NATIONAL AND KAPODISTRIAN UNIVERSITY OF ATHENS

SCHOOL OF SCIENCE
DEPARTMENT OF INFORMATICS AND TELECOMMUNICATION

MSc THESIS

Simulating a Classical Analogue of a Quantum Key Distribution Protocol with VPI

Ahmed W.Waheed

Supervisor (or supervisors): **Dimitris Syvridis ,** Professor
Dr Thomas Nikas
Dr Aikaterini Mandilara

ATHENS

September 2022

MSc THESIS

Simulating a Classical Analogue of a Quantum Key Distribution Protocol with VPI

Ahmed W.Waheed
S.N.: 7115192100006

SUPERVISORS: **Dimitris Syvridis ,** Professor
Dr Thomas Nikas
Dr Aikaterini Mandilara

ABSTRACT

Quantum Key Distribution (QKD) is an evolving research area and receiving growing attention as it provides unconditional security in data communication. The BB84 QKD protocol is a fundamental protocol in quantum communication. In the original BB84 protocol the polarization of the photon is employed as the relevant degree of freedom but since that time more convenient scenarios have emerged. The VPI-Photonics software does not offer the features of quantum, for example a single or few photon source and photo diode that can detect single or few photons. So it is difficult to build a QKD model for the users. Instead of this, they already offer a plethora of built in classical photonic modules with a lack of quantum detail. This Classical analogue model of phase-encoding BB84 QKD protocol helps to understand all the details of original phase-encoding BB84 QKD protocol and explore the sensitivity of to various photonic parameters such as the fiber dispersion, PMD etc. We proved that with the help of experiments, that the functioning of this classical protocol is same as the original QKD protocol except the security feature, as this classical protocol can be easily eavesdropped. The major difference of this classical protocol is that the optical pulses have much higher number of photons then the original QKD protocol where the average number of photons per coherent pulse is less than 1.

SUBJECT AREA: Photonics

KEYWORDS: Quantum cryptography (QC), Quantum Key Distribution (QKD), secure Communication

ACKNOWLEDGEMENTS

This Master Thesis has been accomplished in the framework of the European Funded Project: **SMART Telecom and Sensing Networks (SMARTNET)** - Erasmus+ Programme Key Action 1: Erasmus Mundus Joint Master Degrees – Ref. Number 2017 – 2734/001 – 001, Project number - 586686-EPP-1-2017-1-UK-EPPKA1-JMD-MOB, coordinated by **Aston University,** and with the participation of **Télécom SudParis, member of IP Paris** and **National and Kapodistrian University of Athens.**

CONTENTS

LIST OF FIGURES

LIST OF TABLES

PREFACE

Ahmed Waheed received his Bachelor degree in Electrical Engineering with Gold Medal from University of Punjab, Pakistan in 2012.He has worked as Lecturer in Electrical Engineering Department of Superior University Lahore, Pakistan. He has completed his Master degree in program Smart Telecom and Sensing Network (SMARTNET) from National kapodistrian University of Athens (NKUA) and Institut Polytechnique De Paris.

I would like to appreciate and thank to a number of people,

Professor Dimitris Syvridis for giving me the opportunity to study and research in Photonic laboratory (OptCom). Before starting this thesis I have completed one project 'Physical Security in Optical Communication' which really build my interest in photonic field.

Dr Thomas Nikas and Dr Aikaterini Mandilara for assisting me for conducting experiments and their explanation for solving problem and finally with the proof reading of this thesis.

I really want to thank SMARTNET team who helped in every prospect of this master degree problem.

My Dad and Mom who have inspiration for me, their psychological and continuous financial support since my childhood help me to deal with numerous challenges.

1. INTRODUCTION

1.1 Overview of Quantum Cryptography

The security of current communication systems is based on the premise that breaking cryptography is slow using the existing conventional computers. This includes communications between data-centres, inter-governmental communications, or critical financial and energy infrastructures. However, the commonly adopted classical cryptography schemes can be jeopardized by the advent of quantum computers owing to their capability to solve computationally intensive problems much faster than conventional computers. Although sufficiently powerful quantum computers are not yet fully developed today, this evolving research area is drawing a growing attention in the face of a risk that quantum computers will be used to break the encryption in the future. Interestingly, we can use the quantum properties to create strictly secure cryptography beyond the capabilities of current classical systems. Specifically, QKD (Quantum Key Distribution) uses laws of quantum mechanics to enable the unconditional security for exchange of encryption keys.

In QKD systems, encrypted data is sent as classical bits over networks, while the keys to decrypt the information are represented by the quantum states of the photons that are transmitted in terms of quantum bits (qubits) [1]. As follows from the laws of quantum mechanics, the eavesdropping of the quantum keys can be detected, which allows to take counter-measures and e.g. change the key. Hence, QKD has a capability to maintain information-theoretic security. These quantum technology advancements pave the way towards establishing a novel communication network based on QKD which will be able to interconnect remote computers and servers similar to the classical Internet. QKD protocols is unconditional secure to share secret keys. Previously extremely high computational complexity required to decrypt the message in traditionally cryptographic methods, but in QKD the security is based on physical laws. There are two fundamental laws of quantum mechanics which protect quantum information to be eavesdropped. First the no-cloning theorem states that it is impossible to copy a quantum system in a deterministic way. Second, distinguishing non orthogonal unambiguous quantum states cannot be perfectly achieved.

Theoretically QKD is perfectly secure but there are several problems encounters. One of them is decoherence that is basically the loss of quantum coherence. There are many reason of decoherence including electromagnetic waves, vibrations, and variation in temperature. Another problem is error correction which is used to secure information from errors. The errors is generated due to noises and decoherence. The basic principle of error correction based on repetition. Due to no cloning theorem the copies of quantum information is not possible. So an efficient error correction scheme [2] is needed which not contradict the laws of physics.

1.2 Basic Elements of Quantum Mechanics

In order to arrive to present the QKD protocol under study we review here some basic elements of quantum mechanics.

Qubits

The basic unit of quantum information is qubit. This is also known as quantum bit. There are several particles whose degree of freedom can be used in quantum computing for example photons. Qubit is also considered as two state quantum mechanical system for example spin of electron in two level either spin up or spin down [3].While classical Bit is considered as one state in classical system in quantum mechanics qubit allows to be in coherent superposition of both states at the same time. Qubit state is the coherent superposition of basis state and it is described by linear combination of $|1>$ and $|0>$.

$$|\varphi> = a|0> + b|1>$$

Where a and b are complex numbers that represent probability amplitudes.

The probability ampitude is calculating as follow:

$$P(0) = |a|^2 \quad , \quad P(1) = |b|^2$$

Coherent State

The coherent state of quantum harmonic oscillator is a classical practices of classical harmonic oscillator [4]. Mathematically, coherent state $|\alpha>$ is represented by

$$\hat{a}|\alpha> = \alpha|\alpha>$$

$$\alpha = |\alpha| e^{i\theta}$$

Where $|\alpha|$ = Amplitude of the state

θ = Phase of the state

The earliest quantum cryptography protocols consider single photon sources but it is non-classical and impossible to build. The current quantum protocols based on coherent states because laser that emit coherent states is easy to operate. When the number of photons are very high the Heisenberg uncertainty becomes negligible and the coherent states become classical one.

1.3 Quantum Key Distribution (QKD) Protocols

1.3.1 General QKD Protocol

There are two basic ways to implement QKD schemes [5]. 1) Discrete Variable Quantum Key Distribution DVQKD: In this scheme on the receiver side (Bob), the single photon detector is used. This scheme satisfy the both physics law mentioned above. 2) Continuous variables Quantum Key Distribution CVQKD: Homodyne/Heterodyne detection is used in this scheme. This scheme follow the uncertainty law of physics, both the in-phase and quadrature component cannot be measured simultaneously with precision in case of coherent state. In this thesis we will occupy with a phase-encoding scheme that mainly belongs to the DVQKD category, using single photon detectors but which borrows elements CVQKD using weak coherent pulses as a source.

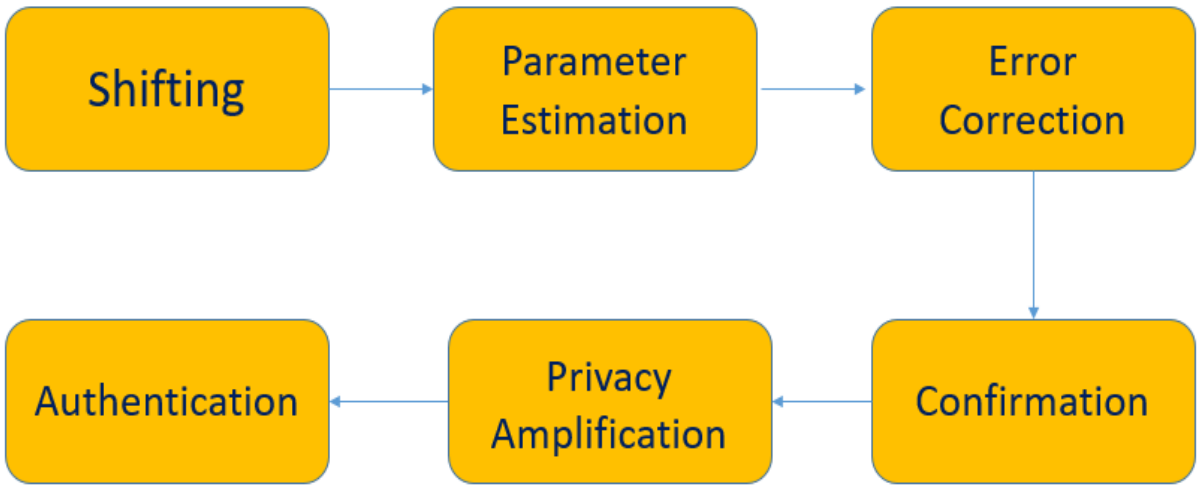


Figure 1-1: Six Steps of General QKD Protocol

The general QKD protocol [6] have 6 steps as shown in Figure 1-1. Alice sends qubits through insecure quantum channel. In the first step shifting phase eliminate the qubits by Alice and Bob that are measured using uncorrelated bases. The second step is parameter estimation which help to calculate the amount of access noise by sharing small part of key sequence between Alice and Bob over classical public channel. The presence of Eavesdropper can be detected with the help of this noise variance estimation. Accordingly, if the estimated noise variance is too large, the protocol is re-initialized. If no eavesdropping is detected, error correction is performed either by Alice or Bob by exchanging information about the key, which can be viewed as redundancy in sense of traditional forward error correction coding. This is done in order to decouple the non-orthogonal quantum states and decide about the actual qubits. There is still probability of wrong detection after the error correction step. Therefore confirmation step is required where Alice and Bob apply a common hash function to their bit streams and compare the results. This operation confirms that the keys on both sides are identical. After that in privacy amplification step Alice and Bob select some identical and random sets of bits to decrease the probability that eavesdropper can access some of qubits. The last is authentication where both legitimate users use universal hash function to guarantee the security of classical channel.

