons in a pulse, and uncorrelated photons in entanglement based encoding that can cause errors are considered then a general form of QBER [11] is as follows,

$$QBER = QBER_{wd} + QBER_{dc} + QBER_{ent}$$

Here $QBER_{wd}$ is the error due to wrong detection, $QBER_{dc}$ is error due to dark count and $QBER_{ent}$ is error due to uncorrelated photons which appears only in entanglement based encoding system.

3. Methodology

This research is both theoretical and simulation analysis oriented. Theoretical analysis is performed related to the thesis objective. The BB84 protocol algorithm using both polarization and phase shift encoding are implemented and stimulated in Matlab. In the test, random photon states are produced by the light source. Each random photon states are entered through the two encoders where they undergo polarization and phase shift. These encoded photon that exists from the transmitter are applied to the same noise channel operation. These noise coupled photons enters the receivers where uncorrelated random basis of measurement is applied. The QBER generated are recorded for each of the method. Then a comparative analysis is performed on the result. This result obtained are analyzed and compared with theoretical results obtained by researchers to draw conclusion.

The steps taken the research objective are summarized below,

- Theoretical examination of observables
- Construction of separate simulation model BB84 protocol Polarization encoding and Phase shift encoding
- Data testing, analysis and investigation obtained from the simulated models
- Interpretation of simulation result with theoretical examination

4. Analysis

5. Theoretical Preliminaries

The BB84 protocol, security and QBER was already described in details in the literature review. Here, other essential theoretical aspects relevant to this thesis objective are discussed. First classical theory of electromagnetic waves are described wherein, the polarization of waves and particles are described. Next, the theory of quantum information, the experimental apparatus and finally the measurement process are described.

5.1. Electromagnetic Waves and Polarization

Electromagnetic waves are energy waves which are generated as a result of transition of electrons from higher energy state to lower energy state. The transition of electrons between two energy states causes release of photons. The collection of photons emitted from the atoms constitutes the electromagnetic waves. Hence electromagnetic waves contain number of photons which are in motion. If the Power of the light source is P, and the frequency of the light is f, then the average number of photons per sec (<n>) is given by,

$$\langle n \rangle = P/hf$$

where, h is the plank constant

The emitted electromagnetic wave is made of electric and magnetic fields components which oscillates in two orthogonal directions in a plane which is perpendicular to the direction of the propagation of electromagnetic waves. Each electric and magnetic field can in turn be resolved into two components each having

its own phase. By convention the polarization state of of electromagnetic wave is described by the time varying direction and relative magnitude of the electric field. As such polarization is the curve traced by the end point of the vector arrow representing the instantaneous electric field. And the field is observed along the direction of propagation. The different phase relation of the two electric field components gives different polarization which can be classified into linear, circular or elliptical polarization. These different polarizations are described below.

Linear Polarization is the state of electric field vector of the electromagnetic wave at a point in space in which electric field is always directed along a line. For linearly polarized wave, the phase difference $\Delta\phi$ between the two electric field components is an integer multiple of π. That is, $\Delta\varphi = \varphi_y - \varphi_x = n\pi$ for n=0,1,2,3....Here we denote the horizontally x polarized electric field states by $|\leftrightarrow\rangle$and the vertically y polarized electric field states by $|\updownarrow\rangle$.

Circular polarization is the time harmonic variation of electric field in a given point in space if the electric field (or magnetic field) vector at that point traces a circle as a function of time. The condition for circular polarization is that magnitudes of the two components are equal and the phase difference between the two electric field components is an odd multiple of $\pi/2$. When the phase difference is $+\pi/2$ the direction of rotation of the electric field is clockwise (cw) and the wave is called left circularly polarized and when the phase difference is $-\pi/2$ the direction of rotation is counter clockwise (ccw). and the wave is called right circularly polarization. That is in general, the phase difference($\Delta\varphi$) is such that, $\Delta\varphi = \varphi_y - \varphi_x = (1/2+2n)\pi$ for clockwise direction and $\Delta\varphi = \varphi_y - \varphi_x = -(1/2+2n)\pi$ for counter clockwise direction with n taking integer values n=0,1,2,3 ...These two circular polarizations can be viewed as two orthogonal polarizations. The right and left circular polarization state is denoted here by $|R\rangle$ and $|L\rangle$.

Any state between the linear and circular polarization state is called elliptical polarization.

5.2. Quantum Information Theory

Here in this chapter, the theory of quantum states formalised by QM, the theory of quantum information theory, the entropy and the inequalities of QIT are described

5.2.1. Quantum States

In QIT the qubits is the elementary unit of information like bits in classical information theory. In QIT qubit are quantum state can be represented as a combination of its basis state. The linearly polarized electromagnetic waves- vertical, horizontal, +45 and -45 diagonal polarized electromagnetic waves are ultimately quantum states. We may represent horizontal and vertical linearly polarized states as $|0\rangle$ and $|1\rangle$ respectively in dirac notation of quantum state.

That is,

$|0\rangle = |\leftrightarrow\rangle$ is a horizontally polarized state

$|1\rangle = |\updownarrow\rangle$ is a vertically polarized state

Now, the +45 diagonally polarized(↗) and -45 anti-diagonally polarized states (↖) can be represented as the superposition of linearly horizontal and vertical polarized wave can be written as follows,

$$|+\rangle = |\nearrow\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$$

$$|-> = |↖> (|0> - |1>)/\sqrt{2}$$

Similarly the right circularly and left circularly polarized wave can be written as the superposition of linearly horizontal and vertical polarized wave as follows,

$$|R> = (|0> + i|1>)/\sqrt{2}$$

$$|L> = (|0> - i|1>)/\sqrt{2}$$

5.2.2. Entropies

Central to information theory is the concept of Entropy. As in classical information theory, there are various entropy quantities in QIT. The definition of measure of these entropies in QIT are provided below.

Von Neumann Entropy is defined as follows-

$$S(Q) = -Tr(QlogQ)$$

where, Q is the density matrix of a quantum state and Tr denotes the trace of matrix.

Quantum Relative Entropy is defined as follows,

$$S(Q_1||Q_2) = Tr(Q_1 log Q_1) – Tr(Q_1 log Q_2)$$

where Q_1 and Q_2 are two density of states of two system and Tr( ) denotes trace operation

Quantum Mutual Information is defined as follows,

$S(Q_1{:}Q_2) = S(Q_1) + S(Q_2) - S(Q_1Q_2)$

Quantum Conditional Entropy are defined as follows-

$S(Q_1|Q_2) = S(Q_1Q_2) - S(Q_2)$

and, $S(Q_2|Q_1) = S(Q_1Q_2) - S(Q_1)$

5.2.3. Inequalities of QIT

Here, the important inequalities results of QIT are provided. Any quantum state or system can be described with its density matrix. Given quantum states or sub-systems of a system described by density matrix Q_1, Q_2 and $Q_{12}$with corresponding Von Neumann entropies $S(Q_1)$, $S(Q_2)$ and $S(Q_1,Q_2)$then we have the following inequalities in QIT.

