Quantum Key Distribution

Rayan Hussien Alsedig Madany (rayan@aims.ac.za)
African Institute for Mathematical Sciences (AIMS)

Supervised by: Prof. Jeff Sanders
AIMS South Africa, South Africa

14 May 2020

Submitted in partial fulfillment of a structured masters degree at AIMS South Africa

Abstract

Quantum key distribution is a new and secure method of communication in cryptography to create an identical keys between two or more parties to exploit the concepts of quantum mechanics. Quantum mechanics make the parties able to distinguish any interception from Eve due to the disruption in the qubit due to the measurement on different and similar bases. In this paper we shall present the theoretical description of BB84 by using polarization of photons and spin of the electrons to create identical keys between parties and the practical implementation of BB84 protocol to store and read the quantum state or qubit.

Declaration

I, the undersigned, hereby declare that the work contained in this research project is my original work, and that any work done by others or by myself previously has been acknowledged and referenced accordingly.

Rayan Hussien Alsedig Madany, 14 May 2020

Contents

1. Introduction

Before The internet people shared keys to encrypt secrets. But then Diffie and Helman proposed public-key cryptography for the internet and RSA implemented their proposal. But then Shor's quantum algorithm made RSA insecure because it becomes easy to find the factors of a large prime number in a short time and so the alternative had to be found to public-key cryptography. BB84 showed that How the keys can be disturbed securely so that the old pre-internet idea of shared key still works for the internet under quantum conditions.

In chapter 3 we will discuss Blum's coin tossing over the phone to know who is the winner by using an encryption or hash function satisfies the proposal of the protocol and how Alice can cheat by using the conjugate of the function to convince Bob she does not cheat. BB84 is protocol proposed by Bennett and Brassard in 1984 (Bennett et al., 1992), In chapter 4 we will demonstrate the theoretical implementation of BB84 by using polarization of photons and spin of electrons, whereas the photons of light polarized in four orthogonal states and the spin of the electron have two directions, spin up and spin down, and will discuss how to creates the identical keys by measuring the polarization of photon or spin of an electron by their specific bases, the interception of Eve is will be detectable if she measures in wrong bases, Alice and Bob use error correction and privacy amplification to reduce the errors in Bob bits and Eve's information, in. In 4.5 we show how Alice can cheat in order to create non-identical keys. In 4.7 we will discuss a modified version of the BB84 protocol proposed by Bennett is called B92 protocol (Mehic et al., 2015).

In chapter 5 we will discuss the implementation of BB84 (Mehic et al., 2015) by using polarization photons and phase encoding which each implementation needs Mach-Zehnder interferometer (Hughes et al., 2000) and quantum channel either fiber optic or free space to transmit the signal from Alice to Bob, and the implementation of polarization and phase encoding have a disadvantage due to the difficulty to produce pulse contains one photon where Eve can intercept the transmission and divide the pulse into to and gain information about the key. In 5.7 we will learn how to used the single photon source quantum dot to produce single photon use in the implementation of BB84 instead of use pulse to make the implementation secure.

2. Background

2.1 Quantum Key Distribution

Quantum key distribution is a secret method of communication (Bennett et al., 1992) between two or more parties in order to establish a secret identical keys between them without having any initial information between them. The two parties create an identical keys to encrypt and decrypt their information and protect it from eavesdropping. Quantum key distribution in order to protect the information, it uses quantum mechanics concepts which makes parties able to detect any attempts of interception from the third party. Quantum mechanics is the theory builds on probabilistic, to determine the exact information it should measure the quantum state of the system, according to the quantum any measurement will change the original state, the two parties able to detect any change in the system does not happen from them. The transmission between two parties complete by using channels:

- The classical channel which it easy for eavesdropper to listen to the two parties nevertheless any information from classical channel does not give Eve any information without knowing the quantum state.
- Quantum channel used to transmit the quantum state from sender to reviver, an example for the quantum channel is fibre optics.

The physical phenomena that quantum key distribution exploits to create secure communication are entanglement, the polarization of photon, spin of the electron and other phenomena.

2.2 Entanglement

Entanglement is physical concept describes the association between two or more particles created from the same state of energy, the measurement of the physical properties are associate with each other, the entangled particles do not describe individually. Tensor products used to describe the entangled particles. For instance, take the physical property spin of an electron, the two entangled electrons created from the same level of energy, according to the superposition of quantum mechanics the two electrons have four probabilities for the actual state, after measurement the four states reduce to one sate with probability one, we denoted to the state of two electrons by $\mid \psi\rangle$ and the spin up of electron $\uparrow$ and spin down $\downarrow$.

$$\mid \psi\rangle = \frac{1}{\sqrt{4}} \left(|\uparrow\uparrow\rangle + |\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle + |\downarrow\downarrow\rangle\right)$$

2.2.1 EPR Pair.

An EPR pair is the special case of entanglement concept proposed by **Albert Einstein**,**Boris Podolsky** and **Nathan Rosen** (Griffiths, 2005), the two entangled particles have opposite information about the state, for instance, if pair of electrons are entangled, one of them will be spin up and the other will be spin down (Griffiths, 2005), if we make measurement for one particle we can know simultaneously the outcome of other particle without measurement, the concept of EPR makes quantum mechanics incomplete due to discrepancy between entangled an EPR pair and quantum mechanics :

- Quantum mechanics states that we are not able to acquire any information about particles without measurement.
- An EPR pair states if we make a measurement for one entangled particles in a specific axis we can get information about the other particle in the same axis without measurement.

The EPR pair maintain entangled even we separate them for long-distance. The EPR pair are anti-correlated to each other, it impossible to measure EPR pair of electrons and foind both of them spin up or both of them spin down in the same axis.

2.3 No-Clone

The traditional definition of a clone is to create an identical version from an object, whereas there is no difference between the original and clone object. In quantum mechanics any attempt to duplicate the quantum state will make a disturbance in the state (Bhandari, 2014), this concept called a no-clone. In the cases that requited a copy from state of quantum mechanics, instead of take copy, quantum mechanics used entanglement phenomena. In quantum key distribution, non-clone theorem forbid Eve from making any copy from the quantum state.

2.4 Beam Splitter

Beam splitter is an equipment has optical properties, beam splitter made off mirror one of its side cover with dielectric material. When the incident beam strikes the beam splitter will divide into two beams one reflected and the second transmitted (Perry et al., 2019). The beam reflected due to the dielectric material does not allow for the beam of light to pass through its atoms according to this reason the beam of light reflects, the transmitted beam does not meet with the dielectric material into its way. The reflected beam reflects with phase shift $\varphi = \pi$ and transmitted beam transmit with phase shift $\varphi = 0$.

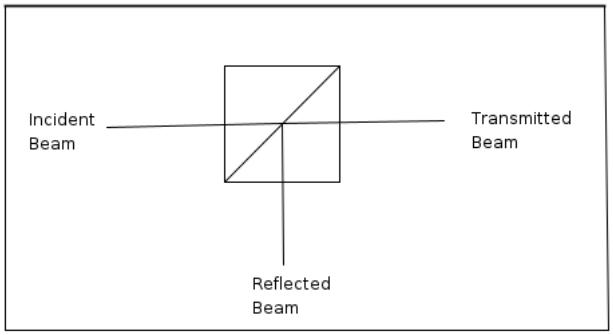

Figure 2.1: The beam of light split into two by using the beam splitter

2.5 Mach-Zehnder Interferometer

The waves have some properties like interference and diffraction, light classified as the wave has these properties. Interference of light is physical phenomena occur when two beams of light combine with each other to create either instructive interference or distinctive interference (Perry et al., 2019). Mach-Zehnder interferometer is a device proposed by two scientists **Luding Mach** and **Luding Zehnder** to measure the phase difference between two beams of light when they interface with each other. The laser source emitted beam of light divides into two beams when it strikes the half-silvered beam splitter BS_1 (see Figure 2.2 below), BS_1 reflects one beam with phase shift $\phi = \pi$ and transmits the second beam with the phase shift $\phi = 0$. The reflected and transmitted beams go to two mirrors M_1 and M_2 which reflects both of them into beam splitter BS_2, BS_2 recombines the two reflected beams into one beam. If the two beams have the same phase shift, the interference will be constructive as result the

phase difference between two beams is $\triangle\varphi = 0$ and BS_2 transmits the beam to the detector D_1, and if the phase shift of the two beams are different, the interference of two beams will be distributive with face difference $\triangle\varphi = \pi$, BS_2 reflects the beam to detector D_2 (Inoue, 2006).