1.3.2 BB84 Protocol

The first QKD BB84 protocol was introduced by Bennett and Brassard in 1984 [7]. Its basic steps are as follows:

Objective: Alice and Bob wants to share information through public and quantum channel.

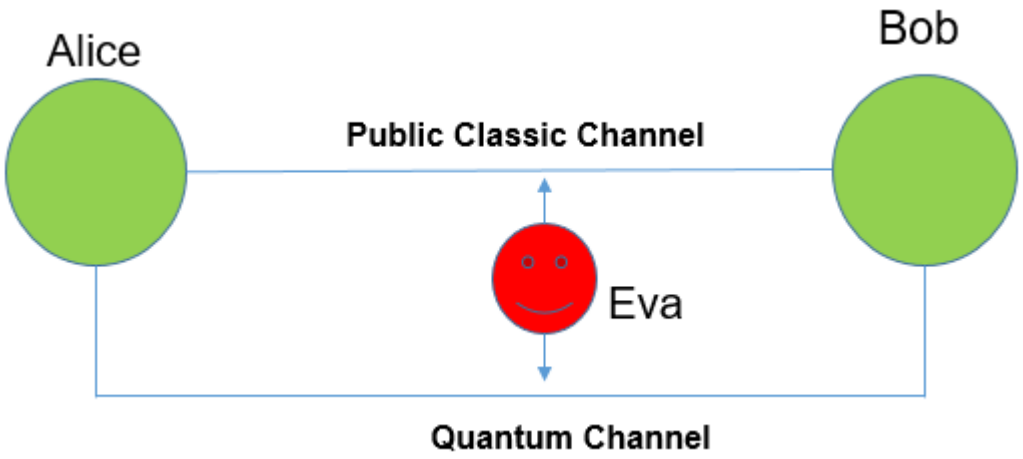


Figure 1-2: Information Sharing between Alice and Bob

Alice Encoding:

Step-1: Alice generates two two n bit strings

$$x = x_1x_2x_3.....x_n$$

$$y = y_1y_2y_3.....y_n$$

Where

y_k determines the basis of encoding

x_k determines the encoded state

Step-2: Alice create of the quantum state

$$|\Psi> = {}^{n}\bigotimes_{k=1} |\Psi_{x_k y_k}>$$

There are four possible quantum states given in Table 1-1.

Table 1-1: Four Quantum States of BB84 QKD Protocol

Basis-Z	Basis-X
$\|\Psi_{00}> = \|0>$	$\|\Psi_{01}> = \|+>$
$\|\Psi_{10}> = \|1>$	$\|\Psi_{11}> = \|->$

Alice encode the information either in basis X or in basis Z using four possible state.When y_k = 0 the quantum state will be in basis Z either 0 or 1. When y_k is 1 the

quantum state will be in basis X. It is either + or -. Similarly when x_k is zero Alice will create +1 quantum state and in case of 1 it create -1 state. In order to understand these consider Alice encode information with the help of these two states $|\Psi_{00}> = |0>$, $|\Psi_{10}> = |1>$ in Z basis , If Bob also performed measurement in Z basis the outcome will always +1 or -1 with 100% probability because the basis is same. Similary When Alice encode information with two states $|\Psi_{01}> = |+>$, $|\Psi_{11}> = |->$ in X basis and Bob measure in X basis the outcome will always be +1 or -1.On the other hand if Alice encode information with these two states $|\Psi_{00}> = |0>$,$|\Psi_{01}> = |+>$ and Bob measure in Z basis then for first state outcome will always be +1 but for second state the outcome can be +1 or -1.For the first state Alice and Bob basis are same this is the reason the 100% probability of outcome +1 but for the second state Alice encode with basis X and Bob measure in Z basis.Therefore the outcome can be +1 or -1 because basis are different .In the same manner If Bob meseure these two states in X basis first state outcome is +1 or -1 and second state outcome will always +1.

Lets take an example of Alice side encoding.

Table 1-2: Alice Encoding

string x	0	1	1	0
string y	1	1	0	0
basis	X	X	Z	Z
Encoded qubits	$\|+>$	$\|->$	$\|1>$	$\|0>$

Alice generate two randome string x and y as shown in Table 2. String x is information and string y is randomly generated secret key. First bit of string x is 0 and y is 1 , Alice encode this into X basis and encoded qubit is $|+>$ according to Table 1-1. Similarly for the second bit the basis is X but encoded qubit is $|->$. Third and fourth bit of string y is 0, Alice encode into Z basis and encoded qubits are $|1>$ and $|0>$ because string x third and fourth bit is 1 and 0.

Bob Measurements:

After the encoding process,Alice sends encoded qubits to Bob through public channel.Bob receive the encoded qubits but still unaware of secret sting y, because Alice did not share sceret string y.Now Bob unable to decode the Information due to lack of string y.Bob know the encoded qubits will be any of the four possible states.So Bob generate his own random bit string y` and measure the basis of received qubits accoring to string.

$$y` = y_1`y_2`y_3`.....y_n`$$

Similary to Alice

If $y_k` = 0$, Bob measure K^{th} in Z basis

If $y_k` = 1$, Bob measure K^{th} in X basis

If K^{th} outcomes is +1 , then $x_k` = 0$

If K^{th} outcomes is -1,then $x_k` = 1$

In this way Alice and Bob share their bit strings y and y`over public classical channel with each others.

When $y_k = y_k`$ , both keep $x_k$ and $x_k`$ bits

If $y_k \neq y_k`$, both dicards the $x_k$ and $x_k`$ bits

If Bob and Alice measure the basis in same manner they both keep the encoded state bits otherwise they discard.

Bob decoding example:

Table 1-3 : Bob Decoding

String y`	1	0	0	1
Bob basis	X	Z	Z	X
String x`	0	0/1	1	0/1

From Table 1-2 and Table 1-3,we can observe Bob measure first bit of string y` in same basis as Alice first bit and $x_k$ and $x_k`$ are same.So we can say there is 100% probability of outcome +1.Bob measure second bit of string y` in different basis as compared to Alice second bit so there will be 50% probability of outomes for string x` either 0 and 1.They dicard this bits.Similarly for third bit they both measure in same basis so there is again 100% probability of outcome -1 and same rule apply for the fourth bits.In this example the **Alice and Bob have shared key 01**.

1.3.3 Phase Encoding BB84 QKD Protocol with Single Photons

The elements for the initially proposed experimental set-up [8] for phase encoding QKD shown in Figure 1-3. Laser diode as source ,Beam Splitter ,Phase Modulator and Photon Detector. The source is emitting sinlge photons described by the Fock states. These are inputs to the one port of the beam splitter and in the other vaccuum. The steps for sharing the key with this set-up are in detail described below.

Step-1: Fock basis state at the input of beam splitter is $|01>_{ab}$

Step-2: The beam splitter converts this state into

$$\frac{1}{\sqrt{2}}(i \,|01>_{cd} + \,|10>_{cd})$$

Step-3: The next stage consist of Mach zehnder branches ,which help to introduced phase shift

$$\frac{1}{\sqrt{2}} (i . e^{-i.\frac{\varphi}{2}} . |01>_{cd} + e^{i.\frac{\varphi}{2}} |10>_{cd})$$

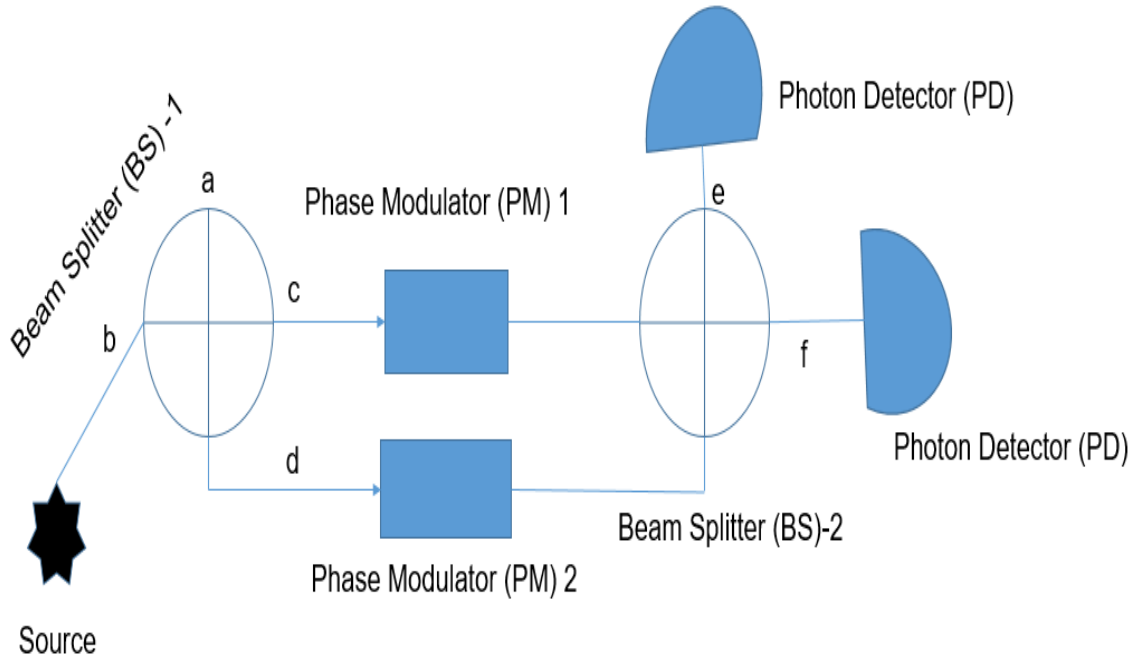


Figure 1-3 : Phase Encoding BB84 QKD Protocol

Where $\phi = \phi_1 - \phi_2$

ϕ_1 is phase shift in Upper branch

ϕ_2 is phase shift in Lower branch

Step-4: Later stage consists of beam splitter which convert this beam into fowllowing states:

$$|01>_{cd} = \frac{1}{\sqrt{2}}(i\,|01>_{ef} + |10>_{ef}$$

$$|10>_{cd} = \frac{1}{\sqrt{2}}(i\,|10>_{ef} + |01>_{ef}$$

The output can be shown with the help of wave function

$$|\Psi(\varphi)> = i.(\sin(\tfrac{\varphi}{2})).|01>_{ef} + \cos(\tfrac{\varphi}{2}).|10>_{ef}$$

Alice randomly selects the phase shifts [9] ϕ_1

$$\phi_1 = \{0, \pi, -\pi/2 \text{ and } \pi/2\}$$

Bob randomly selects the phase ϕ_2

$$\phi_2 = \{0, \pi/2\}$$

Based on these phases BB84 QKD protocol states are as follow:

$$|\Psi(0)> = |0>$$

$$|\Psi(\pi)> = |1>$$

$$|\Psi(\pi/2)> = i.\, 2^{-1/2}\,(\,|10>_{ef} + |01>_{ef}\,) = |+>$$

$$|\Psi(-\pi/2)> = i.\, 2^{-1/2}\,(\,|10>_{ef} - |01>_{ef}\,) = |->$$

Single photon detector is used at the last in order to detect the photons.