Klein Inequality states that the quantum relative entropy is non-negative and is expressed as below

$$S(Q_1||Q_2) \geq 0$$

with equality if and only if $Q_1 = Q_2$

Fano Inequality states that if Q_1 and Q_2 are density matrices such that the trace distance between them satisfies $Tr(Q_1,Q_2) \leq 1/e$, then

$$|S(Q_1)-S(Q_2)| \leq Tr(Q_1,Q_2)\ \log d + \eta(T(Q_1,Q_2))$$

Subadditivity Inequality states the following entropy inequality relation for sub-system 1, sub-system2 and joint system12.

$$S(Q_1,Q_2) \leq S(Q_1) + S(Q_2)$$

Similarly, the Triangular inequality states the following entropy inequalities for system consisting of of sub-system 1, sub-system2 and joint system12.

$$S(Q_1,Q_2) \geq |S(Q_1) + S(Q_2)|$$

5.3. Optical Instruments

Here optical components will be described as they are used produce, detect and manipulate different quantum states in experimental laboratory. First two forms of beam splitters(BM)- the 50:50 beam splitter and Polarization Beam Splitter (PBS) are described then two wave retarders- Quarter Wave Plate (QWP) and Half Wave Plates (HWP) which are light transparent birefringent crystal materials are described. A material is said to be birefringent if the speed of light through the material varies relative to the polarization orientation state of the incident light ray. The property of such material is that the speed of light is faster in one polarization direction called the fast axis and slower in the other polarization direction called the slow axis. Finally, the Mach Zehnder Interferometer(MZI) are described which is used for observing interference of two particles and is used in phase encoding.

5.3.1. Beam Splitter

A beam splitter is an optical device that splits light beam into two parts. Here the

effect of beam splitter and quantum nature of light is described. When electromagnetic wave of electric field intensity E, and power $P_{in}= |E|^2$ is incident on a 50:50 beam splitter then the beam will split into two beams of equal E-field amplitude $E/\sqrt{2}$. The two detectors placed in the path of the output beams will measure equal EM power of $P_{out}=P_{in}/2$. This is shown in the figure below.

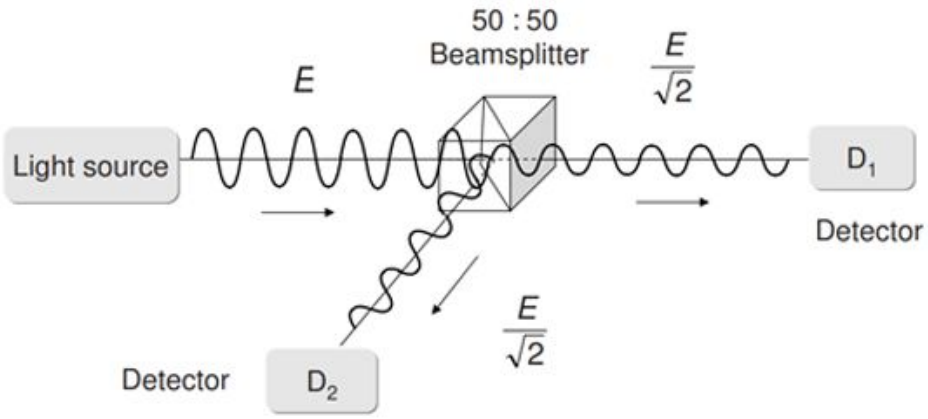

Figure 3: Dividing an EM light beam through a 50:50 beam splitter resulting in two beams of detected powers both equal to P/2

Now, when the power of the electromagnetic wave light source is reduced by proper amount then it is possible to emit single photon per unit time. When the emitted single photons are incident on the beam splitter then each of them will choose one of the two possible paths randomly. This is because photons cannot be split as they are elementary particles of quanta energy. The paths that these photons take are recorded in the single photon detectors (SPD). The numbers of pings generated at each of the single photon detectors over a period of time are equal. Thus, the probability of that each photon will take the straight path or the reflection path is equal to ½. This is illustrated in the picture below:

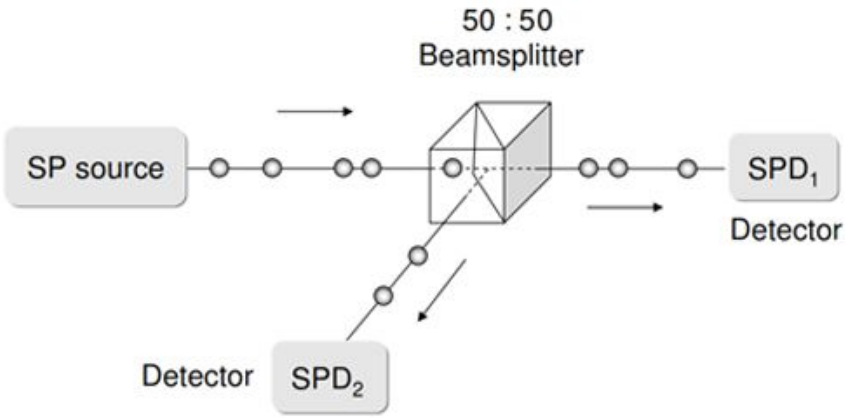

Figure 4: Same experimental setup with single photon (SP) being emitted and detected

5.3.2. Polarization Beam Splitter

The Polarization Beam Splitter (PBS) is a special assembly of birefringent crystal prism whose effect is to separate an incident polarized or unpolarized light beam into two orthogonally polarized components. This is used in polarization decoding to separate horizontal and vertical polarized photos as illustrated by the figure below.

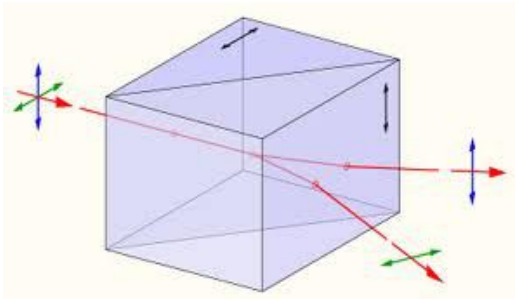

Figure 5: Polarization Beam Splitter

5.3.3. Quarter Wave Plates

A Quater Wave Plate(QWP) is a light transparent birefringent crystal materials which produces a relative phase change of $\Delta\phi = \pi/2$ between the components of the electric field. This can be obtained by controlling the thickness of the QWP. Thus QWP can be used to convert linearly polarized wave or photons into circularly polarized wave or photons and vice versa.