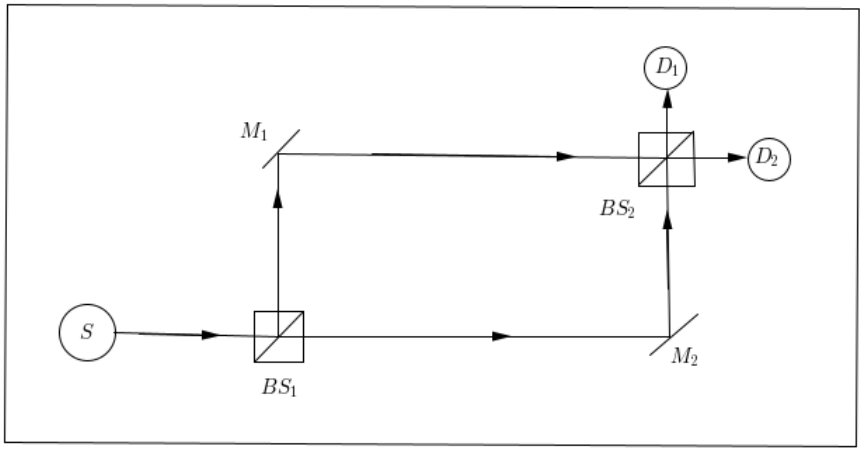

Figure 2.2: Mach-Zehnder interferometer components

2.6 Stern-Gerlach Experiment

The movement of charged electron in a circular motion around the nucleus of atom creates a magnetic moment μ in the atom. The magnetic moment is the vector orientation of the electron in an atom. A hot beam of silver atoms directed to pass through a collimator in order to make the beam parallel, the parallel beam goes between two poles of magnetic field different in shape and size to create inhomogeneous magnetic field oriented is $\hat{z}$ (Zhu and Singh, 2011), sliver atoms have different magnetic moment orientations in $\hat{x}, \hat{y}, \hat{z}$ when these atoms pass through the inhomogeneous magnetic field, the atoms that have a magnetic field orientated in the directions $\hat{x}, \hat{y}$ they will change their orientations to be in the direction of the magnetic field $B\hat{z}$. The interaction between magnetic moment μ and magnetic field B crates potential energy $U = -\mu_z B$, the presence of potential creates magnetic force.

$$F = -\frac{\partial U}{\partial z} = \mu_z \frac{\partial B}{\partial z}$$

The value of magnetic moment orientation has a maximum value of μ_z and minimum value $-\mu_z$. In the front of two poles there is screen works as detector. The gradient of the magnetic field is negative, when the magnetic interact with the atoms that have a positive magnetic moment, these atoms will be detected down in the screen, if the negative magnetic interact with the atoms that has a negative magnetic moment, these atoms will be detected up in the screen. The deflection of atoms down and up in the screen due to the effect of the magnetic field is known as the **spin of electron**.

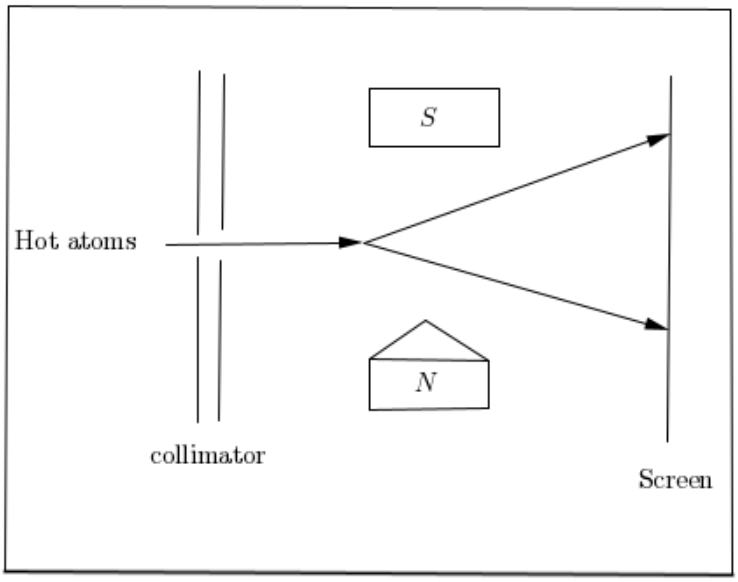

Figure 2.3: The design of Stern-Gerlach experiment

2.6.1 Measurement Of Spin Electron.

- When the atoms pass through the magnetic field either in the direction $\hat{z}$ or $\hat{x}$, the outcome is two beams in the direction of the magnetic field, the beam in the top of the detector(screen) read as spin up $e\uparrow$ of atoms and the second beam in the bottom of detector read as spin down $e\downarrow$
- When the beam of atoms pass through stern equipment which denoted by $SG\hat{x}$ its magnetic field aligned in the $\hat{x}$ direction with traps the beam of atoms has spin down and lets the beam of atom that has spin down up pass through another stern equipment its magnetic field in the $\hat{z}$, the outcome will be two beams one has spin up $e\uparrow$ and other has spin down $e\downarrow$, if the same beam passes through another stern equipment in $\hat{x}$ direction with traps the beam that has spin down the outcome will be two beams one has spin up and the other has spin down.

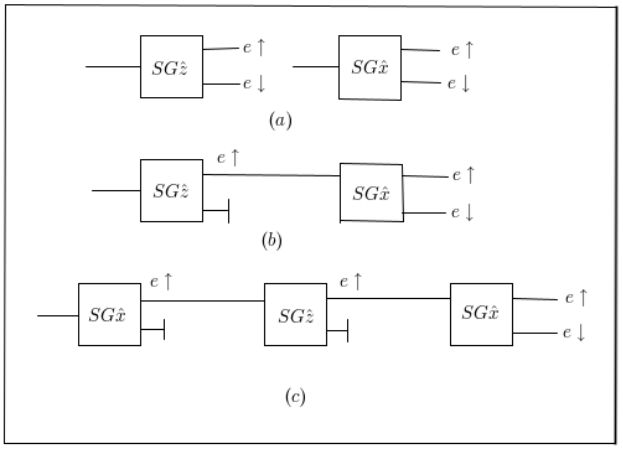

Figure 2.4: The figure (a) shows the stern device in the direction $\hat{z}$ and $\hat{x}$, figure (b) shows the two successive stern device with block the bottom beam, figure (c) shows the three successive stern device

3. Coin Tossing Protocol

Coin toss protocol is method of communication between two parties they do not trust in each other by distributing a uniform random bit (Blt, 1981).

3.1 Motivation

Alice and Bob are divorced, they live in different cities the only way to communicate between them is just by phone, they want to get a house, the dispute between them continue for a long time, in order to solve the problem one of them come with an idea to toss a coin, the winner of the game will get the house and the other person should accept. Alice throws the coin, then she asks Bob about his guess, if he guesses correctly he will win otherwise he will lose. But the problem that concerns Bob if Alice cheats and there is no third party to confirm who is the winner and loser. In **1983** Manuel Blum introduced a coin toss protocol, the protocol achieves to the two parties to use a secure function to encrypt and transmit information between them and how to communicate in order to get their goal and protect their information from eavesdropper, but the function that they used unknown from one party(receiver), also guarantee for both parties 50 percent chance for winning and losing.

3.1.1 Specification of Blum's protocol Achieves:.

- Makes Bob guarantees That Alice will choose her sequence of bit randomly, Alice bits is 1 if the coin is heads and 0 if the coin is tails (Blt, 1981).
- Makes Alice guarantees that Bob will not know what the sequence of bits she flipped (Blt, 1981).
- The function that Alice used to encrypt the classical bit **a**, it is should not give any information about **a** (Todd et al.).