1.3.4 Phase Encoding BB84 QKD Protocol with Coherent States

In BB84 QKD protocol proof, Transmitter (Alice) consider single photon source. In practice ideal single photon source is not available at demand but it acts in a probabilistic way while coherent. Coherent state laser are widely used as a source in practical QKD [10].There are two inputs coherent state $|\alpha>_B$ and vaccuum $|0>_A$.

The Fock state representation of coherent state $|\alpha>$ is given

$$e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}\,|n>$$

The coherent state input is provided to beam splitter.

Stage -1: Passing through 50:50 Beam Splitter (BS) -1

For normalized state $<\alpha|\alpha) = 1$

Since

$$|\alpha> = D(\alpha)\,|0>$$

As

$$D(\alpha) = \exp(\alpha a^{\dagger} - \alpha^{*} a)$$

Now

$$|0>_A\,|\alpha>_B = |0>_A\,D(\alpha)\,|0>_B$$

$$|0>_A\,|\alpha>_B = D(\alpha)\,|0>_A\,|0>_B$$

$$|0>_A\,|\alpha>_B = \exp(\alpha a^{\dagger} - \alpha^{*} a)\,|0>_A\,|0>_B$$

After replacing above value the output of beam splitter is given below

$$|0>_A\,|\alpha>_B \rightarrow \left|\frac{\alpha}{\sqrt{2}}\right>_C \left|\frac{\alpha}{\sqrt{2}}\right>_D \qquad (1)$$

The output of first beam splitter (BS) is two coherent state. When the inputs of beam splitter are coherent state and vacuum. From the eq. 1 we observed that the coherent state become weak.

Stage -2: Passing through Mach-Zehnder branches:

The output after phase modulator are followings:

$$C = \left(\frac{\alpha}{\sqrt{2}}\right) . \exp\ (i. \varphi_1)$$

$$D = \left(\frac{\alpha}{\sqrt{2}}\right) . i. \exp\ (-i. \varphi_2)$$

Stage -3: Passing through Beam Splitter (BS)-2 :

The input of second beam splitters are now two coherent state C and D.

$$|C>_C\ |D>_D = D(C)\ .D(B).\ |0>_C\ |0>_D$$

$$|C>_C\ |D>_D = \exp(Cc^{\dagger} - C^{*}c)\ .\exp(Dd^{\dagger} - D^{*}d).\ |0>_C\ |0>_D$$

Replace the values of C and D

$$|C>_C\ |D>_D \rightarrow$$

$$\left|\left(\frac{\alpha}{\sqrt{2}}\right) .\exp\ (i.\varphi_1) - \left(\frac{\alpha}{\sqrt{2}}\right) . i.\exp\ (-i.\varphi_2)>_E\ \right| \left(\frac{\alpha}{\sqrt{2}}\right) .\exp\ (i.\varphi_1) - \left(\frac{\alpha}{\sqrt{2}}\right) . i.\exp\ (-i.\varphi_2)>_F \qquad (2)$$

The output of second second beam splitter is shown in above equation 2.

Step -4 : Photo detector

The laser source generate coherent pulses mentioned in equation 1. with μ (average photon number)

Where $\mu = |\alpha|^2$

The probability is calculate with Poisson statistics [11] that pulse having n photons pass through beam splitter is given below

$$P_n = \frac{\mu^n.\exp(-\mu)}{n!}$$

The photo detector APD detect two independent Poisson statistics beam with quantum efficiency less than 1 repsented by η.The probability to generate photoelectron in detector is given by the following equation

$$P_n = \frac{(\frac{1}{2}\mu\eta)^n . \exp(-\frac{1}{2}\mu\eta)}{n!}$$

1.3.5 Decoy State Protocol

In order to reduce the effect of multi-photon source, one method is to utilize very weak laser source. The disadvantage of this technique is that it will reduce the speed of QKD. Another method to solve the multi-photon issue is using different photon intensities instead of one [12]. This technique is called **Decoy state** .This is very effective method to solve the problem of PNS attack. In decoy state technique Alice transmit qubits using randomly choosing intensities levels consists of 1 (one) signal state and several decoy states. This will result in varying photon number statistically all over the channel. When the transmission between Alice and Bob has completed Alice publicly announce the intensity level he used during the transmission of each qubits. Each intensity level associated with BER, by observing BER the Alice and Bob detect a PNS attack [13, 14]. This technique will help to increase transmission rates and increase channel length.

1.3.6 T12 Protocol

In this section we explain an improved version of phase encoding BB84 with weak pulses and decoy states which is used in the apparatus of the group.

Earlier for the security proof of Quantum Key Distribution (QKD), there are two consideration has been taken into account:

1) Single photon source is ideal

2) For experiments infinite dataset is available.

In practical experiments of BB84 QKD protocol the situation is not same. Ideal single photon is not available. Secondly asymptotic scenario (infinite dataset) consider for experiment. This create problem to overestimate the security level of protocol because the parameters of QKD including QBER and security key etc. estimate with infinite dataset.

Since QKD doing fast progress towards real world application. The demand of efficient protocol is much needed. This efficient protocol is not only considering ideal scenario but also demonstrate security proof in real experiment situation. Efficient version of BB84 protocol is proposed in [15].This introduced a technique by combining the decoy state with attenuated laser. It is more efficient than using single photon source.

This efficient protocol named as T12 protocol which focus on practical implementation of QKD protocol rather than idealisation assumption. This protocol consider finite size security proof. This offer tremendous advantages firstly the security key is secure with respect to the application it is used with small probability of failure. Secondly, the use of sequential model and threshold detector. The drawback of this protocol the key rate remains position for large sample sizes when decoy states are considered.

1.4 Motivation for the Research in this Thesis

Since traditional networking methods are vulnerable to a variety of attacks, classical data encryption cannot provide unconditional security anymore. In contrast, QKD protocols allow to share secret keys with unconditional security. Unlike traditional cryptographic methods that rely on the extremely high computational complexity required to decrypt the message, the security of QKD is based on physical laws. These quantum technology advancements pave the way towards establishing a novel communication network based on QKD which will be able to interconnect remote computers and servers similar to the classical Internet.

Many QKD protocols have been proposed. The celebrated BB84 QKD protocol work as a fundamental protocol. Studying the classical analogue of this protocol give us the opportunity to delve into its key practical points with the help of VPI software. In this thesis we mainly focus on Phase encoding BB84 QKD protocol. Since this is related to the experimental equipment available in the optical communication (OptCom).

1.5 Summary

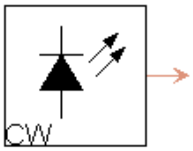
Chapter 1 starts with the brief introduction of quantum cryptography techniques.Some basic elements, including qubits and specially coherent states used as input of classical model were briefly discussed here. Next we describe the various protocols starting from the general QKD protocol,BB84 ,Phase-Encoding BB84,Decoy State and T12 protocol. We also shows mathematical derivation with two different input of Phase-Encoding BB84 QKD protocol.One is with single photon and another is with coherent state. In the last section, the motivation behind this research is elaborated.

2. Implementing a Classical Version of Phase-Encoded BB84 QKD Protocol on VPI

2.1 Description of Components

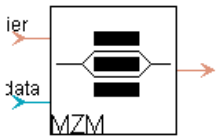
This section describes the working of main components of VPI-Photonics Software used in simulation of classical version of phase-encoded BB84 QKD protocol.

LaserCW



This module generate a CW (continuous wave) optical signal and it models as DFB laser. The radiation of a continuous wave laser is describing by generating a time dependent field E (t) with specific frequency, polarization, linewidth and power. There are two major types of output data 'Parameterized and Blocks'. This module produce parameterized signal with certain polarization and power if the output data type is parameterized. The frequency of this signal is same as the emission frequency parameter value. On the other hand if the output data type is Blocks then module parameters centre frequency and sample rate produce the field E (t) represented by sample band with bandwidth defined by centre frequency.

ModulatorMZ



The amplitude of an optical wave is controlled by Mach-Zehnder modulator (MZM) [17] .This module mainly estimate frequency chirp derive from the modulator asymmetry. There are two ways to specify the chirp of the modulator first chirp sign and second symmetry factor. There are two input port of this module carrier and data. The carrier port derive optical carrier signal .The data type of this port either optical samples or optical blocks. The second input port data is responsible for electrical modulation signal. The data type of this port is either electrical samples or electrical blocks. There is only one output port for modulated optical signal with data type optical samples or optical blocks.

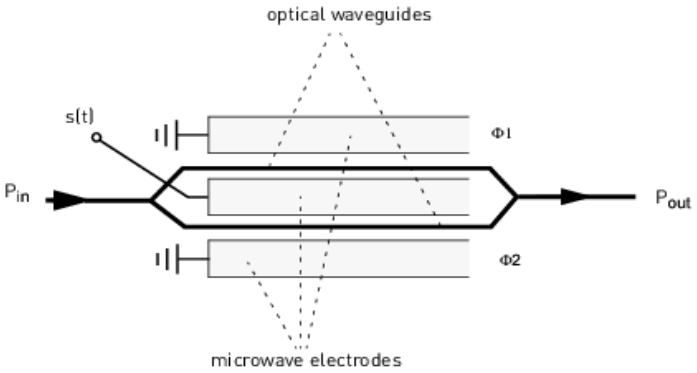
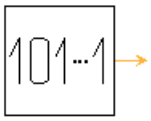


Figure 2-1: Schematic of Mach- Zehnder Modulator

Figure 2-1 shows the Mach-Zehnder Modulator (MZM) derive by single RF port. The operation of this type of modulator mainly depends on the design and configuration of electrodes [18]. For example there are two waveguide interferometer arms. Applied voltage across one of the arm and the wave passing through the same arm induced phase shift. The phase difference between two waves transform into amplitude modulation when the two arms recombine.

PRBS



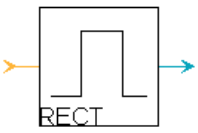
This modules produces different types of pseudorandom data sequences mentioned in table.

Table 2-1: Random Data Types

PRBS
De Bruijn sequences of order N
Alternate zeros and ones
Predefined sequences
All zeros and all ones

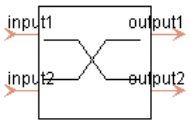
Wichman–Hill–Generator will be used to generate sequence when PRBS type is selected in the module [19]. The probability of '1' can be specified with the help of parameter Mark probability. When the type is DB_KN then this module generate k-ary De Bruijn sequence [20]. The order of this sequence is set by the parameter PRBS_Order. Alternate ones and zeros can be generated by selecting Alternate type. There is also an option in this module to read from user defined file.

PulseRectangEl



When the bit sequence is given as a input to module, this produce sample electrical rectangular pulses. These pulses can be used to derive amplitude modulator.