That is,

$$|+> \rightarrow |R>$$

$$|-> \rightarrow |L>$$

And,

$$|R> \rightarrow |+>$$

$$|L> \rightarrow |->$$

This transformation is equivalent to Hadamard gate action as follows:

$$H|0> = |+>$$

$$H|1> = |–>$$

$$H|+> = |0>$$

$H|-\rangle = |1\rangle$

The figure below illustrates this action of QWP,

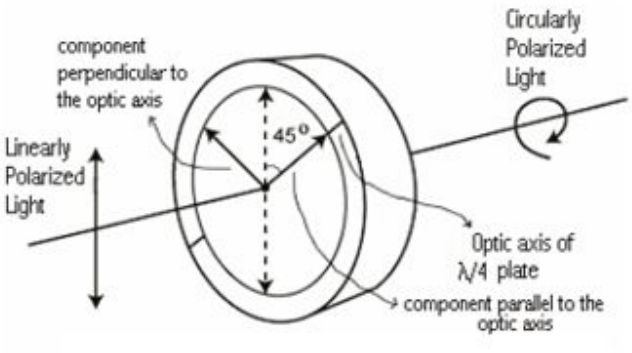

Figure 6: QWP Action

5.3.4. Half Wave Plates

Half wave plates (HWP) are light transparent birefringent crystal materials that produces a net phase delay between two orthogonal electric field components by π or one half of the wavelength. When the linearly polarized photons are incident on HWP the basis $\{\leftrightarrow, \updownarrow\}$ are interchanged. For this the fast axis of the plate must be oriented at 45° of the incident E-field polarization direction. Since this phase shift corresponds to a factor of $e^{i\pi} = -1$, the sign of one of the two polarization component is reversed and the result is a 90° rotation of the incident linear polarization. This HWP effect on linearly polarized photon is equivalent to action of Pauli matrix X on the $|0\rangle$ and $|1\rangle$.

That is,

$X|0\rangle = |1\rangle$

$$X|1> = |0>$$

Similarly, when +45 diagonally and -45 anti-diagonally polarized photons are incident on HWP the basis {↗,↖} are interchanged. However, unlike in case of HWP the fast axis of the plate is not changed that is 0°. This causes the change in direction of rotation of the incident circularly polarized waves. This HWP effect on circularly polarized photon is equivalent to action of Pauli matrix Z on the |+> and |->quantum states.

That is,

$$X|+> = |->$$

$$X|-> = |+>$$

The action of HWP is illustrated below,

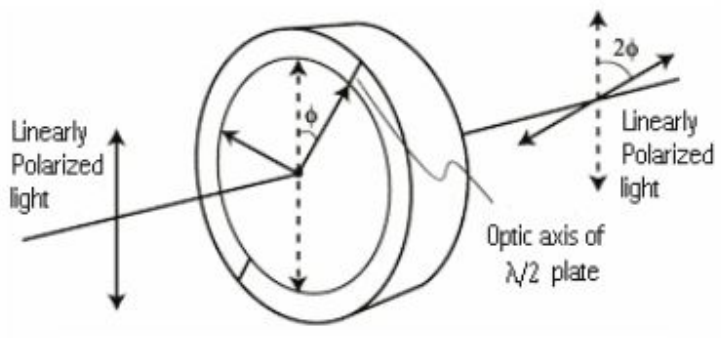

Figure 7: HWP Action

5.3.5. Mach Zehnder Interferometer

Mach Zehnder Interferometer is an apparatus set up and also a device that can be used to measure the interference pattern produced by constructive and destructive interference of light. In this a light is first split by a beam splitter into two parts, then one part is phase shifted by controlling the distance it travels or by using phase shifter in that path while the other part is allowed to travel without phase shift. Then the two beams of particles which undergoes phase shift and no phase shift are recombined by a second beam splitter. Depending upon the phase shift acquired by one part constructive and destructive interference is observed at the detector A and B.

The principle of operation of Mach Zehnder Interferometer is illustrated below.

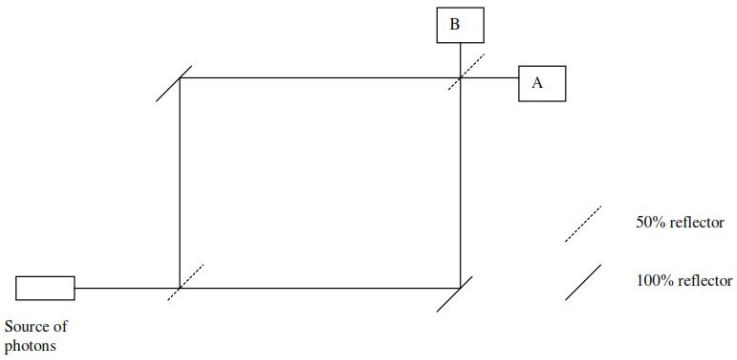

Figure 8: Mach Zehnder Interferometer

In the picture above, the dotted line 50% reflectors are beam splitters and the solid 100% reflectors are mirrors and A and B are detectors.

5.4. Measurement of Polarized States

Here the measurement and detection of linearly polarized photons and circularly polarized photons will be described next.

5.4.1. Measurement of Linearly Polarized Photons

The linearly polarized photons can be detected and measured by using one polarization beam splitter (PBS) and two single photon detectors (SPD) as shown in the figure below.

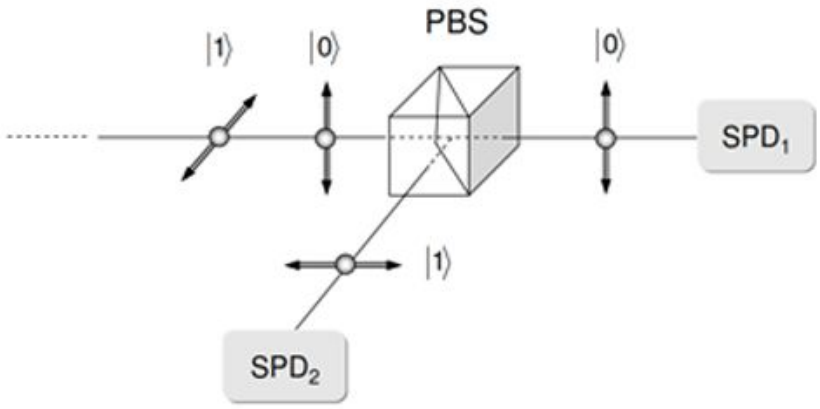

Figure 9: Splitting of light beam of single, linearly polarized photons through a PBS

SPD1 placed in the straight through path only detects vertically polarized or |0> photons, while the SPD2 placed in the reflection path detects only horizontally polarized or |1> photons. If a count is obtained from SPD1 or SPD2 we can attribute +1 or -1 respectively to these possible measurements.

This corresponds to measurement in the Z-basis in quantum mechanics. The eigenvectors and eigenvalues of Z operators are |0>, |1> and ±1. The transformation is,

$$Z|0\rangle = |0\rangle$$

or,

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

and,

$$Z|1\rangle = - |1\rangle$$

or,

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

5.4.2. Measurement of Circularly Polarized Photons

Similarly, to measure circular polarization state of photons, the circularly polarized photons are transformed into linearly polarized states first by QWP and then detected by the PBS-SPD1-SPD2 combination as in figure below.