3.1.2 The Properties Of Blum's Protocol Is :.

- Any attempt from one of the parties to bias the outcome in order to cheat, it will be detected by other parity, then the outcome should be rejected.
- If one of the parties is cheated and other parties do not figure out his attempt, the chance to win coin toss is 50 percentage will still the same.
- Alice knows which coins are heads which coins are tails.
- Bob does not know which coins are heads and which ones are tails.
- After implementing the steps of coin tossing protocol, Alice should confirm to Bob which coins are heads and which coins are tails (Blt, 1981).

3.2 How Blum's Protocol Work?

- Alice flips the coin, then choose **a** $\in \{0, 1\}$, where 1 represent a head and 0 represents tail of coin, she encrypts **a** with the function F, then Alice sends $F(a)$ to Bob via public channel(phone)(Todd et al.).

$Alice1$

$a : \mathbb{B}$
$b : \mathbb{B}_{\perp}$
$w_b : \mathbb{B}_{\perp}$
$F(a)!$: Alice $\rightarrow$ Bob

$w_b = (a = b)$
$b = \perp$

The first four lines represent the variables of the coin tossing system, whereas **a** is a binary number that Alice chooses, **b** is binary number represents Bob's guess, Alice does not know **b** yet and w_b is the boolean operation to figure out if Bob wins or not by comparing **a** and **b**, Alice does not know yet who is the winner because she does not know **b**, the parties know w_b by knowing both **a** with **b** . The function F applied on the binary number **a** and send to Bob, the symbol ! means $f(a)$ is output of the system . The process below the line of the schema is the boolean operation if Alice know **b** she can knows w_b.

- Bob receives from Alice $F(a)$ and he guesses the coin $b \in \{0, 1\}$, Bob sends his guesses to Alice by public channel, Bob is not able to figure out who is a winner because he does not know a, he just knows $F(a)$.

$Bob2$

$F(a)?$: Alice $\rightarrow$ Bob
$b : \mathbb{B}$
$w_b : \mathbb{B}_{\perp}$
$b!$: Bob $\rightarrow$ Alice

$w_b = (a = b)$
$a = \perp$

$F(a)?$, $b!$ are the input and output variable of the system respectively , Bob does not know **a** due to this reason he can not know w_b.

- Alice receives b, the she will work out to know who is the winner by comparing a with b, if $a = b$ it means Bob's guess is correct then Bob wins, if $a \neq b$ it means Bob's guess is wrong, then Alice wins, Alice in order to confirm her result she sends **a** and F to Bob.

$Alice3$

$b?$: Bob $\rightarrow$ Alice
$F!$: Alice $\rightarrow$ Bob
$a!$: Alice $\rightarrow$ Bob

$w_b = (a = b?)$

Alice receives Bob's guess as input b and compare if a and b are equal by using boolean operation w_b to know who is winner.

- Bob receives F and a, then he checks w_b if he wins or not and the boolean operation ok is to check if the two encrypted functions are equal.

*Bob*4

$F?$: Alice $\rightarrow$ Bob
$a?$: Alice $\rightarrow$ Bob

$w_b = (a = b?)$
$ok = (F(a) = F(a))$

Alice after figure out Bob who is winner, she could cheat to wins the coin instead of Bob.

3.2.1 Alice Cheating.

Alice in order to cheat, she sends to Bob the opposite of a which denoted by $\neg a$ with the function F^* which satisfy $F(a) = F^*(\neg a)$, Bob will be convinced that Alice is the winner.

*Alice*3

$b?$: Bob $\rightarrow$ Alice
$F^*!$: Alice $\rightarrow$ Bob
$\neg a!$: Alice $\rightarrow$ Bob

$w_b = (a = b?)$

*Bob*4

$F^*?$: Alice $\rightarrow$ Bob
$\neg a?$: Alice $\rightarrow$ Bob

$w_b = (a = b?)$
$\neg ok := (F(a) = F^*(\neg a))$

the boolean operation $\neg ok$, if it true means Alice cheated, then Alice wins, if it false means Alice does not cheat and Bob wins.

3.3 Iteration of Blum's Coin Toss Protocol N times

Blum's protocol guarantee, if one of two parties do not honest and the other party does not catch him, he still gets the same uniform coin toss outcome. In a single coin toss the probability to get head or tail is equal one-half for both of them. The question arises here what happens if the protocol extends to N-coin toss?. when Alice throws the coin N times the outcome of the flipping coin is 2^N, the probability to get head or tail N times is $(\frac{1}{2})^N = 2^{-N}$. If Alice bias the outcome to cheat, Bob needs probability grater than 2^{-N} to win.

4. BB84 Protocol

From the previous chapter of Blum's coin tossing protocol, we know that how Alice convinces Bob about her choice a by encrypting a with a certain function F, if Alice and Bob repeat the coin tossing operation, we found that Alice has a list equal to bits a with length equal the number of times that the coin was flipped, then Bob guesses $b \in \{0, 1\}$, then after Alice tells him the function, Bob will make sure which bits match with his choice. The method of repetition coin tossing was modified to became an essential method in quantum key distribution known as the BB84 protocol. BB84 is a type of quantum key distribution protocol proposed by **Charles Bennett** and **Gilles Brassard** in 1984 (Bennett et al., 1992). In BB84 protocol there are two parties Alice(sender) and Bob(receiver) exchange information between them to create their own identical keys to encrypt and decrypt the transmitted information and protect their information from eavesdropping. As any quantum key distribution protocols, BB84 uses quantum mechanical phenomena to transmit the information between parties. The common phenomena that have been used is polarization of photon and spin of electron.

4.0.1 The Postulates of BB84 protocol.

- The two parties communicate via two channels, the first channel is a quantum channel that carries the qubit from receiver to sender, the second is a classical channel(phone,internet).

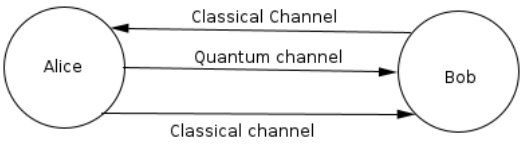

Figure 4.1: The communication between Alice and Bob via two channel

- The two parties agree about the bases that they will use in communication.
- Any attempt to cheat from any party will make them create a non-identical keys.
- If All parties are honest and there is no interception from Eve, the identical keys are secure.
- The identical keys are used once to transmit information, then after using them, the two parties will discard the keys.
- The interception by Eve is detectable by the disruption in the qubit state.

4.1 BB84 By using polarization Of Photons States

BB84 as a quantum key distribution gains advantages from the polarization of photons to transmit information, the qubit of communication that two parties use is photon state. Photon light polarized in four directions each two directions are perpendicular to each other, these four directions classified into two bases:

- Rectilinear basis with the directions of polarization in $0°$ horizontal and $90°$ vertical to x-axis.
- Diagonal basis with the directions of polarization in $45°$ and $135°$ to x-axis.

The parties identify the two bases with two bits 0 and 1 (see Figure 4.2 below). If Alice and Bob measure the state of a photon on the same bases (Kohnle and Rizzoli, 2017), the receiver will get the correct bit otherwise will consider it as error due to noise in a quantum channel or eavesdropping interception. If Alice and Bob use different bases, the probability that the receiver gets the correct bit is one-half.