X_Coupler

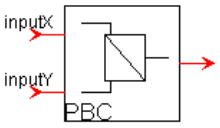


The main purpose of this module to split or combine the optical pulses. The splitting and combining depends on the coupling factor signals. This module have two input port and two output port. The optical signal division depends on coupling factor [21].

ModulatorPM

This module is an ideal phase modulator. There are two input ports of this module carrier and data. The phase modulation is done based on the electrical signal provided at the data input. This module has no effect on the optical power of the signal provided at the input.

CombinerPol



This module model as Polarization Beam Combiner (PBC) rotated through an angle. The working of PBC is shown in Figure.

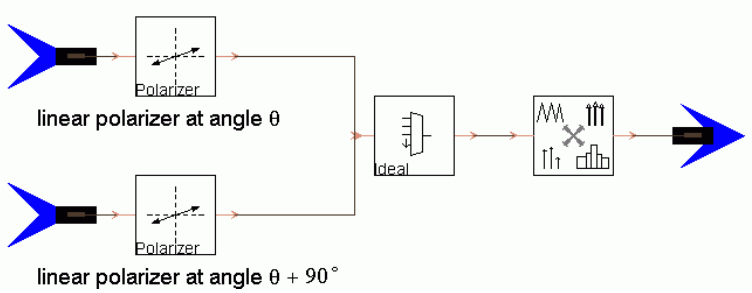
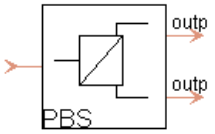


Figure 2-2 : Operation of Polarization Beam Combiner (PBC)

The input X and input Y consists of two ideal linear polarizer. These are orthogonal to each other. After selecting the appropriate polarization the result is feed to ideal multiplexer. Signal converter is used after the multiplexer. This signal converter module help to join the parameterized signals for example when there are parameterized signals with same frequency at both input X and input Y the multiplexer output spectrum consists of two signals with same frequencies.

SplitterPol



This module models as Polarization Beam Splitter (PBS) rotated through an angle theta. The working of PBS is shown in Figure 2-3.

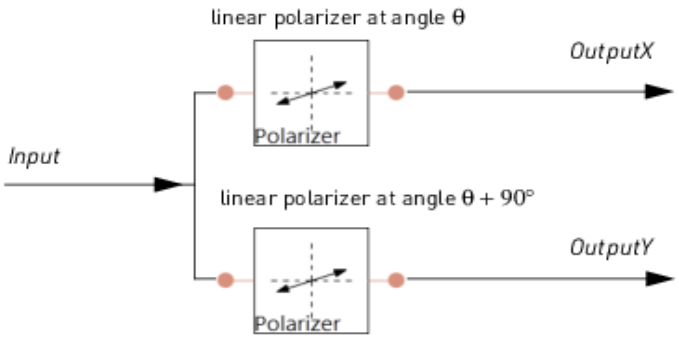
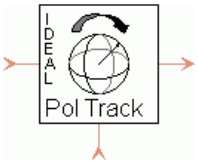


Figure 2-3 : Operation of Polarization Beam Splitter (PBS)

It consists of two linear ideal polarizer placed orthogonal to each other.The input optical signal polarization components aline with accordingly to x polarizer (upper path) and y polarizer (below path). It is represented as outputX and OutputY.

PolTrackIdeal

When the signal is passing through the fibre the signal is disturb by polarization mode dispersion (PMD) and attenuation etc. This module will help to correct the original SOP (State of Polarization).The signal after the optical fibre linked to the input of polarization controller and the reference signal provided to the reference port.

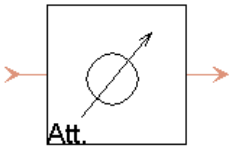


This module aligns the output SOP to the reference SOP.This module assess the rotation matrix given to the input signal in order to correct the state of polarization based on reference signal with maximum accuracy.

Photodiode

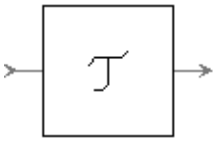
There are two types of photodiode PIN and APD. This module deal with both type of optical signal single mode and multi-mode. The functionality of this module depends on the avalanche multiplication, responsivity, noise and dark current. In optical communication this module also used as receiver as it receive optical signal and convert it into electrical signal.

Attenuator



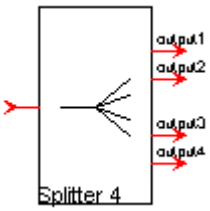
This module attenuate the optical signal. In our design this module is used to adjust the intensity of optical signal.

Delay Signal



By applying the time shift of the sample signal this module estimate propagation delay of electrical and optical signal. This delay induce a phase shift in case of optical signals on either relative or absolute signal frequency. It can also be constant phase shift. The delay time is non integer or integer multiple of the sample period in case of sampled signal. This module is also helpful to remove deadlocks

Beam Splitter



Beam splitter have one input and four output ports. It helps to split optical input signal into four output signals. This module consists of three cross couplers.

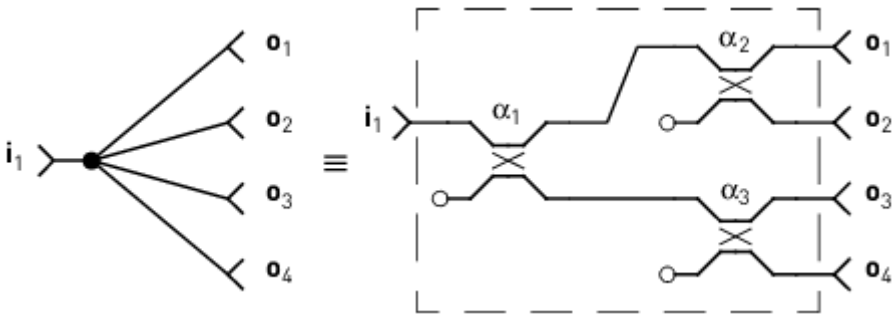


Figure 2-4 : Schematic of beam splitter_1_4 module

2.2 Design of Phase-Encoding BB84 QKD Protocol with Coherent State

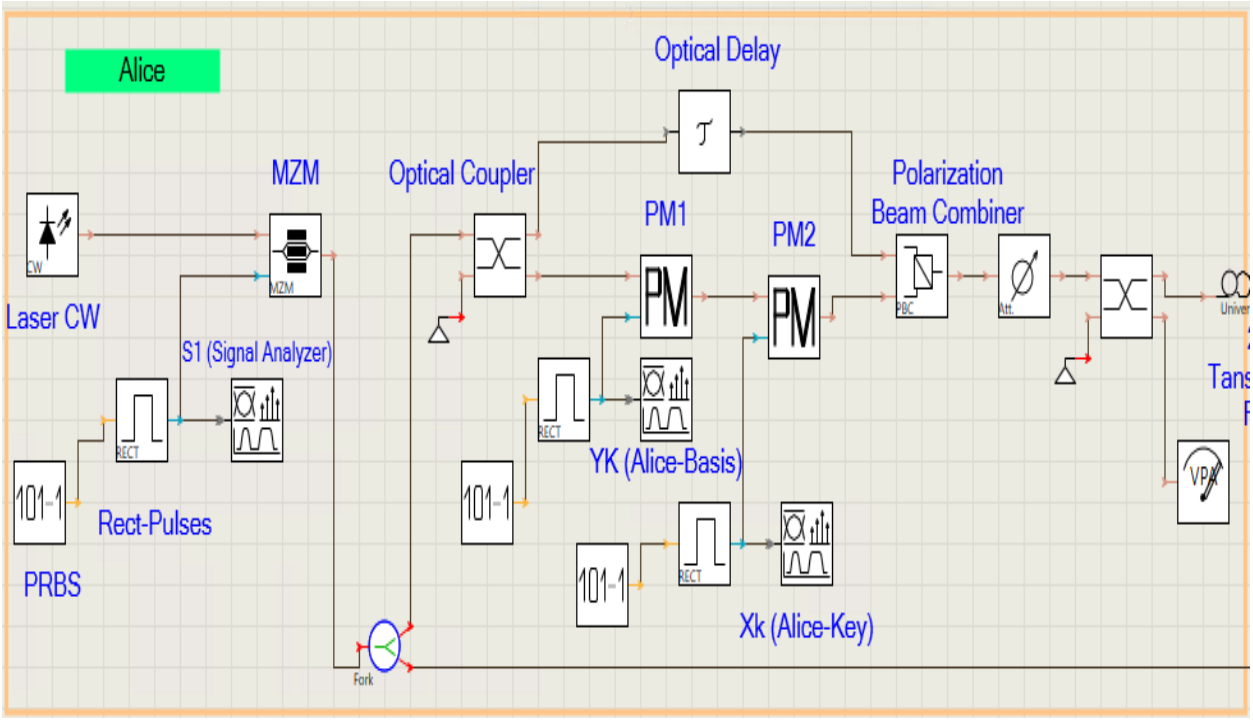


Figure 2-5 : Schematic of Phase-Encoding BB84 QKD protocol _Transmitter (Alice)

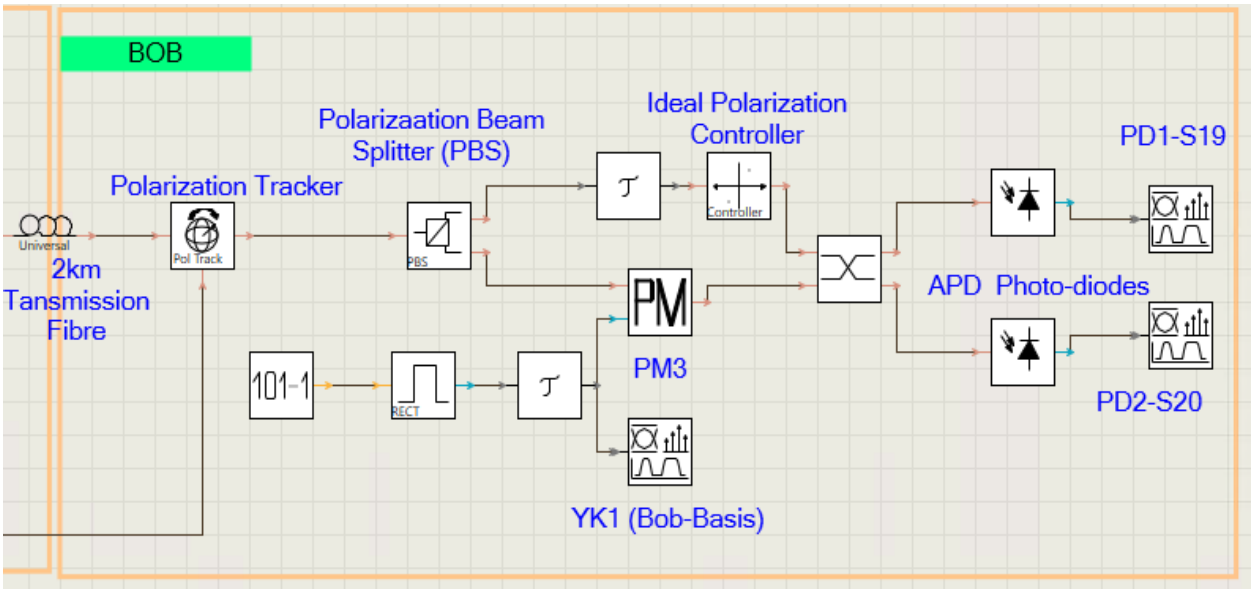


Figure 2-6 : Schematic of Phase-Encoding BB84 QKD protocol _Receiver (Bob)

The classical version of phase-encoded BB84 protocol schematic of transmitter (Alice) and receiver (Bob) is shown in the Figures 2-5 and 2-6 respectively.The parameters of this design is mentioned in ANNEX 1 .For classical system the information is transferred between transmitter and receiver by means of optical pulses [22]. This system using phase encoding technique to share the key. Alice reside key information in phase and share this to Bob.