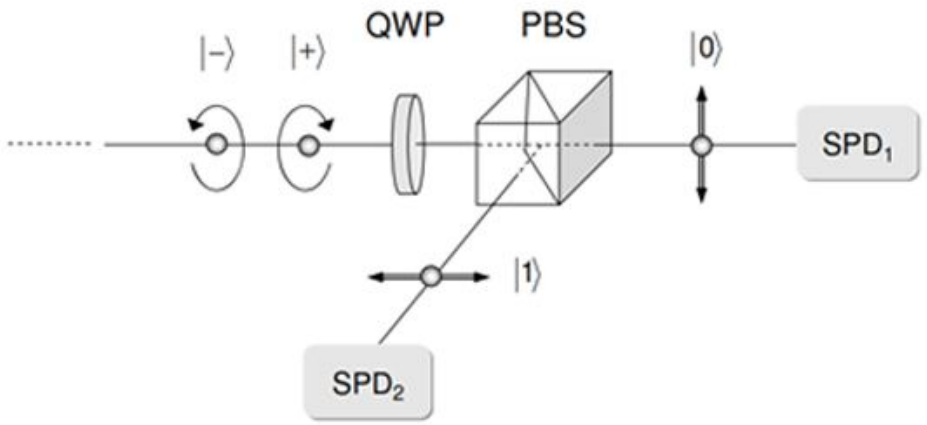

Figure 10: : Measurement and Detection for Circularly Polarized Photons

Thus, QWP-PBS-SPD1-SPD2 constitutes a quantum measurement apparatus to determine the state of circularly polarized photons. If a count is obtained in the SPD1 then we can attribute +1 and if a count is obtained in SPD2 then we can attribute -1 value. This corresponds to measurement in the X-basis as the eigenvector and eigenvalue of X are |+>,|-> and ±1.

That is,

$X|+> = |+>$

or $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

And,

$X|-> = |->$

or, $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = -\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$

6. Analysis and Simulation

Here theoretical and simulation analysis are provided.

Let us consider the transmitter section. In the transmitter, the sender, Alice generates photons and quantum state of a single photon can be described by the following equivalent Jones vector notation,

$$|\psi\rangle = \begin{bmatrix} \cos\theta \\ \sin\theta e^{i\varphi} \end{bmatrix}$$

where, θ is the angle made by electric field vector with the x-axis and φ is the phase difference between the x and y component. Both θ and φ are assumed to have random uniform distribution.

Such state can also be represented in density matrix form as,

$$Q_\psi = \begin{pmatrix} \cos^2\theta & \cos\theta \sin\theta e^{-i\varphi} \\ \cos\theta \sin\theta e^{i\varphi} & \sin^2\theta \end{pmatrix}$$

The sender also generates N uniformly distributed random binary bits according to which the photons(Q_Ψ) are encoded into polarization and phase shifted photonic states. The corresponding encoding lookup table are as follows.

Alice Random Bits	Polarized Encoded State	Encoded Quantum State	State Vector
00	Horizontally Polarized	|0>	$\begin{pmatrix}1\\0\end{pmatrix}$
10	+45 Diagonally Polarized	|+>	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$
01	Vertically Polarized	|1>	$\begin{pmatrix}0\\1\end{pmatrix}$
11	-45 Diagonally Polarized	|->	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$

Alice Random Bits	Phase Encoded State	Quantum State	State Vector
00	0	|0>	$\begin{pmatrix}\cos\theta\\ \sin\theta e^{i\varphi}\end{pmatrix}$
01	$\pi/2$	|+>	$i\begin{pmatrix}\cos\theta\\ \sin\theta e^{i\varphi}\end{pmatrix}$

10	π	|1>	$-\begin{pmatrix}\cos\theta \\ \sin\theta e^{i\varphi}\end{pmatrix}$
11	3π/2	|->	$-i\begin{pmatrix}\cos\theta \\ \sin\theta\end{pmatrix}$

Now, lets look at the communication channel. The photonic encoded states enters the quantum communication channel. It is described by a unitary operator Ɛ that acts on the transmitted quantum states. The quantum channels is modeled as a depolarizing channel that acts on the transmitted qubits, equivalently its density matrix(Q_Ψ) as follows-

$$Q\gamma = \mathcal{E}(Q_\Psi) = p_c I/2 Q_\Psi + (1-p_c)Q_\Psi$$

where, p_c is the probability that the channel input state described by Q_Ψ is transformed into a mixed state and $(1-p_c)$ is the probability that the input state is remains unaffected by the channel noise. Also I is the unit matrix.

Here, p_c is modeled as a uniformly distributed random probabilities.

Finally, the noise coupled signal are detected and measured at the receiver. Here each Qγ received is measured with N randomly generated X and Z basis operator in case of polarization encoding or 0 and π/2 basis in case of phase shift encoding which correspond.

These measurements are described by the following relation,

If Z was generated then the expected value of Z is,

$$\langle Z \rangle = Tr(ZQ\gamma)$$

And if X was generated then the expected value of X is,

$$\langle X \rangle = Tr(XQ\gamma)$$

Thus we get the expected value of the Z and X operators. These also represents the probability of correctly identifying the state $Q\gamma$.

Then the probability of wrong detection or probability of errors for the Z and X measurements as follows-

$$Pe(z) = 1-\langle Z \rangle$$

$$Pe(x) = 1-\langle X \rangle$$

The total probability of error is given by,

$$Pe = \frac{1}{2^{nR}} \sum_{j=X,Z} Pe(j)$$

As previously described in the QBER literature chapter, the QBER can be expressed as,

$$QBER = QBER_{wd} + QBER_{dc} + QBER_{ent}$$

However, this thesis is not concerned with detector efficiency, dark counts and entanglement based encoding implementation, the two factors $QBER_{dc}$, $QBER_{ent}$ are not essential and can be dropped out. The QBER that is of interest here is the $QBER_{wd}$ which is only concerned with the wrong detection of photons due to channel noise and wrong basis selection. This term then can be expressed as follows,

$$QBER = QBER_{wd} = p_{wd}$$

where, p_{wd} is the probability of wrong detection

This probability(Pe) is provided above.

7. Results and Discussions

A simulation model for the BB84 protocol was constructed with polarization and phase encoding. A photon source is considered that produced photons with random polar and azimuthal angles (θ,φ), which is then subsequently encoded in polarized and phase encoded form. These encoded photon was acted by channel noise and decoded with random basis. QBER was finally calculated for both the encoding methods.

Shown below are results of the simulation for N=32 , 64 and 128 key bits.

For N=32

Alice Basis: 1 1 1 0 0 0 0 0 1 1 0 0 1 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 1 1 0 1

Bob Basis: 1 0 0 0 1 1 1 0 0 0 0 1 0 1 0 1 0 1 0 0 1 0 0 1 0 0 0 0 0 1 0 0

Bob Result: 1 1 1 0 0 1 0 1 0 0 1 0 1 1 1 1 1 0 1 0 0 0 1 1 0 1 0 0 1 0 0 1

Basis Compared Result: 1 0 0 1 0 0 0 1 0 0 1 0 0 0 1 0 1 0 1 1 1 1 1 0 1 1 1 1 0 1 1 0

Shifted Key: 1 0 1 1 1 1 1 0 0 0 1 0 1 0 0 0 0

Polarization Shifted Key Length: 17

QBER: 0.46875

Alice Basis: 0 1 1 0 1 1 1 1 1 0 0 0 0 0 0 0 1 0 0 0 0 0 1 1 1 0 1 0 0 0 1 0

bob Basis: 0 0 0 0 0 0 1 1 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0