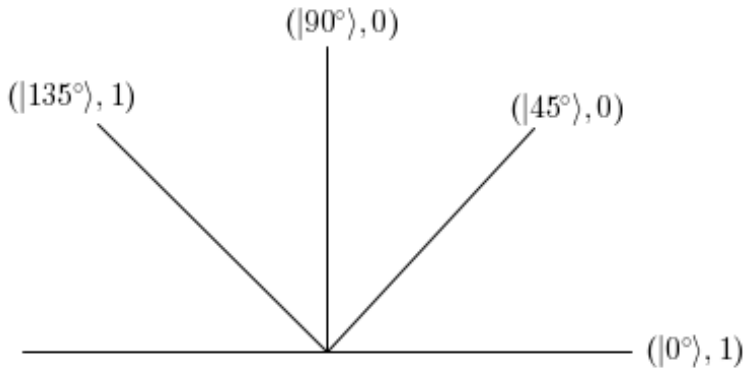

Figure 4.2: The directions of photon light polarizations with associated classical bits

4.1.1 The Theoretical Implementation Of BB84 Protocol .

- Alice creates a list of bits $a \in \{0, 1\}$ with a certain length, then she chooses a list of bases polarization with the same length to the bits list, in order to expresses the classical bits(one photon express one bit), She does this operation individually, She records the bases that She used in a list. The next step Alice sends the polarized photons to Bob via the quantum channel Bennett et al. (1992).
- Bob receives the incoming photons and extracts the information about the classical bits by measuring photons, to measure the photons Bob chooses randomly one of two bases either rectilinear(R) or diagonal(D), then he records the bases that he used in his list. Bob communicates with Alice via a classical channel to tell her about his bases.
- Alice reveals her bases of measurement to Bob via the same quantum channel.
- Alice and Bob have mutual information about their bases, The parties simultaneously keep in their lists the bits with a similar bases and cancel the bits with a different bases.

Table (4.1) shows the process of creating a key in the BB84 protocol.

Alic's bits	1	0	1	1	0	0	1	0
Alice' bases	D	D	R	D	R	R	D	D
angle of bases	$135°$	$45°$	$0°$	$135°$	$90°$	$90°$	$135°$	$45°$
Bob's bases	R	D	R	R	R	D	R	D
angle of bases	$0°$	$45°$	$0°$	$90°$	$90°$	$135°$	$0°$	$45°$
Bob's bits	1	0	1	0	0	1	1	0
key		0	1		0		0	

Table 4.1: The process of creating identical key BB84 protocol

In the absence of Eve the discrepancy between Alice and Bob due to using different bases is solved by discarding the bits on a different bases. The two parties are able to detect Eve according to postulates of quantum mechanics,, any measurement will make disruption on the states. If Eve intercepts transmission of the quantum state, she is not able to take a copy of the quantum state due to no-cloning theorem, attempting to clone will disrupt the quantum state and will be detectable by parties, Eve can gains knowledge about the keys by trying to guess correctly the bases.

4.2 Error Correction Process

After revealing the bases publicly, the two parties agree to cancel the bits from their lists that they have been used different bases for measurement, to reduce the probability of errors in Bob's bits due to the introduction of a non-identical keys. The errors in Bob's bits occurrence for two reasons:

- The interception by an eavesdropper selecting the wrong bases of measurement.
- The errors because of noise in the quantum channel.

The two parties are not able to recognize the real reasons for the errors in Bob's bits, So they must consider all the errors that occurs due to eavesdropper interception. The two parties have two lists of length n, nevertheless, they do not guarantee if they have the same bits, In order to get the same bits, the two parties agree to divide their lists into x sets of length y. They choose randomly bits from each set x and compare it publicly, then discard the last bit in each set x (Goneid et al., 2009), in this case they obtain a new keys with length $z = x(y-1)$. If the percentage of error is small, they will consider the key, if the percentage of error is too hight they agree to discard the keys and start from the beginning to establish a new keys with the same postulates until they get the desired and perfect keys with low errors.

4.2.1 The Methods That Eve Use To Gain Information About The Key .

- When Eve uses the same bases as Alice does, Eve's knowledge in this case depends on Bob's choice, whereas if Bob chooses the correct bases, then the parties will keep the bits on a similar bases (Bhandari, 2014). All the three parties will have the same bits.
- When Eve succeeds to guess the classical bit when she used the wrong basis while two parties use an identical bases.
- During the error correction process, the two parties choose the part of their list and announce publicly to check weather Eve gained information about the keys.

4.3 Privacy Amplification

Privacy amplification is a secure method used to reduce the eavesdropper's knowledge about the keys bits (Bhandari, 2014). In the error correction process, Eve acquires knowledge about the key due to the announcement of some bits publicly. Privacy amplification uses different functions to reduce Eve's information nevertheless the outcome of applying the function F to the keys, will reduce the length of the key strings For this reason Alice should choose a long string of bits to create the shift keys. Whenever they apply more operations on the keys, the keys become more securer, an example of the function is a class of universal hash function. After the error correction process the length of the key list become Z. By assuming Eve knows J bits about the key, the next step is to apply the hash function to key, The outcome will a secure key with length $Z - J - S$, S is parametric security (Abbas et al., 2014).

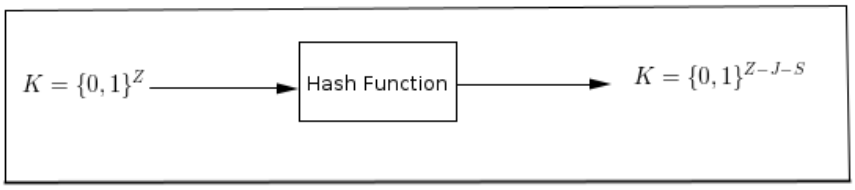

Figure 4.3: Mapping hash function to the key

4.3.1 Privacy Amplification By Applying XOR Operator .

The XOR operator is a logical process, when XOR applied on the two binary number 0 and 1, the outcome of the process given as. $a \oplus b = 0$ if $a = b$ otherwise $a \oplus b = 1$ where $a, b \in \{0, 1\}$

Alice and Bob agree to divide their shifted keys into sets that have a certain and equal length, the smallest division has length two. Then they will apply the XOR operation on the sets (Skander et al., 2008), the outcome of operation will be appended to the new lists as a new bit. The XOR operation reduces Eve's information because applying this process requires knowing all the bits that includes the XOR process. If Eve knows only one bit from the set she is not able to get the outcome of XOR with probability one. Eve's knowledge about the keys will build on probabilities and guessing. Alice and Bob communicate publicly to know how many times they will apply the XOR operation.

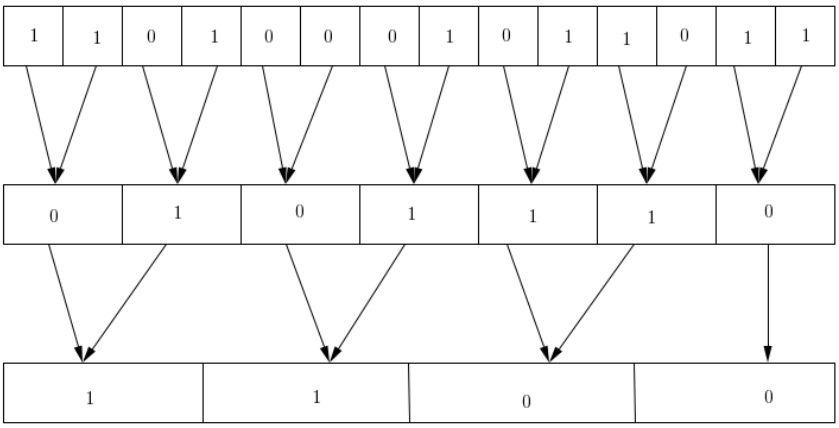

Figure 4.4: XOR operation applied on the sifted key

4.4 BB84 Protocol By Spin of electron

Quantum key distribution gains an advantage from the spin of the electron to transmit information between two parties. In the Stern-Gerlach experiment, the electron of atom deflect when it passes through the magnetic field, This deflection called the spin of the electron, The deflection in the positive direction and negative direction of the magnetic field is spin up and spin down respectively.

4.4.1 The Bases of Spin of Electron .

Alice and Bob use Stern-Gerlach device in two different directions as a bases, For instance, Stern-Gerlach device with magnetic field in the directions $(\hat{Z},\hat{X})$,$(\hat{Z},\hat{Y})$ and $(\hat{X},\hat{Y})$, in this scheme, we will use $(\hat{Z},\hat{X})$ basis (Perry et al., 2019). Alice and Bob read the classical bits from the spin of electrons in the two directions as shown (4.2) table.