Coherent source

We create simulated coherent states source for this classical design with the help of laser and Mach-Zehnder Modulator (MZM). Alice side is a transmitter which include light source LED that generate optical signal. Alternate rectangular pulses is generated through PRBS and rectangular module.

These alternate pulses feed into the data input port of MZM that perform amplitude modulation of input optical signal provided by light source and creates optical pulses as shown in Figure 2-7.The pulse is high for 1.34 ns and low for 4.74 ns. The pulse period is 6.6 ns.

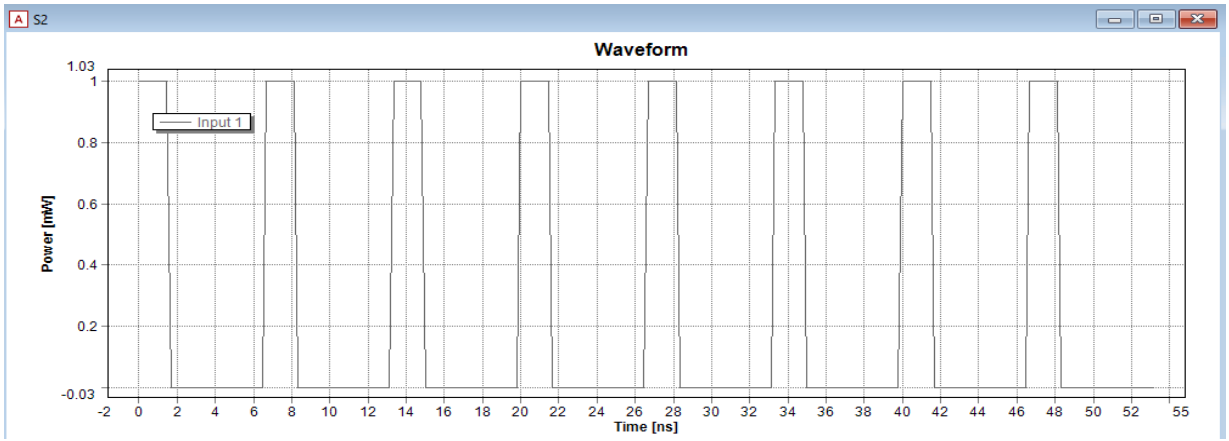


Figure 2-7 : Mach-Zehnder Modulator (MZM) Pulses

Alice Measurements

Mach-Zehnder Interferometer (MZI) is constructed. It has two branches optical delay and two phase modulators. Coupler splits the optical pulses into the two paths feed to the input of MZI.

On Phase modulator branch Alice generate basis and key information, two Phase Modulators PM1 and PM2 are used in this branch. Two different random pulses Xk and Yk are generated with the help of PRBS to define as shown in Figure 2-8. Xk is the key information link to PM1 and Yk determine the basis of the encoding key link to PM2. The duty cycle of these random pulses is 50%.

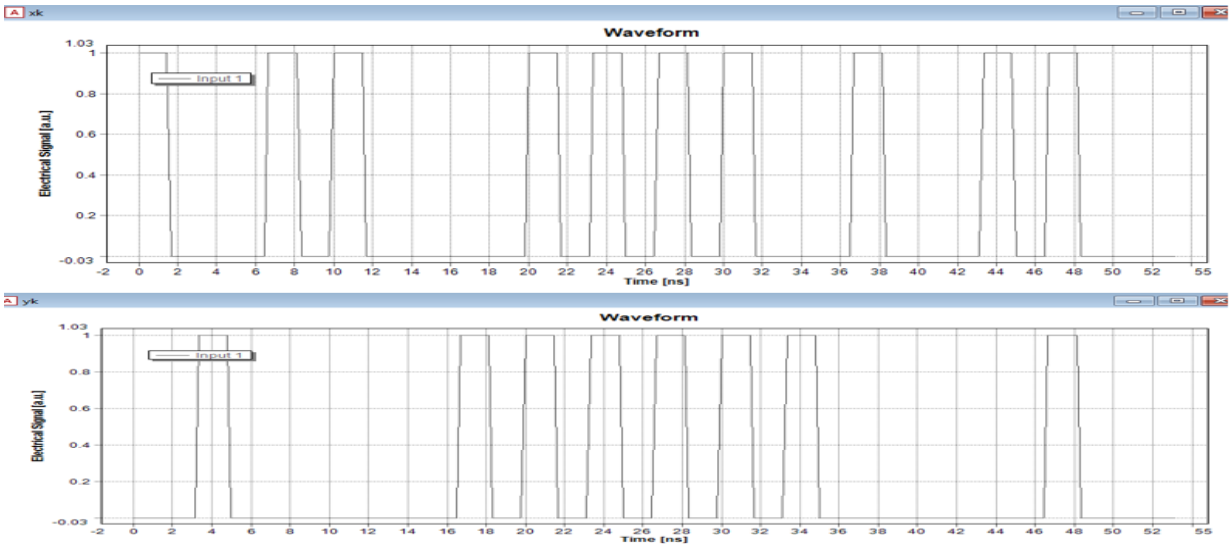


Figure 2-8 : Generation of Random Pulses for Defining Basis to Encode Information

The basis define by the Alice is as follow:

Phase Modulator-1	
0	Basis-1
90	Basis-2

The PM2 is linked with Key Information which has phase shift as follow:

Phase Modulator-2
0
180

Information between Alice and Bob transmits with phase information, the output of two modulation is shown in Figure 2-9, we can observe the variations in phases with respect to time.

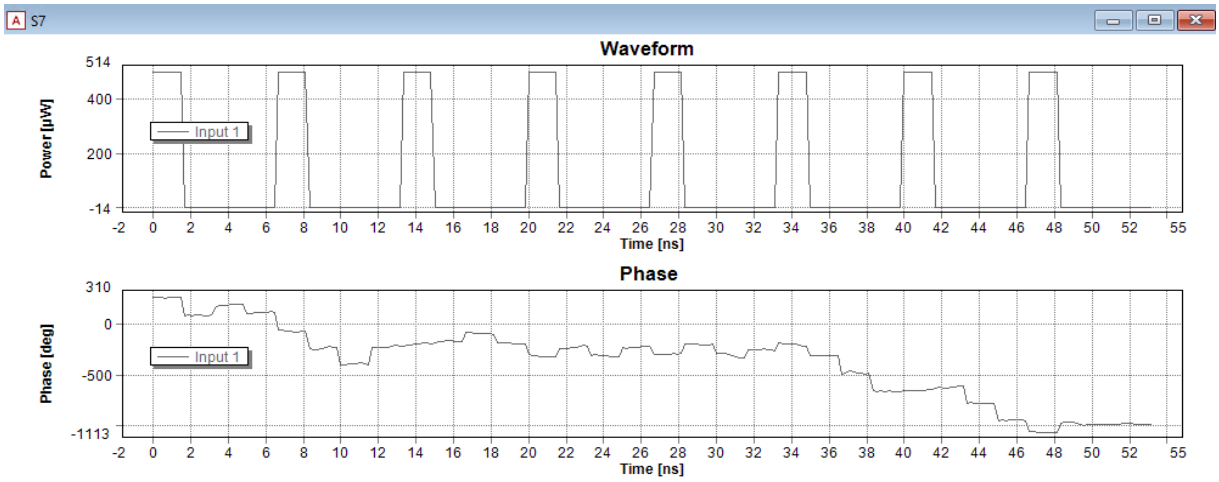


Figure 2-9 : Alice Phase Information

The other branch has optical delay of 2ns. Modulated and un-modulated pulses combine at Polarization Beam Combiner (PBC).

Weak pulses

Attenuator is used to adjust the intensity of the pulses. Coupler further splits the optical signal into two paths in order to reduce the power level then Optical pulses pass through the optical fibre.

Alice Output

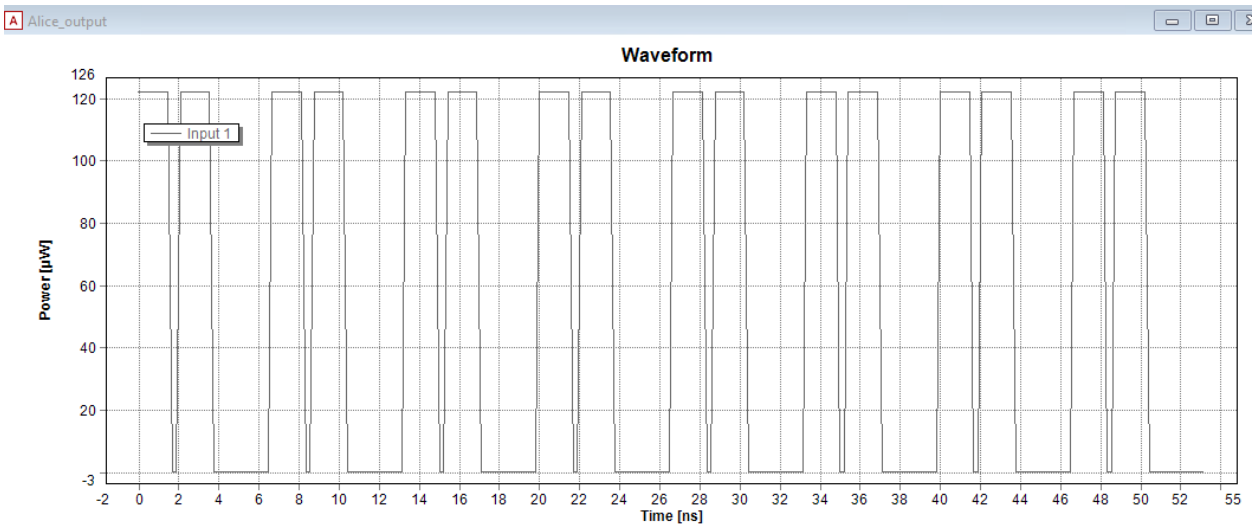


Figure 2-10 : Alice (Transmitter) Output

Calculation of Transmitted Number of Photons

The output of Alice is shown in Figure 2-10.Now let's calculate the number of photons transmitted by the Alice

$$\text{Power} = 122\ \mu\text{W}$$

$$\text{Duration of Pulse} = 1.34\ \text{ns}$$

$$\text{Energy of one pulse} = \text{power} * \text{duration of pulse}$$

$$= 122\mu * 1.34\,n$$

$$\text{Energy of one pulse} = 163.48 \times 10^{-15}\ \text{J}$$

$$\text{Energy of a Photon} = E = hf = \frac{hc}{\lambda}$$

$$h = \text{Planck's Constant} = 6.6 \times 10^{-34}\ \text{J} * \text{S}$$

$$c = \text{Speed of light} = 3 \times 10^{8}\ \text{ms}^{-1}$$

$$\lambda = \text{Photon wavelegth} = 1550\ \text{nm}$$

$$\text{Energy of a Photon} = \frac{6.6 \times 10^{-34} \times 3 \times 10^{8}}{1550 \times 10^{-9}}$$

$$\text{Energy of Photon} = 1.28 \times 10^{-19}\ \text{J}$$

$$\text{Number of photons in one pulse} = \frac{\text{Energy of one pulse}}{\text{Energy of a photon}}$$

$$= \frac{163.48 \times 10^{-15}}{1.28 \times 10^{-19}}$$

$$\text{Number of photons in one pulse} = 1.27 \times 10^{6}$$

So the average number of photons transmitted by Alice is

$$1.27 \times 10^{6} \left(\frac{2 \times 1.34\,\text{ns}}{6.6\text{ns}}\right) = 516 \times 10^{3}$$

We can observed that in classical model we can transmits thousands of photons as compared to actual BB84 QKD protocol where the average number of photons per coherent pulse is less than 1.