Result: 1 9 9 1 9 9 0 1 9 9 1 9 0 9 1 0 9 1 1 0 0 0 9 9 9 0 9 1 9 1 0 1

Basis Compared Result: 1 0 0 1 0 0 1 1 0 0 1 0 1 0 1 1 0 1 1 1 1 1 0 0 0 1 0 1 0 1 1 1

Shifted Key: 1 1 0 1 1 0 1 0 1 1 0 0 0 0 1 1 0 1

Phase Shifted Key Length: 18

QBER: 0.4375

For N=64

Alice Basis: 1 1 1 0 1 1 0 1 0 0 1 0 1 0 1 0 1 1 1 1 0 1 0 0 1 1 0 1 1 1 0 0 1 0 1 0 0 0 1 1 0 1 0 0 1 0 0 0 0 1 0 1 1 1 1 1 1 1 0 1 0 0 0 0

Bob Basis: 1 1 0 0 1 1 1 1 0 0 1 1 1 0 1 1 0 0 0 1 0 1 0
0 0 1 1 1 1 0 0 1 1 1 0 0 1 1 1 1 0 1 1 1 1 1 0 1 1 0
1 1 0 0 0 1 0 0 1 0 0 0 0 1

Bob Result: 0 1 0 0 0 0 1 1 1 0 0 1 1 0 0 0 1 1 0 1 0 1 0
1 1 0 0 1 1 1 0 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 1 0
1 0 0 0 1 1 0 1 0 0 1 0 0 1

Basis Compared Result: 1 1 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 0
1 1 1 1 1 0 1 0 1 1 0 1 0 1 0 0 1 0 0 1 1 1 1 0 0 1 0
1 0 0 0 0 1 0 0 0 1 0 0 0 0 1 1 1 0

Shifted Key: 0 1 0 0 0 1 1 0 0 1 0 0 1 0 1 0 1 0 1 1 0 0 1
0 0 0 0 0 1 0 1 1 0 0

Polarization Shifted Key Length: 34

QBER: 0.46875

Alice Basis: 1 0 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 1
0 0 1 0 0 0 0 0 1 1 0 1 0 0 0 0 0 0 1 1 0 0 0 0 0 1 0
0 0 1 0 0 0 0 0 0 0 0 1 0 1

bob Basis: 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0 0 0
0 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0
1 0 0 0 1 0 0 0 0 0 0 1 1 0

Result: 9 9 1 1 1 9 1 1 9 0 0 1 1 1 0 1 0 9 1 0 1 1 9 1

0 9 1 0 0 9 1 9 9 1 9 1 9 1 1 0 1 0 9 9 1 1 1 0 9 1 9 1 9 1 1 0 1 1 1 0 9 9

Basis Compared Result: 0 0 1 1 1 0 1 1 0 1 1 1 1 1 1 1 1 0 1 1 1 1 0 1 1 1 0 1 1 0 1 1 1 0 1 0 0 1 0 1 0 1 1 1 1 1 0 0 1 1 1 1 0 1 0 1 0 1 0 1 1 1 1 1 1 1 0 0

Shifted Key: 1 1 1 1 1 0 0 1 1 1 0 1 0 1 0 1 1 1 0 1 0 0 1 1 1 1 1 0 1 0 1 1 1 0 1 1 1 1 1 0 1 1 1 0

Phase Shifted Key Length: 44

QBER: 0.3125

For N=128

Alice Basis: 0 0 0 0 0 1 0 1 1 1 1 0 0 1 1 1 0 0 1 0 1 1 1 0 0 1 0 1 0 1 0 0 1 1 1 0 1 0 0 1 1 1 1 0 0 1 1 0 0 1 0 0 0 0 1 1 1 1 1 1 1 0 1 1 1 0 0 0 0 0 1 0 1 0 1 1 0 1 0 1 1 0 1 0 0 0 1 0 1 0 1 0 0 1 1 1 0 1 1 1 0 0 0 1 1 0 1 1 0 0 0 0 0 1 0 0 1 1 0 0 0 1 0 1 1 0 1

Bob Basis: 0 0 1 0 1 0 0 0 0 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 1 1 0 0 0 1 0 1 1 1 0 1 0 1 1 0 0 1 1 1 1 1 0 0 1 0 1 0 0 0 0 1 1 1 1 1 1 1 0 1 0 1 1 0 0 1 0 1 1 0 1 1 1 1 0 0 0 0 0 1 0 1 1 1 1 1 1 0 1 0 0 1 1 1 1 0 1 1 0 1 1 0 0 0 1 1 0 0 1 1 1 0 1 1 1 0 0 0 1 1

Bob Result: 0 1 1 0 0 0 1 1 0 0 0 1 1 0 1 1 1 1 1 0 1 1 0
0 0 1 1 1 0 1 0 1 0 1 1 1 1 1 1 0 0 1 1 0 1 0 0 0 0 0
1 0 1 0 0 0 1 1 0 1 0 1 0 1 1 1 1 0 1 1 1 1 0 0 1 1 1
0 1 0 0 1 1 1 1 0 1 0 1 0 0 0 0 0 0 1 0 0 0 0 1 1 1 0
0 0 0 0 1 0 1 1 1 1 1 0 1 1 1 1 0 1 0 1 0 1 1 1

Basis Compared Result: 1 1 0 1 0 0 1 0 0 0 1 1 1 0 0 0 1 1 1
0 0 0 1 1 0 1 1 0 1 1 1 0 1 1 0 0 0 0 0 0 0 1 1 1 0 0
0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 0 1 1 0 1 1 0
0 0 1 1 0 0 1 1 1 0 1 0 1 1 0 1 0 0 0 0 0 1 1 1 0 0 1
0 1 0 0 1 1 1 1 1 1 1 1 0 0 0 1 0 1 1 1 0 0 1 1 0 0 0
1

Shifted Key: 0 1 0 1 0 1 1 1 1 1 0 0 1 1 0 1 0 0 1 1 1 0 0
1 0 1 0 0 0 1 1 0 1 0 1 0 1 1 0 1 1 1 1 1 0 0 1 1 0 1
1 0 1 0 0 1 0 0 0 0 1 0 1 1 0 1 1 1 0 1 1

Polarization Shifted Key Length: 71

QBER: 0.44531

Alice Basis: 0 1 0 1 0 0 1 0 0 0 0 0 1 0 0 1 1 1 0 0 0 0 0
0 1 0 1 0 0 0 1 0 1 1 0 0 0 0 0 1 0 0 0 0 1 1 0 1 0 1
0 0 0 1 0 0 0 0 0 1 0 1 0 0 1 0 1 0 0 0 0 1 0 1 0 1 1
0 0 0 1 1 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1
0 0 0 1 0 1 0 0 1 0 0 0 1 1 0 0 1 1 1 0 0 0 0 0

bob Basis: 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

1 1 0 0 0 1 0 0 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 1 1
0 0 0 0 0 0 0 0 0 0 0 1 1 1 0 0 0 1 0 0 0 1 0 1 0 0 0
0 1 0 1 0 0 0 0 0 0 0 0 0 1 1 0 0 0 0 1 0 1 0 1 0 0 0
0 1 1 0 0 1 0 1 0 0 0 1 1 1 1 0 0 0 0 0 0 0 1 0