Direction of magnetic field	Spin Alignment	Classical bit	The Basis
$+\hat{Z}$	$\uparrow$	0	Z
$-\hat{Z}$	$\downarrow$	1	Z
$+\hat{X}$	$\longleftarrow$	0	X
$-\hat{X}$	$\longrightarrow$	1	X

Table 4.2: The direction of spin of the electron and associated classical bit

Alice measures her electrons in one of two bases either Z or X, Bob receives the incoming electron then he chooses randomly one of the two bases.

Alice's bits	0	1	0	0	1	1	1
Alice's basis	Z	X	X	Z	Z	X	Z
Alice's state spin	$\uparrow$	$\rightarrow$	$\leftarrow$	$\uparrow$	$\downarrow$	$\rightarrow$	$\downarrow$
Bob's basis	Z	X	Z	Z	X	X	Z
Bob's state spin	$\leftarrow$	$\rightarrow$	$\downarrow$	$\uparrow$	$\leftarrow$	$\leftarrow$	$\downarrow$
Bob's bits	0	1	1	0	0	0	1
probability	1/2	1	1/2	1	1/2	1	1
key		1		0		1	1

Table 4.3: The process of BB84 protocol by using Z and X basis

4.5 Cheating By Using EPR pair

The main goal for BB84 is to create an identical keys, being identical means Alice guarantees Bob will receive the correct information and protect the information from Eve. In some cases Alice does not want to share her information with Bob nevertheless she is forced to share her information, She would like to send the wrong information which is impossible with identical keys. Alice in order to share wrong information with Bob, may could cheat to create a non-identical keys with Bob. Alice uses an EPR pair of photons or electron to cheat according to the way of implementation, assuming Alice and Bob choose the photon qubit to communicate between them. Alice creates an EPR pair of photons instead of a single photon. The special property of an EPR pair of photons is they have the opposite direction of polarization if measured on the same basis. Suppose the angle of polarization of the first photon is α and the angle for the second is β. an EPR pair of photons when they created from the source initially their direction of polarization in the four directions in the four possible directions, whereas α

and $\beta \in \{0°, 45°, 90°, 135°\}$, The extra information if one of the photon pair has polarization in the direction of one of the orthogonal basis the second photon polarized in other direction of the same basis. The initial state of EPR pair $\mid X\rangle$ are in superposition of the two bases.

$$\mid X\rangle = \frac{1}{\sqrt{2}}(\mid 0°, 90\rangle + \mid 45°, 135\rangle)$$

Alice separates an EPR pair photons into single photons, nevertheless, the photons still have the same opposite polarization regardless of the distance between them. The state of the separated photons is :

$$\mid Y_1\rangle = \frac{1}{\sqrt{2}}(\mid 0°\rangle + \mid 45°\rangle)$$
$$\mid Y_2\rangle = \frac{1}{\sqrt{2}}(\mid 90°\rangle + \mid 135°\rangle)$$

Measuring the state $\mid Y_1\rangle$ gives a prediction to the state $\mid Y_2\rangle$ without measurement according to the EPR concept. Alice creates n an EPR pairs from the source and then separates each pair into single photons, In this case Alice has two sets:

- The first set $\mathbf{Z}_1$ represents the first photons from each pair with polarization angle $\alpha \in \{0°, 45°, 90°, 135°\}$
- The second set $\mathbf{Z}_2$ represents the second photons from each pair with polarization angle $\beta \in \{0°, 45°, 90°, 135°\}$

If the measurement of the first photons is with polarized angle $\alpha < 90$, then the second photons will be found to be polarized in direction $\beta = \alpha + 90°$ in the same basis, if the measurement of the first photons is with polarized angle $\alpha > 90$, then the second photons will be found to be polarized in direction $\beta = \alpha - 90°$ in the same basis. Alice measures the first set of photons, The classical bits of measurement has been added to list a and then sent to Bob, Bob records his measurement in list a' and record his basis he used in list $\mathbf{Z}'_1$.

4.6 The Strategies Alice Uses To Create Non-identical Key

- Alice by comparing her basis $\mathbf{Z}_1$ and Bob Basis $\mathbf{Z}'_1$ she knows Bob's but with consideration there are error in list a'.
- Alice measures the second set of photons $\mathbf{Z}_2$ by choosing basis opposite to Bob's basis and record the basis in a list $\mathbf{Z}'_2$ and record the classical bit in a list a_1.
- Alice reveals basis $\mathbf{Z}_1$ to bob, after reconciliation process the two lists reduce to $v_1 = a - t$ and $v_2 = a' - t$, where t is the bits that have been measured in a different basis.
- Alice in the process of error correction and privacy amplification used the bit from the list v_1 to create a perfect key.
- But in transmission Alice used the key that crate from list a_1 as the same length of the identical key.
- The interception of Eve by using the wrong basis make an error in Bob's bit in the case of using single photons when the two parties use similar basis, but in the case of using An EPR pair the interception of Eve make correction in Bob's it with low probability

4.7 B92 protocol

Charles Bennett in 1992 proposed a new version of BB84 called B92 protocol, the two protocols are similar but quite different, while in BB84 parties used four orthogonal states of polarization, nevertheless in B92 protocol the parties used any of two non-orthogonal states of polarization to transmit the signal between them. The non-orthogonal is to choose one state $\alpha \in \{0°, 90°\}$ to encode the bit 0 and chose the other state $\beta \in \{45°, 135°\}$. The two non-orthogonal states satisfy the equation (4.7.1)

$$\cos^2(\alpha - \beta) = \frac{1}{2} \tag{4.7.1}$$

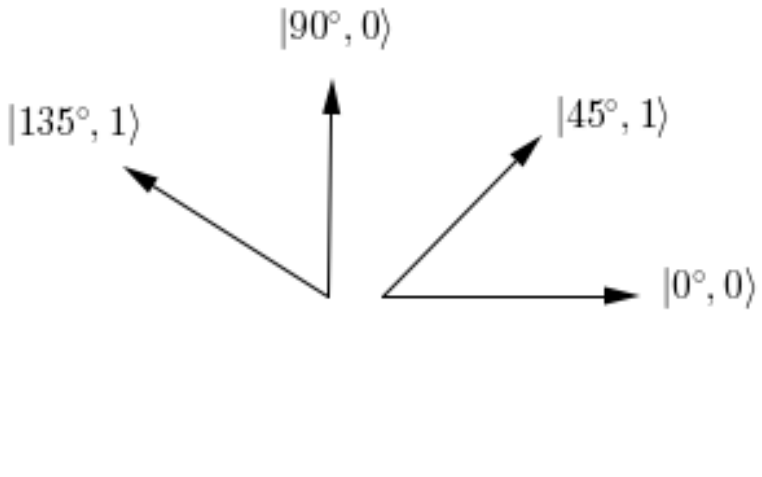

Figure 4.5: Examples for the bases that Alice used to encode her bit in B92 protocol

Alice generates a list of of bits $X_1 = \{\text{length of n}\}$ (Mehic et al., 2015) and choose her bases (α, β), Alice After measure her bits, She send the polarized states to Bob. Bob Measures the incoming photons by choosing the second non-orthogonal basis, for instance, if Alice chooses the basis $(0°, 45°)$ Bob will choose the basis $(90°, 135°)$ (Yang et al., 2002), if Bob measures the photon in different bases, he will get the correct bit, then he will record his measurement in his list as Yes, if he measures in the same bases he will get nothing, then he will record his measurement in the list as No (Yang et al., 2002). Bob sends to Alice by classical channel the positions of the bits that he measured with different bases without revealing the bases of measurement. After discarding the bits with similar bases Alice and Bob apply the process of error correction and privacy amplification to reduce the errors in Bob's Bits and reduce Eve's information about the keys.