In this design we installed dispersion and attenuation free fibre. There is only one factor polarization mode dispersion taken into account.

Bob Measurements

The receiver side Bob shown in Figure 2-6 receive the optical pulses, first these pulses feed into polarization controller that correct the state of polarization of receiving pulses. Polarization Beam Splitter (PBS) splits the polarization state into two paths. Bob also has constructed Mach-Zehnder Interferometer (MZI) having two same branches as Alice side. Alice Modulated signal given to optical delay. The un-modulated optical pulses feed to Bob side Phase Modulator (PM3). Bob generates random pulses through PRBS and define the basis of these random pulses with the help of phase modulator as shown in Figure 2-11.

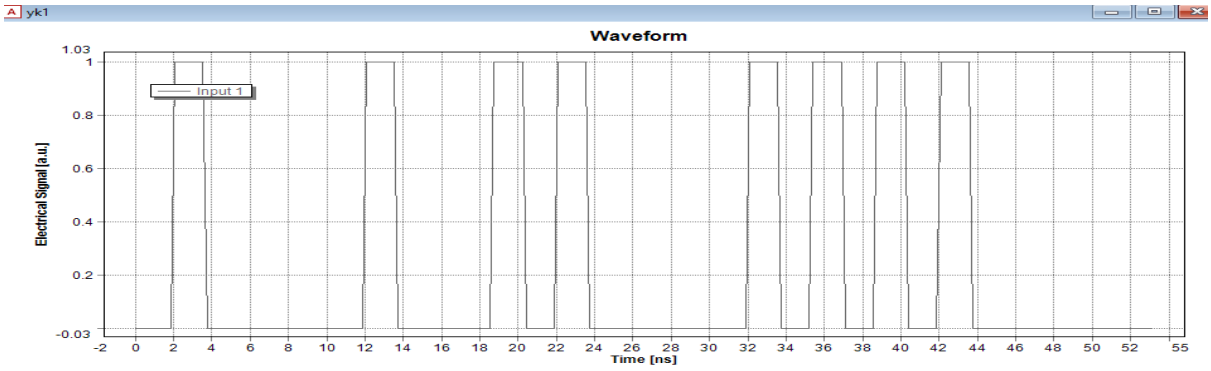


Figure 2-11 : Generation of Random Pulses for Defining Basis to decode Information

Bob decode random pulses in two basis

Phase Modulator-3	
0	Basis-1
90	Basis-2

The output of Bob phase modulator is shown in Figure 2-12. MZI output provide to coupler which splits the optical pulses into two paths and observe the signal at two Avalanche photo diode (APD).

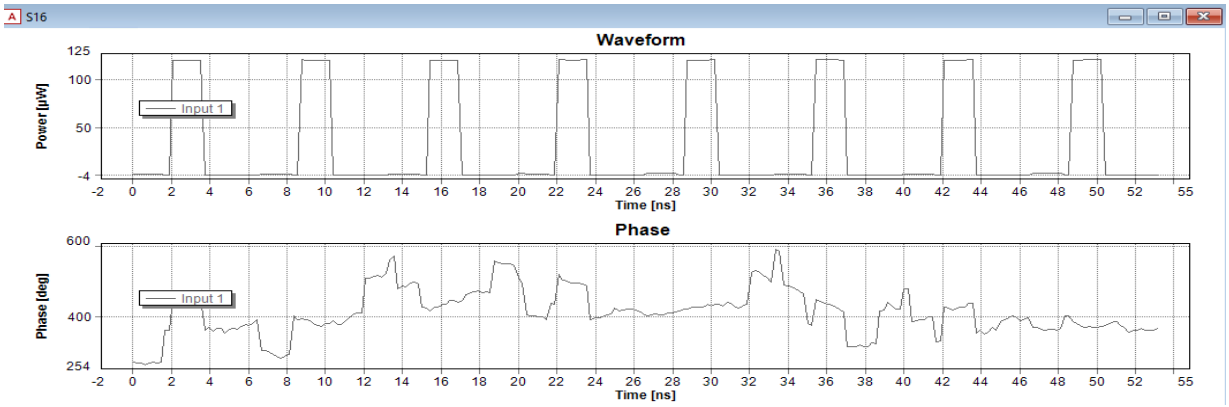


Figure 2-12 : Bob Phase Information

2.3 Principle for Communication between Alice and Bob

Alice and Bob define two basis 0º and 90º. If Alice encode the information in 0º and Bob decode the information using the same 0º then decoded bits are accepted.Similary if Alice encode information in 0º and Bob decode in 90º then decoded bits are rejected. After that Alice and Bob announced their basis information via classical channel.

2.4 Results of Phase-Encoding BB84 QKD Protocol Design

We check the correctness of our design with the help of Table 2-2. We can observed that When the Alice (Phase modulator) PM1 encode optical pulses information in 0º and Bob PM3 decode the information in 0º the decoded bits are accepted and the output of Photo Detectors PD1 and PD2 are 1 and 0 respectively as shown in Figure 2-13. When the Alice PM1 encode the information in 90º and Bob PM3 decode the optical pulses in 0º .Since the basis are different, the decoded bits are rejected and the output of Photo Detectors PD1 and PD2 is 0.5 and 0.5 respectively as shown in Figure 2-14.Similarly we can verify the remaining entries of table by running the classical model of phase-encoded BB84 QkD protocol.

We have set following values of received optical power at photo diode.

1.60 µw	1 (high)
80 µw	0.5 (half)
0	0 (low)

Table 2-2 : Results of Classical Phase-Encoded BB84 QKD Protocol Design

Alice		Bob	PD1	PD2
PM1	PM2	PM3	S19	S20
0	0	0	0	1
0	180	0	1	0
0	0	90	0.5	0.5
0	180	90	0.5	0.5
90	0	0	0.5	0.5
90	0	90	1	0
90	180	90	0	1
90	180	0	0.5	0.5

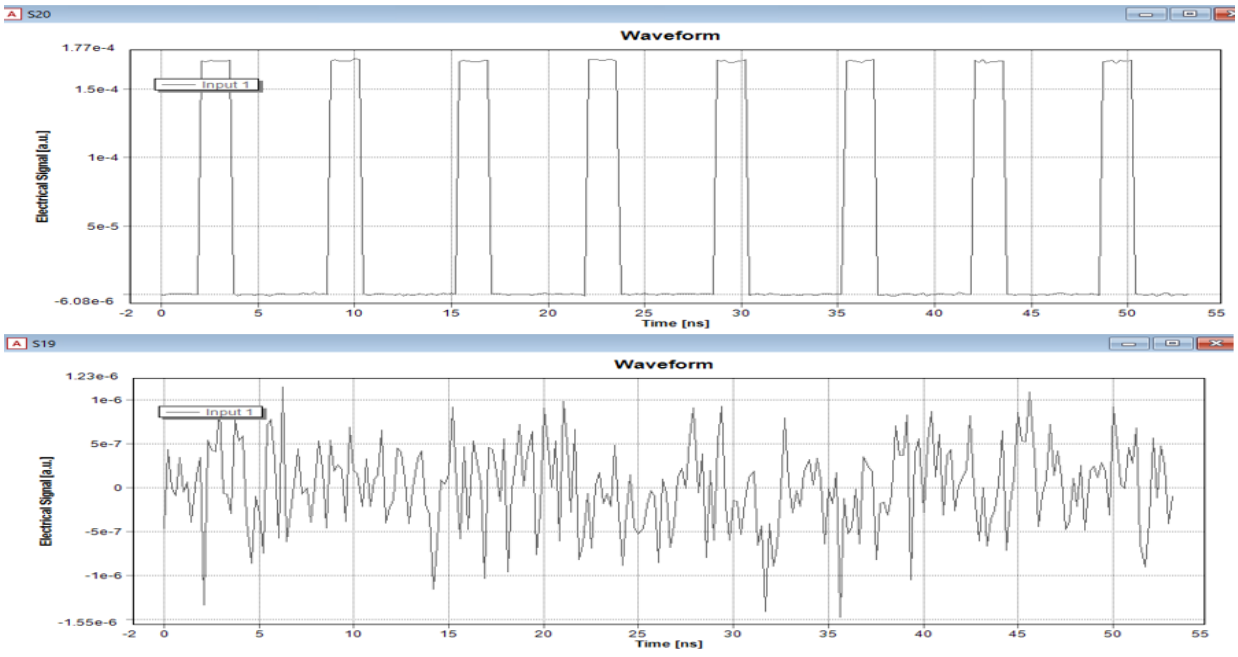


Figure 2-13 : Photo Detectors Output in Case of Communication

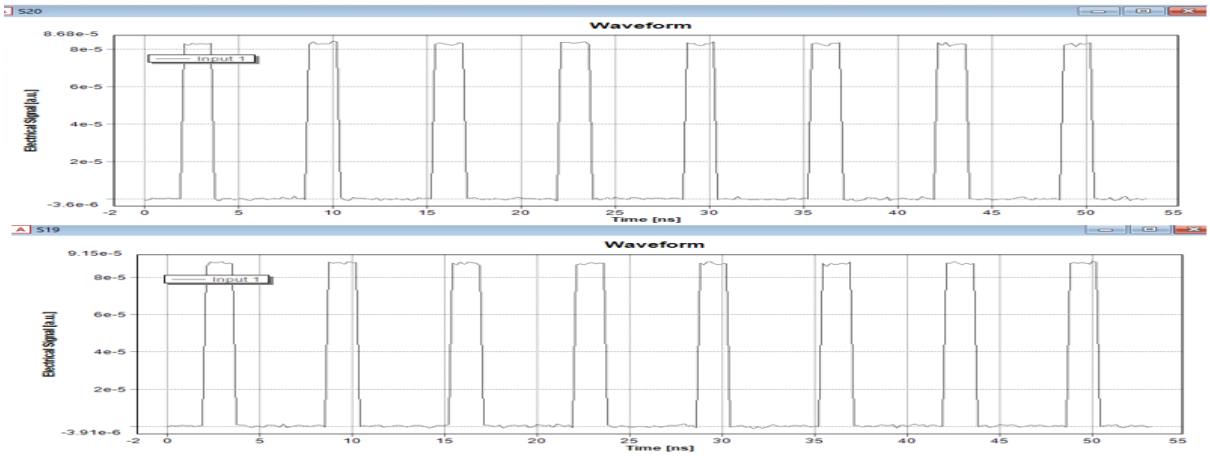


Figure 2-14 : Photo Detectors Output in Case of No Communication

2.5 Key Distillation Process

In order to get key at the receiver we modify the receiver side of Phase-Encoding BB84 QKD model as shown in the Figure 2-15. The output S19 and S20 are gated with rectangular pulses S23.The gated pulses shown in Figure 2-16. These pulses help to identify the meaningful information.New outputs of our model is now S21 and S22.