Result: 9 0 0 9 0 1 9 1 1 0 1 1 9 0 0 9 9 9 0 1 0 1 1 9
1 0 9 0 9 0 9 1 9 9 1 9 0 9 1 9 0 1 0 0 9 9 1 9 9 1 1
1 1 9 1 1 0 1 1 9 1 0 9 9 9 1 9 9 1 1 1 1 0 1 0 9 9 1
9 1 1 9 1 9 1 1 1 1 1 0 9 9 9 1 1 1 9 1 9 0 9 1 1 9 1
9 9 9 1 0 0 9 9 1 0 9 0 1 9 0 9 9 9 1 1 1 9 1

Basis Compared Result: 0 1 1 0 1 1 0 1 1 1 1 1 0 1 1 0 0 0 1
1 1 1 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 1 1 1 0 0
1 0 0 1 1 1 1 0 1 1 1 1 1 0 1 1 0 0 0 1 0 0 1 1 1 1 1
1 1 0 0 1 0 1 1 0 1 0 1 1 1 1 1 1 0 0 0 1 1 1 0 1 0 1
0 1 1 0 1 0 0 0 1 1 1 0 0 1 1 0 1 1 0 1 0 0 0 1 1 1 0
1

Shifted Key: 0 0 0 1 1 1 0 1 1 0 0 0 1 0 1 1 1 0 0 0 1 1 0
1 0 1 0 0 1 1 1 1 1 1 1 0 1 1 1 0 1 1 1 1 1 0 1 0 1 1
1 1 1 1 1 1 1 0 1 1 1 1 0 1 1 1 1 0 0 1 0 0 1 0 1 1 1
1

Phase Shifted Key Length: 78

QBER: 0.39063

8. Conclusion

From the foregoing result, we see that both polarization and phase shift encoding protocols produces almost half bits as shifted key for input N bits. The result also shows that the phase shift encoding produced more shifted key resulting less QBER. We can say that phase shift encoding on arbitrary quantum state of photons produces less error.

9. References

[1] C.E. Shannon. "*A Mathematical Theory Of Communication*" Bell Syst.Tech.J, 1948

[2] M.A Nielsen and I.L.Chuang, *Quantum Computation and Quantum Information*. Cambridge Univ. Press, 2000

[3] C. H. Bennett and G. Brassard. "Quantum Cryptography: Public key distribution and coin tossing," in Proc. IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, 1984, pp. 175

[4] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," Phys.Rev.Lett. 68. 3121, May. 1992.

[5] C. H. Bennett, G. Brassard, C. Cr´epeau, and U. M. Maurer,"Generalized Privacy Amplification," IEEE Trans. Inf. Theo. 41, 1915 (1995).

[6] C. H. Bennett, "Intercept-resend attacks in the Bennett-Brassard 1984 quantum-key-distribution protocol with weak coherent pulses," Phys. Rev. A 71, 062301, Jun. 2005.

[7] Fabio Grazioso, Frédéric Grosshans, "Photon-Number-Splitting-attack resistant Quantum Key Distribution Protocols without sifting", Laboratoire de Photonique Quantique et Moléculaire, France, Université de Montréal, Canada Laboratoire Aimé, France, September, 2013

[8] Mustapha Dehmani, Hamid Ez-Zahraouy, Abdelilah Benyoussef, "Quantum Cryptography with Several Cloning Attacks", Laboratory of Magnetism and High

Energy Physics, Journal of Computer Science 6 (7): 684-688, 2010, ISSN 1549-3636, 2010 Science Publications.

[9] Cyril Branciard, Nicolas Gisin, Barbara Kraus, Valerio Scarani, "Security of two quantum cryptography protocols using the same four qubit states", Group of Applied Physics, University of Geneva, February 1, 2008

[10] Agnes Ferenczi, Varun Narasimhachar, and Norbert Lutkenhaus, "Security proof of the unbalanced phase-encoded BB84 protocol", Institute for Quantum Computing & Department for Physics and Astronomy, University of Waterloo, 200 University Avenue West, N2L 3G1, Waterloo, Ontario, Canada, Jun, 2012.

[11] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, Quantum cryptography, *Rev. Mod. Phys.,* 2002, 74**,** 145.

[12] Muhammad Mubashir Khan, Salahuddin Hyder, Mahmood K Pathan, Kashif H Sheikh, "A Quantum Key Distribution Network Through Single Mode Optical Fiber", International Symposium on Collaborative Technologies and Systems, May 14-17, 2006 Las Vegas, Nevada, USA

[13] Muhammad Mubashir Khan, Michael Murphy, Almut Beige, "High error-rate quantum key distribution for long distance communication", arxiv.org/abs/0901.3909v4

[14] N. Antonietti, M. Mondin, F. Daneshgaran, G. Giovanelli, I. Kostadinov, B. Lunelli, "Quantum bit error rate in modeled atmospheres" International Journal of Quantum Information, World Scientific Publishing Company, Aug, 2008

[15] Y.-S. Kim, Y.-C. Jeong, and Y.-H. Kim, "Implementation of Polarization-Coded Free-Space BB84 Quantum Key Distribution" ISSN 1054-660X, Laser Physics, 2008, Vol. 18, No. 6, pp. 810–814