Alice's bits	1	1	0	0	1	0	1	0	0	0
Alice's basis	$45°$	$45°$	$0°$	$0°$	$45°$	$0°$	$45°$	$0°$	$0°$	$0°$
Bob's basis	$135°$	$90°$	$135°$	$90°$	$135°$	$135°$	$135°$	$90°$	$135°$	$135°$
bob's bits	0	1	0	1	0	0	0	1	0	0
Bob's measurement	No	Yes	No	No	No	Yes	No	No	Yes	No
key	-	1	-	-	-	0	-	-	0	-

Table 4.4: The process of B92 protocol by using two non-orthogonal bases

Alice and Bob used the qubit either polarised photons or spin of electrons to transmit their information, they need equipment to store the information in the qubit and practical channel, to take the signal from Alice's side to Bob's side, Bob needs equipment to read the signal that Alice sent.

5. The Practical Implementation Of BB84

From the theoretical description of the BB84 protocol, we know that Alice and Bob used the spin of electron and polarization of photons to transmit the classical bits. This chapter will show the practical methods that are used to prepare the qubit and how the two parties store and read the information from the qubit.

5.1 Polarization Encoding Implementation

In this implementation Alice owns four sources of laser (Ruiz Alba Gaya et al., 2011) polarized with $\alpha \in \{0°, 45°, 90°, 135°\}$. Alice, in each transmission, chose one of these sources to send to Bob. In this scheme instead of using four laser sources, Alice used one source of laser and change the polarization of laser by use phase modulator (PM). Alice used a mirror(M) and a beam splitter (BS_1) to increase the amplitude of the pulse, to reduce the number of photons in the pulse She used a set of filters (Fs) because has the ability to attenuate the pulse without changing the direction of polarization. Alice sends the laser beam to Bob by using fiber optic channel. Bob receives the incoming beam of light and passes it through wave plates (WP) to compensate and maintain the initial polarization of beam light that Alice sent. The pulse of photons strikes the beam splitter (BS_2) which divides the beam of light into two, one transmitted and the other reflected. Bob has two partial circuits, these circuits consist of polarized beam splitter polarized with a certain angle and two photon detectors. The partial circuits work as rectilinear and diagonal bases. The reflected beam goes through the half-wave plate and strikes polarized beam splitter (PBS_2) which is polarized by angle $\theta = 45°$ (Ruiz Alba Gaya et al., 2011). PBS_2 connected with two detectors of a photon. This partial circuit represents a rectilinear basis. The transmitted beam hits the polarized beam splitter (PBS_1), then the beam is measured by one of the two photon detectors. The two circuits measure at the same time. Nevertheless, Bob should choose one of the two bases to revealed after to Alice.

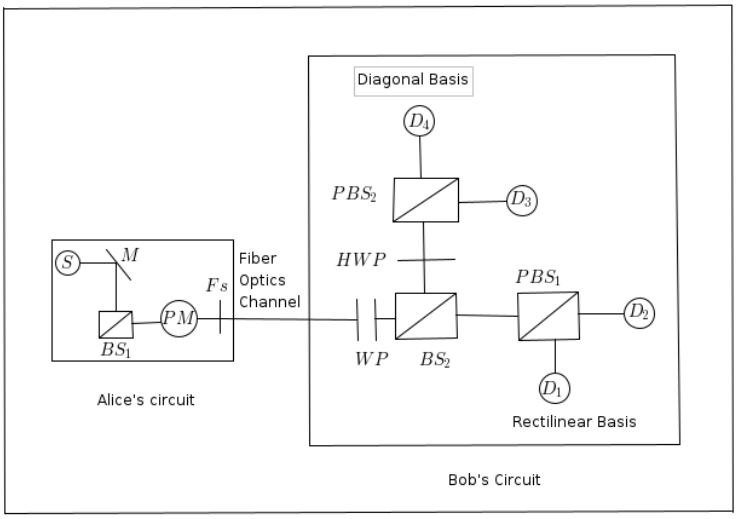

Figure 5.1: The practical implementation of BB84 protocol by using polarization encoding

5.2 Phase Encoding Implementation

Quantum key distribution takes advantage of Mach-Zehnder interferometer device to perform the implementation of BB84 by exploiting the phenomena of interference of light. The qubit in interferometer is the phase difference $\triangle\varphi$. To store and read qubit phase difference, Alice and Bob use two Mach-Zehnder interferometer devices connected by an optic fiber channel to transfer the beam of light from Alice's interferometer to Bob's interferometer as follows:

- In Alice's interferometer, the source of light (S) emits a beam of light. Alice governs the phase of a beam φ by using a phase modulator. The possible values of a phase that Alice use are $\{0°, 90°, 180°, 270°\}$ (Hughes et al., 2000)(Inoue, 2006), where the phase $\varphi_A = 0°$ or $90°$ represent classical bit 0, the phase $\varphi_A = 180°$ or $270°$ represent classical bit 1.
- Alice chooses the phase that represents her classical bit and sends it Bob by using fiber optic channel.
- Bob's interferometer receives the incoming beam, the beam splitter BS_3 divides the beam into two, one reflected to the mirror M_3. Then Bob changes the phase of the reflected beam by using a modulator. The possible values Bob can choose are $\{0°, 90°\}$. After changing the phase beam mirror M_4, the beam is reflected to the beam spitter BS_4 and the transmitted beam from BS_3 will go to the beam splitter BS_4 (Lo and Zhao, 2008).
- The reflected and transmitted beams will combine again in BS_4.
- When the beam is reflected the phase shift will be $\varphi = 180°$. In Bob's interferometer, the beam is reflected twice with the phase shift $\varphi = 360°$ which as the same as the original beam. The beam will have the value of a phase shift that Bob changed by using a modulator φ_B.
- The phase difference between the two beams is $\triangle\varphi = \varphi_A - \varphi_B$ (Hughes et al., 2000). If the two beams have the same phase the outcome will be constructive interference, otherwise it will be destructive interference
- In the implementation of bb84 by using photon polarization, the measurement is done by orthogonal bases, rectilinear and diagonal according to the assumptions made. If Bob uses the same bases as Alice does, he will have the correct classical bit. The same assumptions implemented in this scheme are used in phase encoding implementation basis as follows:
  - $(0°_A, 180°_A, 0°_B)$ basis.
  - $(90°_A, 270°_A, 90°_B)$ basis

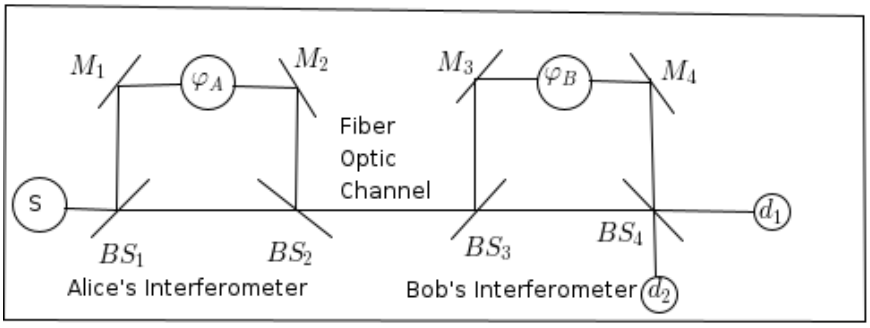

Figure 5.2: The implementation of BB84 protocol by using phase encoding

- When Alice and Bob use the same bases, the outcome of the interference will be:

Constrictive interference	Distinctive interference
$(0^\circ_A, 0^\circ_B)$	$(180^\circ_A, 0^\circ_B)$
$(90^\circ_A, 90^\circ_B)$	$(270^\circ_A, 90^\circ_B)$

Table 5.1: The constrictive and distinctive interference between two bases

The detector d_1 reads the constrictive interference and the detector d_2 reads the distinctive interference (Ruiz Alba Gaya et al., 2011). When Alice and Bob reveal their phase shifts, Bob can calculate the phase difference between them. The measurement on the same bases gives a deterministic outcome and the measurement on different bases builds one probability. That is it will be detect either detector d_1 or d_2. Bob after calculating the phase difference reads the classical bits as (see table5.2)

$\triangle\phi$	Classical bit
0	0
180°	1
90°	0 or 1
- 90°	0 or 1

Table 5.2: The qubit phase difference with associated classical bit

- The theoretical description between Alice and Bob to establish the key shift(see table5.3)