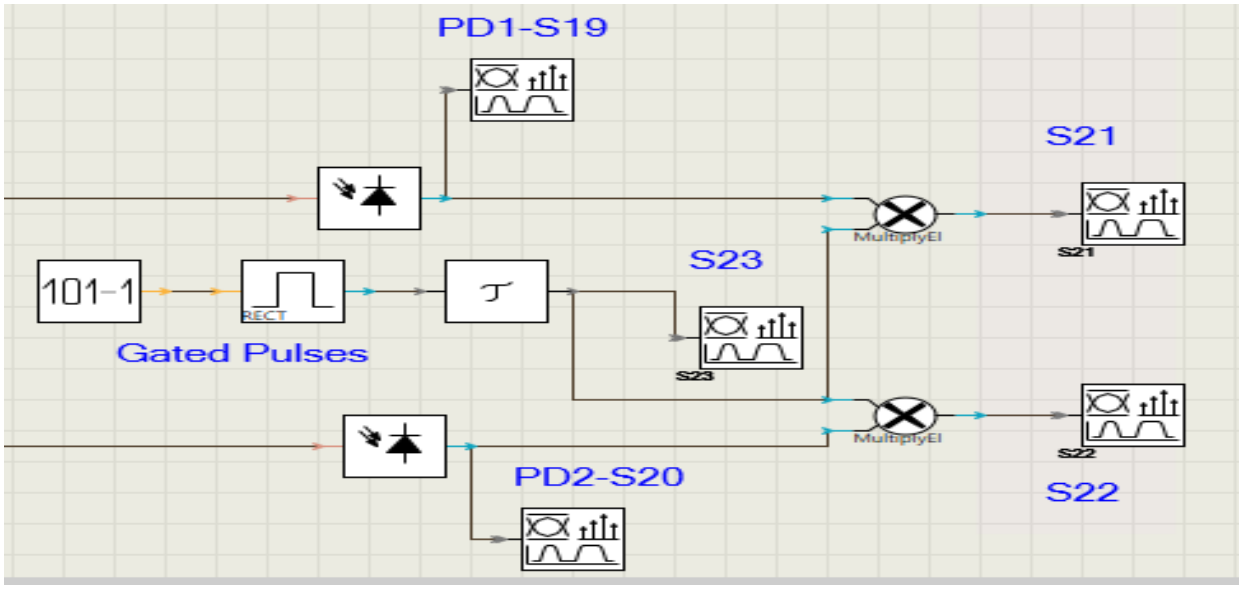


Figure 2-15 : Modification of Bob Side for Key distillation

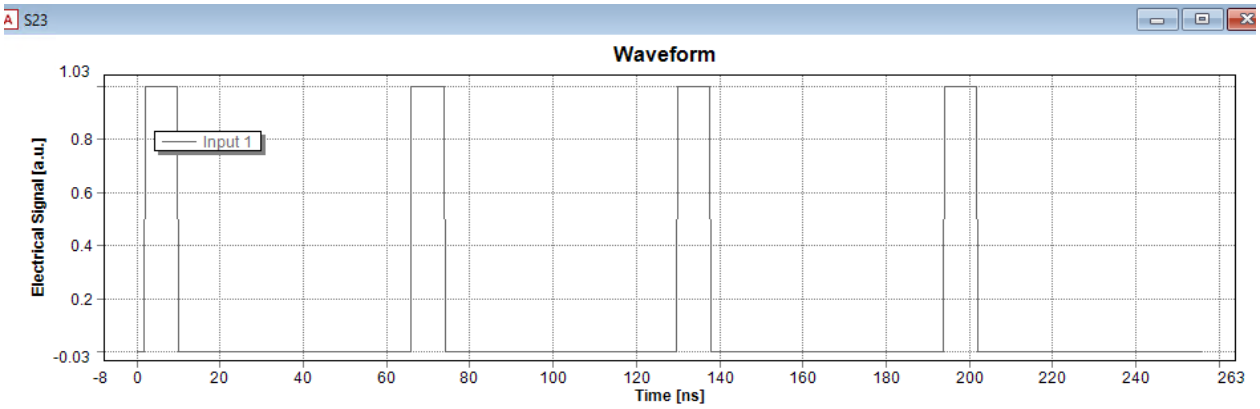


Figure 2-16 : Gated Pulses to Identify Key Information

Optical Pulses for key distillation

Alice generate two random pulses Xk and Yk . Xk is the key information and Yk determine the basis of encoding key. The output of these pulses shown in Figure 2-17. In this analysis the number of samples is 64.

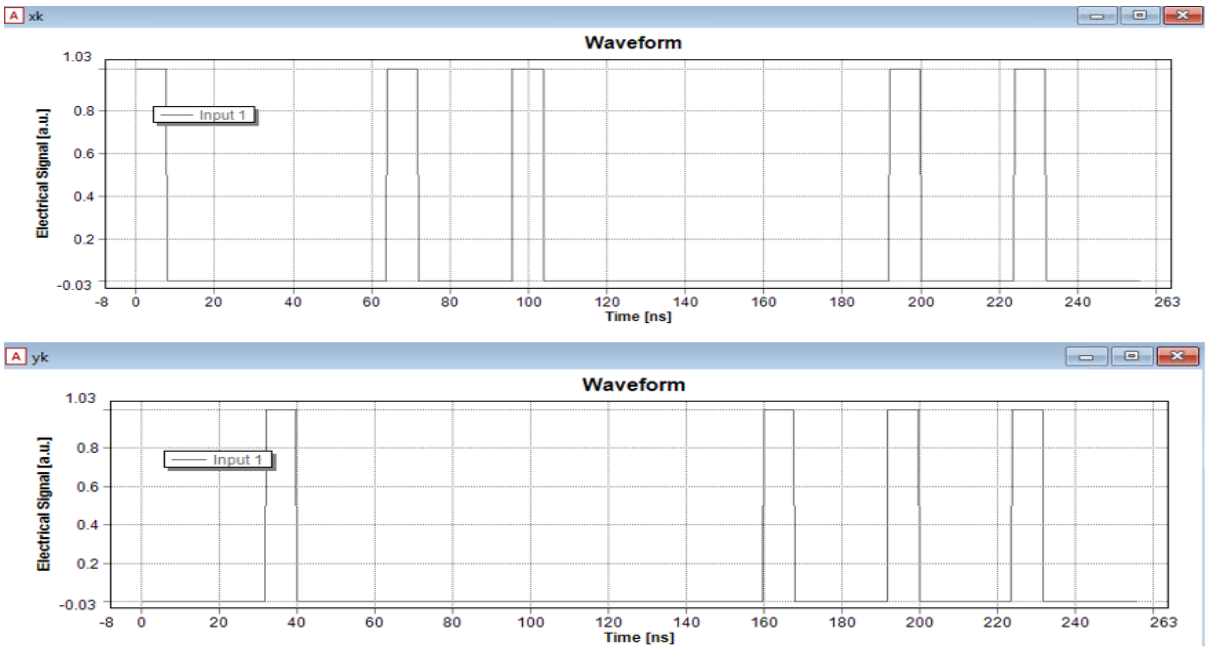


Figure 2-17 : Alice Key Information and Encoding basis for 64 Samples

Bob generate random pulses to define decoding basis using PRBS Yk1 as shown in Figure 2-18.

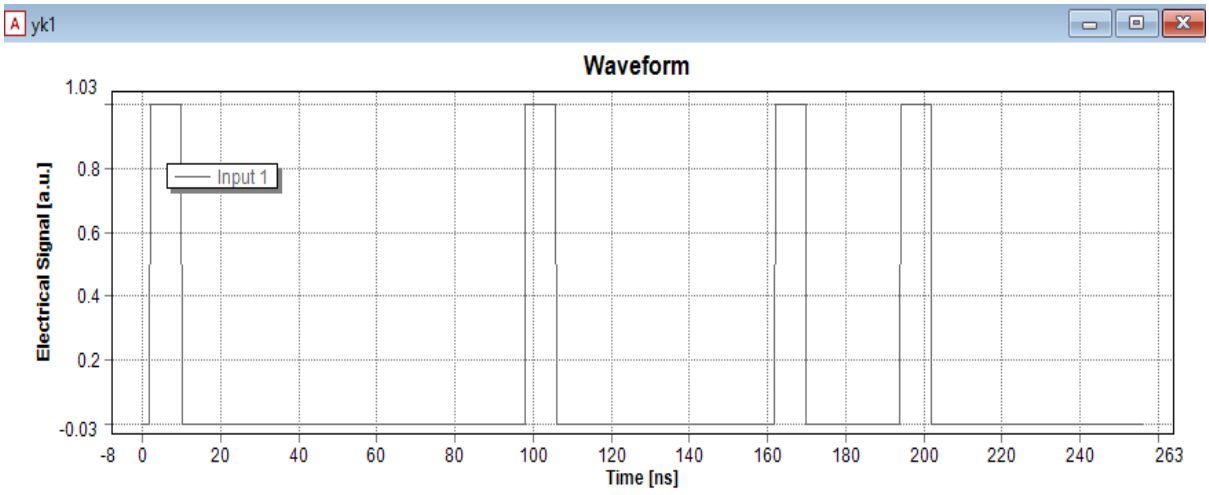


Figure 2-18 : Bob decoding basis for 64 samples

The output of Photo Detectors PD1 and PD2 after gated pulses are shown in Figure 2-19.These outputs are represented by S21 and S22 respectively. We can observed that when the output power of pulses is high around 1.6µW we consider this as 1. When it is 80µW we assume half of power 0.5 and similarly 0 for low.