[16] Id Quantique, URL: http://www.idquantique.com

[17] QuintessenceLabs, URL: http://qlabsusa.com

10. Appendices

10.1. BB84 Algorithm Code

```
clc
clear all

N = input('Enter the number of input bits(N)=');

% ----- Parameter Initialization----------------

% ------Polarization Encoding Initialization & preallocation ----------

Pol=zeros(2,N);                    % : zeros(no. of rows, no. of columns)
alice_basis=zeros(1,N);
bob_basis=zeros(1,N);
basis=zeros(2,2);
bob_result_state=zeros(2,2);
bob_state=zeros(1,N);
bob_result=zeros(1,N);
compare=zeros(1,N);
basis_pol_info=zeros(1,N);
shifted_key_pol=zeros(1,N);

n=zeros(1,N);
m=zeros(1,N);

X=[0 1;1 0];
Z=[1 0;0 -1];

% ------Polarization Encoding Initialization ----------

% Phase Shift at the Transmitter

alpha1 = exp(1i*cos(0));                    % basis 0
alpha2 = exp(1i*cos(pi/2));                 % basis 1
alpha3 = exp(1i*cos(pi));                   % basis 0
alpha4 = exp(1i*cos(3*pi/2));               % basis 0

% Phase Shift at the Receiver

beta1 = exp(1i*cos(0));                     % basis 0
beta2 = exp(1i*cos(pi/2));                  % basis 1
beta3 = exp(1i*cos(pi));                    % basis 0
```

```
beta4 = exp(1i*cos(3*pi/2));                    % basis 1

path = zeros(1,N);
Out = zeros(2,N);
result =zeros(1,N);

a = zeros(1,N);
b = zeros(1,N);
c = zeros(1,N);
d = zeros(1,N);
e = zeros(1,N);
f = zeros(1,N);
g = zeros(1,N);
h = zeros(1,N);

alice_basis_phase = zeros(1,N);
bob_basis_phase = zeros(1,N);
basis_phase_info = zeros(1,N);

% ----- Start of Loop ---------------------------------------

for k=1:N;

    % ---------------- Input State Initialization ------------------------

    theta(k) = 180 * rand;
    phi(k) =   360 * rand;

    P(:,k) = [cos(theta(k)) sin(theta(k))*exp(1i*phi(k))]';

    % --------------- Polarization Encoding Starts ----------------------

    %---------------- Alice produces random polarized states----------------

            n(k)=randi([0,1]);
            m(k)=randi([0,1]);

                    if ((n(k)==0)&&(m(k)==0))
                        Pol(:,k) = [1 0;0 0]*P(:,k);
                        alice_basis(k)=0;
                    elseif ((n(k)==0)&&(m(k)==1)),
                        Pol(:,k) = 1/2*[1 1;1 1]*P(:,k);
                        alice_basis(k)=1;
                    elseif ((n(k)==1)&&(m(k)==0)),
```

```
            Pol(:,k) = [0 0;0 1]*P(:,k);
            alice_basis(k)=0;
        elseif ((n(k)==1)&&(m(k)==1)),
            Pol(:,k) = 1/2*[1 -1;-1 1]*P(:,k);
            alice_basis(k)=1;
        end

%   ---------------- Bob generates random Z,X basis -------------------

        B(k)=randi([0,1]);
            if(B(k)==0)
                basis(:,:,k) = Z;      % Z
                bob_basis(k)=0;
            else
                basis(:,:,k) = X;      % X
                bob_basis(k)=1;
            end

% -------------- Bob generated basis acts on received photons --------

        if(bob_basis(k)==0)
            bob_result_state(:,k)=Z*Pol(:,k);
        else
            bob_result_state(:,k)=X*Pol(:,k);
        end

% ------------- To calculate the bits corresponding to decoded bob state

            if(bob_result_state(:,k)==([1 0;0 0]*P(:,k)))
                bob_state(k)=1;
            elseif(bob_result_state(:,k)==((1/2)*[1 1;1 1]*P(:,k)))
                bob_state(k)=2;
            elseif(bob_result_state(:,k)==(-[0 0;0 1]*P(:,k)))
                bob_state(k)=3;
            elseif(bob_result_state(:,k)==((-1/2)*[1 -1;-1 1]*P(:,k)))
                bob_state(k)=4;
            else
                bob_state(k)=5;
            end

% ------------ Bob measurement result ---------------------

        if(bob_basis(k)==0 && bob_state(k)==1)          % Z basis and H
            bob_result(k) = 1;
```

```
elseif(bob_basis(k)==0 && bob_state(k)==2)       % Z basis and D
    bob_result(k) = randi([0,1]);

elseif(bob_basis(k)==0 && bob_state(k)==3)       % Z basis and V
    bob_result(k) = 0;

elseif(bob_basis(k)==0 && bob_state(k)==4)       % Z basis and A
    bob_result(k) = randi([0,1]);

elseif(bob_basis(k)==1 && bob_state(k)==1)       % X basis and H
    bob_result(k) = randi([0,1]);

elseif(bob_basis(k)==1 && bob_state(k)==2)       % X basis and D
    bob_result(k) = 1;

elseif(bob_basis(k)==1 && bob_state(k)==3)       % X basis and V
    bob_result(k) = randi([0,1]);

elseif(bob_basis(k)==1 && bob_state(k)==4)       %X basis and A
    bob_result(k) = 0;

elseif((bob_basis(k)==0 || bob_basis(k)==1) && bob_state(k) == 5)
    bob_result(k) = randi([0,1]);
end

% --------- Polarization Basis Comparision -------------------------------

                                compare(k)=xor(alice_basis(k),bob_basis(k));

                                    if(compare(k)==0)
                                        basis_pol_info(k) = 1;
                                    else
                                        basis_pol_info(k) = 0;
                                    end

                                    if(basis_pol_info(k)== 1)
                                       shifted_key_pol(k)=bob_result(k);
                                    else
                                       shifted_key_pol(k)= 5;
                                    end
                                    ind_pol(k) = (shifted_key_pol(k)==5);

%--------Polarization Encoding Ends-----------------
```

```
% -----------Phase Encoding Starts ----------------

mod1(:,k) = alpha1*P(:,k);                                  % Phase Shift
Modulated State
mod2(:,k) = alpha2*P(:,k);
mod3(:,k) = alpha3*P(:,k);
mod4(:,k) = alpha4*P(:,k);

demod1(:,k) = beta1*P(:,k);                                 % Phase Shift
demodulated State
demod2(:,k) = beta2*P(:,k);
demod3(:,k) = beta3*P(:,k);
demod4(:,k) = beta4*P(:,k);

% --------- Random Path Generation --------------

path(k)=rand;

% -------- Path 1 -----------------------------

if (0<path(k) && path(k)<=0.25)
    Out(:,k) = P(:,k);
    alice_basis_phase(k) = 0;
    bob_basis_phase(k) = 0;
    result(k) = 1;

% -------- Path 2 -----------------------------

elseif (0.25<path(k) && path(k)<=0.5),     % Path 2 is chosen: Photon travels
through the transmitter Phase shifter but not through the receiver phase shifter

                a(k)=randi([0,1]);
                b(k)=randi([0,1]);


                    if (a(k)==0&&b(k)==0)              %a(0)b(0) = 00 => 0
phase shift
                        Out(:,k) = mod1(:,k);
                        alice_basis_phase(k) = 0;
                        bob_basis_phase(k) = 0;
                        result(k) = 1;
                    elseif (a(k)==0&&b(k)==1),        %a(0)b(1) = 00 => pi/2
phase shift
```

```
                    Out(:,k) = mod2(:,k);
                    alice_basis_phase(k) = 1;
                    bob_basis_phase(k) = 0;
                    result(k) = 9;
                elseif (a(k)==1&&b(k)==0),        %a(1)b(0) = 00 => pi
phase shift
                    Out(:,k) = mod3(:,k);
                    alice_basis_phase(k) = 0;
                    bob_basis_phase(k) = 0;
                    result(k) = 0;
                elseif  (a(k)==1&&b(k)==1),        %a(1)b(1) = 00 =>
3pi/2 phase shift
                    Out(:,k) = mod4(:,k);
                    alice_basis_phase(k) = 1;
                    bob_basis_phase(k) = 0;
                    result(k) = 9;
                end

    % -------- Path 3 ------------------------------

   elseif (0.5<path(k) && path(k)<=0.75),                % Third Path is Chosen-
Photon travels through the straight path at the transmitter

        c(k)=randi([0,1]);
        d(k)=randi([0,1]);

                if (c(k)==0&&d(k)==0)
                    Out(:,k) = demod1(:,k);
                    alice_basis_phase(k) = 0;
                    bob_basis_phase(k) = 0;