Alice'bits	1	0	0	1	0
Alice's phase	180°	0°	90°	270°	90°
Bob's phase	0°	90°	0°	90°	90°
phase different	180°	-90°	90°	180°	0°
Bob' bits	1	1	0	1	0
key shift	1			1	0

Table 5.3: The process of transmission between Alice and bob by using Mach-Zehnder interferometer device to create shift key

Another method to describe this implementation is by using another bases that satisfies the same assumptions as the previous bases. The bases are $(45^\circ_A, 225^\circ_A, 45^\circ_B)$ and $(135^\circ_A, 315^\circ_A, 135^\circ_B)$

Constrictive interference	Distinctive interference
$(45^\circ_A, 45^\circ_B)$	$(225^\circ_A, 45^\circ_B)$
$(135^\circ_A, 135^\circ_B)$	$(315^\circ_A, 135^\circ_B)$

Table 5.4: The constrictive and distinctive interference between two bases

5.2.1 Alice Cheating .

In both implementation Alice could cheat by producing EPR beams, She sends one beam to Bob and stores the other beam with her to manipulate the outcome in error correction and privacy amplification to

create non-identical keys. In the implementation of phase encoding, in the case of bases of measurement $(0°, 180°)$ and $(90°, 270°)$ Bob outcome to the phase difference will be shifted with $180°$.

$$\triangle\varphi = \varphi_A - \varphi_B + 180°$$

5.3 The Comparison Between Polarization and Phase Encoding

- Both implementations used the laser beam to transmit the information between two parties.
- In the two implementations Bob's circuit based on the concept of Mach-Zehnder interferometer.
- Polarization and phase encoding can use both of the fibre optic and free space channel but the two parties decide which of two channels are perfect for their implementation.
- In the polarization encoding and phase encoding the quantum state are the polarization of a photon and the phase difference between two beams of laser photons respectively.
- The secure transmission in both implementation required to produce a weak pulse.
- Both Implementations have specific bases, if the measurement with different bases, the receiver will get the correct bit with probability one-half, if the bases of measurement with similar basis the receive will get the correct bit.

5.4 Fibre Optics Channel

Fibre optics is an optical device that is made up of the pure glass to transmit the beam of light between two points. Fibre consists of three parts:

- Core: which represents the glass part.
- Cladding cover the core of fibre, whose functionality is to conserve light in the core.
- Buffer coating, is the plastic part surrounding the coating of the other parts which protect the fibre from damage.

  The index of refraction of the core is greater than the index of refraction of the cladding which is a condition that occurs with internal reflection. Fibre optic transmits the light by total internal reflection. The incident light, once it hits the core, is reflected from point to point until it reaches the end of fibre optic. Fibre optics is used in long distance but it is not perfect because of the phenomena known as birefringence.

5.4.1 Birefringence Fibre Optics.

Birefringence is optical phenomena occurs in the material that has an optical properties like refractive index, when the polarized beam of light fall on this materials, the beam will split into two beams, the direction of the two beams is quietly different from each other. Fiber as any optical material has birefringence, the phenomena of birefringence effect on the signal of pulse, make the transmission of information imperfect.

5.5 Eavesdropping Interception

Quantum key distribution uses the phenomenon of quantum mechanics to make the parties use a protocol to be able to detect Eve. Nevertheless, the smart eve searches for a way to intercept the process of

transmission without being detected by the parties. In the transition of BB84 by using polarization of photon, it is difficult to control the number of photons in a pulse. In some cases, the pulse contains more than one photon, in other cases the pulse does not contain a photon. The number of photons, x, in the pulse is given by the Poisson distribution (Gaidash et al., 2016).

$$P_x = \frac{e^{-\lambda}\,\lambda^x}{\lambda!}$$

Where λ is the average number of photons in the pulse and should be a positive number less than 1 (Goneid et al., 2009). If the pulse contains more than one photon, it makes the process of interception easier for Eve. Eve uses the beam splitter to divide the beam that Alice sent into two, she stores one in this quantum memory (Gaidash et al., 2016) to used at a later time after revealing the basis and the second one is redirected to Bob. Eve makes sure that the process of interception is not detected by checking the number of photons in the pulse by using quantum non-demolition measurement. This process counts the number of photons without changing the states of photons, this interception from eve is called **photon-number-splitting attack** .

5.6 Semiconductors

Semiconductors are materials that have both the properties of insulators and conductors. At room temperature, semiconductors behave as insulators and in high temperatures, they behave as conductors. To increase the conductivity of semiconductors there are impurities added to semiconductors and this process is called **Doping**. The semiconductor atoms are made up of a covalent band with each other to create a crystal structure. In the case of adding impurity to the crystal structure, the impurity makes covalent band with the semiconductor atoms:

- When the valence electrons of the impurity are greater than the valance electrons of the semiconductors, there will be free elections in the crystal structure and this type of semiconductors are called **n-type**.
- When the valence electrons of the impurity are less than the valance electrons of the semiconductors, there will be free holes of elections in the crystal structure and this type of semiconductors are called **p-type**.

The atoms have level of energies and each level has a specific number of electrons. The last filled level of energy by elections is called valance band, the lowest unfilled level of energy is called conduction band. Quantum dot is the smallest particle of semiconductors that has particular features. In a quantum dot when an electron in the valance band absorbs energy, it goes to the conduction band. When the electron comes back to its valance band it emits a single photon light. The light has a special colour that relies on the difference in energy between valance and conduction band. One of the quantum dot applications is in single photon source.

5.7 Single Photon Source (SPS)

Single photon source is a beam of light that contains one photon that is generated by using a semiconductor quantum dot. The process that is used to generate a single photon source is described as follows:

- The semiconductor quantum dot is put into the optical microcavity that has reflecting faces.

- Direct any type for energy towards the semiconductor atom For instance, laser energy and electric pulse. The electron absorbs the energy and goes from the valance band of an atom to the conduction band, then an electron comes again to the valance band with emit a single photon.
- The process of emitting a single photon called simultaneously emission.
- The reflecting faces of microcavity work by reflecting the beam of light inside the microcavity.

5.7.1 Implementation of BB84 By Using Quantum Dot Single Photon Source .

Using the classical source of laser beam it is difficult to produce a single photon of light. The pulse of beam contains more than one photon. The process of transmission in BB84 built on this pulse is not secure because Eve can acquire information about the photon polarization by splitting the beam, all the photons in the same pulse have the same polarization, which means the photons have the same information about the classical bit. Quantum key distribution recently uses the quantum dot single photon to transmit the information in its protocols. The transmission by using quantum dot utilizes quantum key distribution advantages, for instance, any attempt to intercept from Eve will be detected, in addition is to generate successive photons in a short time. There are different types of semiconductors that can be used to generate a single photon. For example, using indium arsenide (InAs)and indium phosphide (InP) samples. The practical implementation of the BB84 quantum dot is described as below:

- In Alice's circuit, Alice excites the sample of semiconductor by using an electrical pulse. The beam of light that is produced is collected by using a microscopic object (MO) (Heindel et al., 2012).
- The light goes through bandpass filter BP (Heindel et al., 2012) which allows for a certain frequency to pass. The BP beam goes inside through single mode fiber (SMF) (Heindel et al., 2012) Its functionality to transmit the single beam of light by total internal reflection from one point to another.
- The beam is polarized by using a polariser and Alice uses electro-optic modulator (EOM) to select her rectilinear or diagonal basis, then she sends the polarized single beam of light through free space channel.
- In Bob's circuit, Bob receives the incoming single beam of light and passes it through two Quarter wave plates (QWP), it used to compensate quite damaged in the polarization of a beam of light.
- The beam strikes the beam splitter (BS) which transmits or reflects the beam with probability one-half for each of two rectilinear and diagonal bases.
- If the single photon is reflected, then it will be measured in the rectilinear basis, If the photon transmitted will be measured on the diagonal basis.
- In this scheme the selection of a basis is built on the probability of either the single photon reflected or transmitted, the probability that bob chooses the wrong basis is one-half.

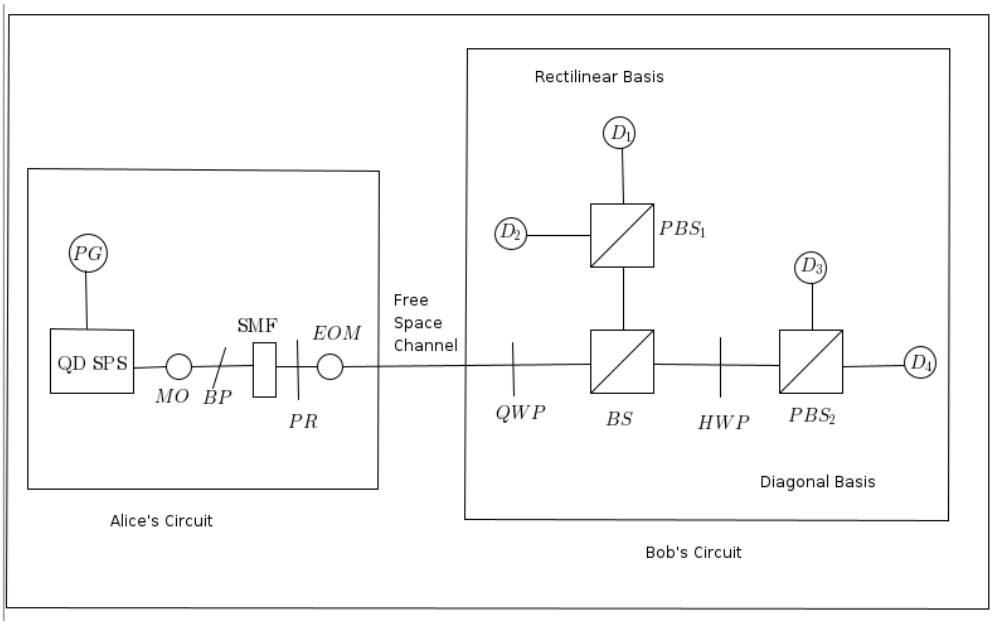

Figure 5.3: The practical implementation of BB84 by using quantum dot single photon source

6. Conclusion

The summary, BB84 protocol used the polarization of photons and spin of the electron to transmit the signal between the two parties, BB84 gain its security due to the disruption in the qubit if Eve intercepts the transmission, Alice and Bob reduce Eve's information about the key by applying the process of error correction and privacy amplification. Alice could cheat by using EPR pair of photons. B92 is a new modified version of BB84 used two non-orthogonal bases instead of used four orthogonal bases. The implementation of polarization of photon and phase encoding not secure due to the photon number single attack where Eve measures the photons in the pulse by using non-demolition measurement before dividing the pulse. Quantum key distribution used the single-photon source quantum dot to creates a single photon in the transmission instead of used a pulse of the photon. We have demonstrated that the quantum dot made the protocol secure by producing single-photon nevertheless reduced the efficiency of the implementation to 50 percent due to the random choice of detectors in Bob's Basis.

6.1 Future Work

From the disadvantage of the quantum dot is to reduce the performance of the implementation to 50 percent due to the random choice of the detector this reason made Bob choose the right bases with probability one-half, to solve his problem we need to figure out a method to modify the beam splitter to govern the direction of reflected and transmitted beams.

Acknowledgements

All applaud and honour belong to Allah, the Almighty. I am very much thankful and appreciative to the Almighty Allah for giving me strength and protection in the completion of this piece of work.

I wish to express my heartfelt appreciation to my humble supervisor Prof. Jeff Sanders, for his tireless guidance during this work. I am also very thankful to my tutor Bernard Lebeko Poulo for his efforts and support. My or A special thanks also goes to entire members of staff and students of AIMS, South Africa for their constant support and motivation. They used most of their precious time and energy in modelling me both morally and academically. Very special thanks also goes to my friends who have also given me extra help and support ever since.

Finally, my very special heartfelt and thanks goes my family members for their unlimited love, prayers, and words of encouragement right from the beginning.

References

Abbas, A. M., Goneid, A., and El-Kassas, S. Privacy amplification in quantum cryptography bb84 using combined univarsal2-truly random hashing. *International Journal of Information and Network Security*, 3(2):98, 2014.

Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., and Smolin, J. Experimental quantum cryptography. *Journal of cryptology*, 5(1):3–28, 1992.

Bhandari, R. Quantum error correcting codes and the security proof of the bb84 protocol. *arXiv preprint arXiv:1409.1452*, 2014.

Blt, M. Coin flipping by telephone a protocol for solving impossible problems. 1981.

Gaidash, A., Egorov, V., and Gleim, A. Revealing of photon-number splitting attack on quantum key distribution system by photon-number resolving devices. In *Journal of Physics: Conference Series*, volume 735, page 012072. IOP Publishing, 2016.

Goneid, A., El-Kassas, S., El-Ashmawy, M., and Abbas, A. Enhancement of error correction in quantum cryptography bb84 protocol. *Egyptian Computer Science Journal*, 31(2), 2009.

Griffiths, D. J. Introduction to quantum mechanics. *2nd, Pearson, Chapter2. The time-independent schrodinger equation*, pages 70–73, 2005.

Heindel, T., Kessler, C. A., Rau, M., Schneider, C., Fürst, M., Hargart, F., Schulz, W.-M., Eichfelder, M., Roßbach, R., Nauerth, S., et al. Quantum key distribution using quantum dot single-photon emitting diodes in the red and near infrared spectral range. *New Journal of Physics*, 14(8):083001, 2012.

Hughes, R. J., Morgan, G. L., and Peterson, C. G. Quantum key distribution over a 48 km optical fibre network. *Journal of Modern Optics*, 47(2-3):533–547, 2000.

Inoue, K. Quantum key distribution technologies. *IEEE journal of selected topics in quantum electronics*, 12(4):888–896, 2006.

Kohnle, A. and Rizzoli, A. Interactive simulations for quantum key distribution. *European Journal of Physics*, 38(3):035403, 2017.

Lo, H.-K. and Zhao, Y. Quantum cryptography. *arXiv preprint arXiv:0803.2507*, 2008.

Mehic, M., Partila, P., Tovarek, J., and Voznak, M. Calculation of key reduction for b92 qkd protocol. In *Quantum Information and Computation XIII*, volume 9500, page 95001J. International Society for Optics and Photonics, 2015.

Perry, A., Sun, R., Hughes, C., Isaacson, J., and Turner, J. Quantum computing as a high school module. *arXiv preprint arXiv:1905.00282*, 2019.

Ruiz Alba Gaya, A., Calvo Díaz-Aldagalán, D., García Muñoz, V., Martínez García, A., Ocampo, A., Alexander, W., ROZO CHICUE, J. G., Mora Almerich, J., and Capmany Francoy, J. Practical quantum key distribution based on the bb84 protocol. In *Waves*, volume 1, pages 4–14. Instituto de Telecomunicaciones y Aplicaciones Multimedia (iTEAM), 2011.

Sabottke, C. F., Richardson, C. D., Anisimov, P. M., Yurtsever, U., Lamas-Linares, A., and Dowling, J. P. Thwarting the photon-number-splitting attack with entanglement-enhanced bb84 quantum key distribution. *New Journal of Physics*, 14(4):043003, 2012.

Skander, A., Nadjim, M., and Malek, B. A new accurate quantum cryptography control error reconciliation (qccer) with xor operator in bb84 protocol. *ICIC Express Letters*, 2(2):187–192, 2008.

Todd, J., Samari, K., Zacharias, T., Zhou, H., and Chaidos, P. Primitives and protocols.

Yang, C.-N., Kuo, C.-C., et al. Enhanced quantum key distribution protocols using bb84 and b92. In *Proceedings of the 2002 International Computer Symposium*, volume 2, pages 951–959. Citeseer, 2002.

Zhu, G. and Singh, C. Improving students' understanding of quantum mechanics via the stern–gerlach experiment. *American Journal of Physics*, 79(5):499–507, 2011.