                    result(k) = 1;

                elseif (c(k)==0&&d(k)==1),
                    Out(:,k) = demod2(:,k);
                    alice_basis_phase(k) = 0;
                    bob_basis_phase(k) = 1;
                    result(k) = 9;

                elseif (c(k)==1&&d(k)==0),
                    Out(:,k) = demod3(:,k);
                    alice_basis_phase(k) = 0;
                    bob_basis_phase(k) = 0;
                    result(k) = 0;
```

```
                elseif (c(k)==1&&d(k)==1),
                    Out(:,k) = demod4(:,k);
                    alice_basis_phase(k) = 0;
                    bob_basis_phase(k) = 1;
                    result(k) = 9;
                end

% -------- Path 4 -----------------------------

elseif(0.75<path(k) && path(k)<1),

                e(k)=randi([0,1]);
                f(k)=randi([0,1]);

                    if (e(k)==0&&f(k)==0)

                            g(k)=randi([0,1]);
                            h(k)=randi([0,1]);

                                        if (g(k)==0&&h(k)==0)
                                            Out(:,k) = (alpha1+beta1)*P(:,k);
                                            alice_basis_phase(k) = 0;
                                            bob_basis_phase(k) = 0;
                                            result(k) = 1;

                                        elseif (g(k)==0&&h(k)==1),
                                            Out(:,k) = (alpha1+beta2)*P(:,k);
                                            alice_basis_phase(k) = 0;
                                            bob_basis_phase(k) = 1;
                                            result(k) = 9;

                                        elseif (g(k)==1&&h(k)==0),
                                            Out(:,k) = (alpha1+beta3)*P(:,k);
                                            alice_basis_phase(k) = 0;
                                            bob_basis_phase(k) = 0;
                                            result(k) = 0;

                                        elseif (g(k)==1&&h(k)==1),
                                            Out(:,k) = (alpha1+beta4)*P(:,k);
                                            alice_basis_phase(k) = 0;
                                            bob_basis_phase(k) = 1;
                                            result(k) = 9;
                                        end
```

```
elseif (e(k)==0&&f(k)==1),

        g(k)=randi([0,1]);
        h(k)=randi([0,1]);

                if (g(k)==0&&h(k)==0)
                    Out(:,k) = (alpha2+beta1)*P(:,k);
                    alice_basis_phase(k) = 1;
                    bob_basis_phase(k) = 0;
                    result(k) = 9;
                elseif (g(k)==0&&h(k)==1),
                    Out(:,k) = (alpha2+beta2)*P(:,k);
                    alice_basis_phase(k) = 1;
                    bob_basis_phase(k) = 1;
                    result(k) = 1;
                elseif (g(k)==1&&h(k)==0),
                    Out(:,k) = (alpha2+beta3)*P(:,k);
                    alice_basis_phase(k) = 1;
                    bob_basis_phase(k) = 0;
                    result(k) = 9;
                elseif (g(k)==1&&h(k)==1),
                    Out(:,k) = (alpha2+beta4)*P(:,k);
                    alice_basis_phase(k) = 1;
                    bob_basis_phase(k) = 1;
                    result(k) = 0;
                end

elseif (e(k)==1&&f(k)==0),

        g(k)=randi([0,1]);
        h(k)=randi([0,1]);

                if (g(k)==0&&h(k)==0)
                    Out(:,k) = (alpha3+beta1)*P(:,k);
                    alice_basis_phase(k) = 0;
                    bob_basis_phase(k) = 0;
                    result(k) = 0;
                elseif (g(k)==0&&h(k)==1),
                    Out(:,k) = (alpha3+beta2)*P(:,k);
                    alice_basis_phase(k) = 0;
                    bob_basis_phase(k) = 1;
                    result(k) = 9;
                elseif (g(k)==1&&h(k)==0),
                    Out(:,k) = (alpha3+beta3)*P(:,k);
```

```
                                        alice_basis_phase(k) = 0;
                                        bob_basis_phase(k) = 0;
                                        result(k) = 1;
                                    elseif (g(k)==1&&h(k)==1),
                                        Out(:,k) = (alpha3+beta4)*P(:,k);
                                        alice_basis_phase(k) = 0;
                                        bob_basis_phase(k) = 1;
                                        result(k) = 9;
                                    end


            elseif (e(k)==1&&f(k)==1),

                    g(k)=randi([0,1]);
                    h(k)=randi([0,1]);

                                    if (g(k)==0&&h(k)==0)
                                        Out(:,k) = (alpha4+beta1)*P(:,k);
                                        alice_basis_phase(k) = 1;
                                        bob_basis_phase(k) = 0;
                                        result(k) = 9;
                                    elseif (g(k)==0&&h(k)==1),
                                        Out(:,k) = (alpha4+beta2)*P(:,k);
                                        alice_basis_phase(k) = 1;
                                        bob_basis_phase(k) = 1;
                                        result(k) = 0;
                                    elseif (g(k)==1&&h(k)==0),
                                        Out(:,k) = (alpha4+beta3)*P(:,k);
                                        alice_basis_phase(k) = 1;
                                        bob_basis_phase(k) = 0;
                                        result(k) = 9;
                                    elseif (g(k)==1&&h(k)==1),
                                        Out(:,k) = (alpha4+beta4)*P(:,k);
                                        alice_basis_phase(k) = 1;
                                        bob_basis_phase(k) = 1;
                                        result(k) = 1;
                                    end

                    end
end

% --------- Phase Basis Comparision -------------------------------
```

```
compare(k)=xor(alice_basis_phase(k),bob_basis_phase(k));

                                        if(compare(k)==0)
                                              basis_phase_info(k)= 1;
                                        else
                                              basis_phase_info(k)= 0;
                                        end

                                        if(basis_phase_info(k)== 1)
                                           shifted_key_phase(k)=result(k);
                                        else
                                           shifted_key_phase(k)= 5;
                                        end
                                        ind_ph(k) = (shifted_key_phase(k)==5);

end

%--------Polarization Encoding Calculation & Output-----

shifted_key_pol(ind_pol) = [] ;
M_pol= length(shifted_key_pol);
QBER_pol = (N-M_pol)/N;

disp(['Alice Basis: ', num2str(alice_basis)]);
disp(['Bob Basis: ', num2str(bob_basis)]);
disp(['Bob Result: ', num2str(bob_result)]);
disp(['Basis Compared Result: ', num2str(basis_pol_info)]);
disp(['Shifted Key: ', num2str(shifted_key_pol)]);
disp(['Polarization Shifted Key Length: ', num2str(M_pol)]);
disp(['QBER: ', num2str(QBER_pol)]);

%--------Phase Encoding Calculation & Output -----

shifted_key_phase(ind_ph) = [] ;
M_ph= length(shifted_key_phase);
QBER_ph = (N-M_ph)/N;

disp(['Alice Basis: ', num2str(alice_basis_phase)]);
disp(['bob Basis: ', num2str(bob_basis_phase)]);
disp(['Result: ', num2str(result)]);
disp(['Basis Compared Result: ', num2str(basis_phase_info)]);
disp(['Shifted Key: ', num2str(shifted_key_phase)]);
disp(['Phase Shifted Key Length: ', num2str(M_ph)]);
disp(['QBER: ', num2str(QBER_ph)]);
```