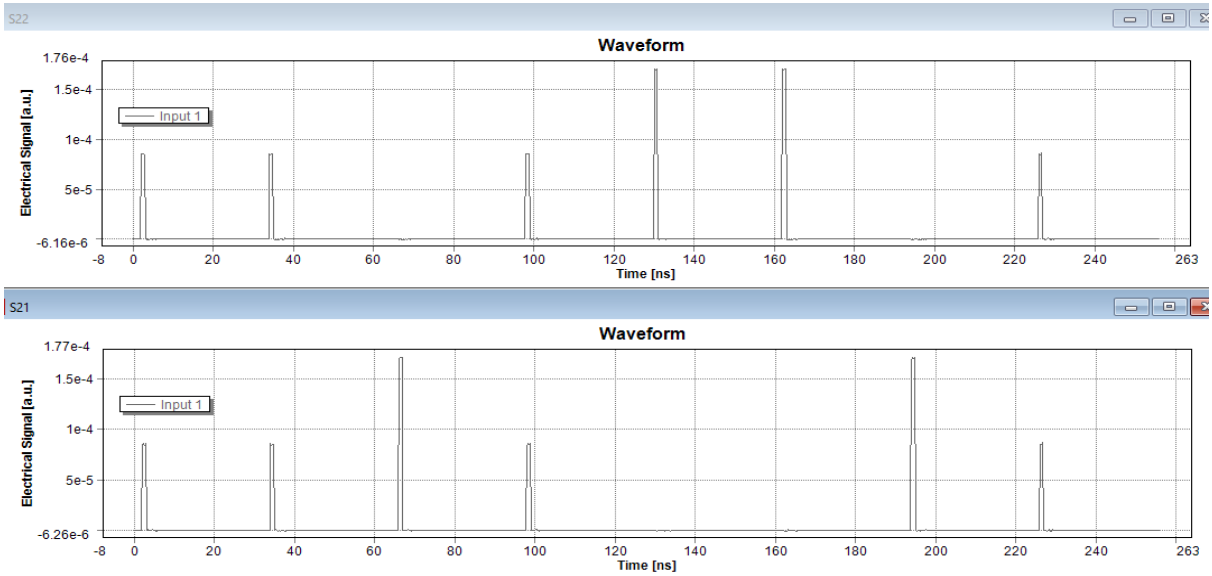


Figure 2-19 : Photo Detector output after gated pulses for 64 samples

For the key distillation we make excel sheet for entries Xk, Yk, Yk1, S21 and S22. We only consider meaningful entries and finally make a table for the key at the receiver side (Bob).

Table 2-3 : Key distillation

Key (Xk)	1	0	1	1	0	0	1	1
Alice Basis (YK)	0	1	0	0	0	1	1	1
Bob Basis (YK1)	1	0	0	1	0	1	1	0
PD-1 Output (S21)	0.5	0.5	1	0.5	0	0	1	0.5
PD-2 Output (S22)	0.5	0.5	0	0.5	1	1	0	0.5

The key distillation is shown in Table 2-3. We can observed that when Alice basis is different from Bob basis the output of Photo Detectors is (0.5,0.5) ,This means no communication take place and we reject this key information.We only accept those key inofrmation where Alice and Bob have same basis. We can conclude that

Shared Key is 1001

In another analysis we increase number of samples to 512 in order to generate long key. We performed same steps as mentioned when number of sample is 64. The following key has been generated.

1001101000011111001010100111010101110 0

2.6 Randomness Test for Key

To check the randomness of key we perform run test also known as Wald-Wolfowitz test [23]. This test check the randomness of given sample.

confidence level 100 (1- α) %.

Key is 10011010000111110010101001110101011100

Number of 1's = n1 = 20

Number of 0's = n2 = 18

Number of Runs =R =22

Following steps have taken for the test

1. Calculate the sample mean
2. If the sample sequence is above the mean the replace with + and if it is below then replace with - .If it is equal with the mean value then discard it.
3. Calculate n1, n2 and R.
4. Calculate expected mean and variance of R

$$\alpha = 1 + 2n_1n_2/(n_1 + n_2)$$

$$\sigma^2 = 2n_1n_2(2n_1n_2 - n_1 - n_2)/[(n_1 + n_2)^2(n_1 + n_2 - 1)]$$

5. Calculate z

$$z = (R - \mu)/\sigma$$

6. If $z > Z_\alpha$ then behaviour is under-mixing

   If $z < -Z_\alpha$ there might be a trend

   If $z < -Z_{\alpha/2}$ or $z > Z_{\alpha/2}$ reject the randomness.

This test is valid if the number of given sample is greater than 10.There is online JavaScript to check randomness by putting the bit sequence [24].

2.7 Randomness Result

The results shows that key generated at the Bob side of phase-encoded BB84 QKD protocol is random.

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

CALCULATE CLEAR

Number of Runs (R) 22

P-value 0.24918

Conclusion

Little or no real evidences against randomness

Figure 2-20 : Key Randomness result

2.8 Summary

In this chapter we discussed classical version of phase encoded BB84 protocol with coherent state.The Quantum Key Distribution (QKD) protocol module existing in VPI-Photonics Software is very expensive. We proposed cost effective classical model and proof its effectiveness by means of successful communication between transmitter and receiver. I first describe the main components of VPI-Photonics software used in the simulation of phase-encoded BB84 QKD protocol. In the next section explanation we proposed the classical design and results. In the last section of this chapter we describes the procedure for obtaining the key at receiver side (Bob) and verify the randomness of key.

3. The Protocol in Realistic Condition (Real Fibre)

The Proposed classical phased-encoding QKD protocol model will be tested in realistic condition. The realistic condition means considering optical fibre with dispersion, attenuation etc. and observe the behaviour of proposed design.

3.1 10000-km Dispersion and Attenuation Free Optical Fibre

In this test case we used optical fibre of length 10000km with no dispersion and attenuation. The only parameter considered is polarization mode dispersion (PMD). The main objective of performing this test is to check whether the communication between Alice and Bob take place in long distance fibre. We set the hypothesis if Bob successfully retrieve the key then communication is successful. To prove this hypothesis we performed key distillation at Bob (receiver) side as shown in Table 3-1.

Table 3-1 : Key Distillation of 10000-km Dispersion Free Optical Fibre

Key (Xk)	1	0	1	1	0	0	1	1
Alice Basis (Yk)	0	1	0	0	0	1	1	1
Bob Basis (Yk1)	1	0	0	1	0	1	1	0
PD1	0.5	0.5	1	0.5	0	0	1	0.5
PD2	0.5	0.5	0	0.5	1	1	0	0.5
	✗	✗		✗				✗

Shared Key 1001

We can observed that for a long distance optical fibre the receiver is able to retrieve the key successfully. So we can conclude that our classical phased-encoding QKD protocol model able to obtain the key information when optical fibre have no dispersion and attenuation even in very long fibre. The important results we noticed in this analysis, polarization mode dispersion is successfully corrected with the polarization controller module.

3.2 1-km Real Optical Fibre

In this analysis the real fibre is used. The setting of fibre parameters are shown in Figure 3-1.The Number of samples is 64.

Physical	
NumberOfFiberSpans	1
Length	1e3
GroupRefractiveIndex	1.47
AttenuationDescription	AttenuationParameter
Attenuation	0.2e-3
ReferenceFrequency	193.1e12
DispersionDescription	DispersionParameters
Dispersion	16e-6
DispersionSlope	0.08e3
PMDCoefficient	0.1e-12/31.62
CorrelationLength	50.0

Figure 3-1 : Real Fibre Parameters

In order to see the behaviour of our classical design in realistic condition we performed key distillation .Alice generate random pulses Xk (key information) and Yk (basis for encoding key information) and similarly Bob generate Yk1 (basis for decoding key Information) as shown in Figure 3-2.

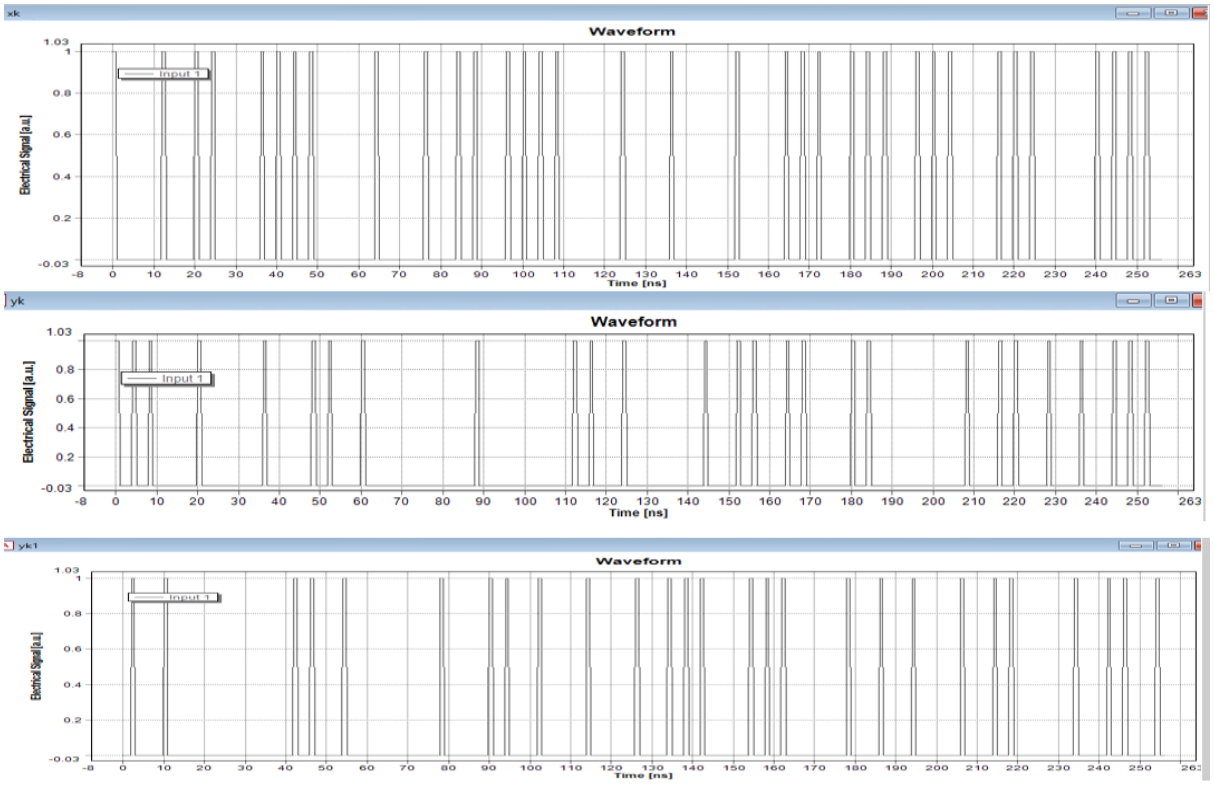


Figure 3-2 : Random Pulses generated by Alice & Bob

The corresponding output of Photo Detectors PD1 and PD2 in respond to these pulses are shown in Figure 3-3.

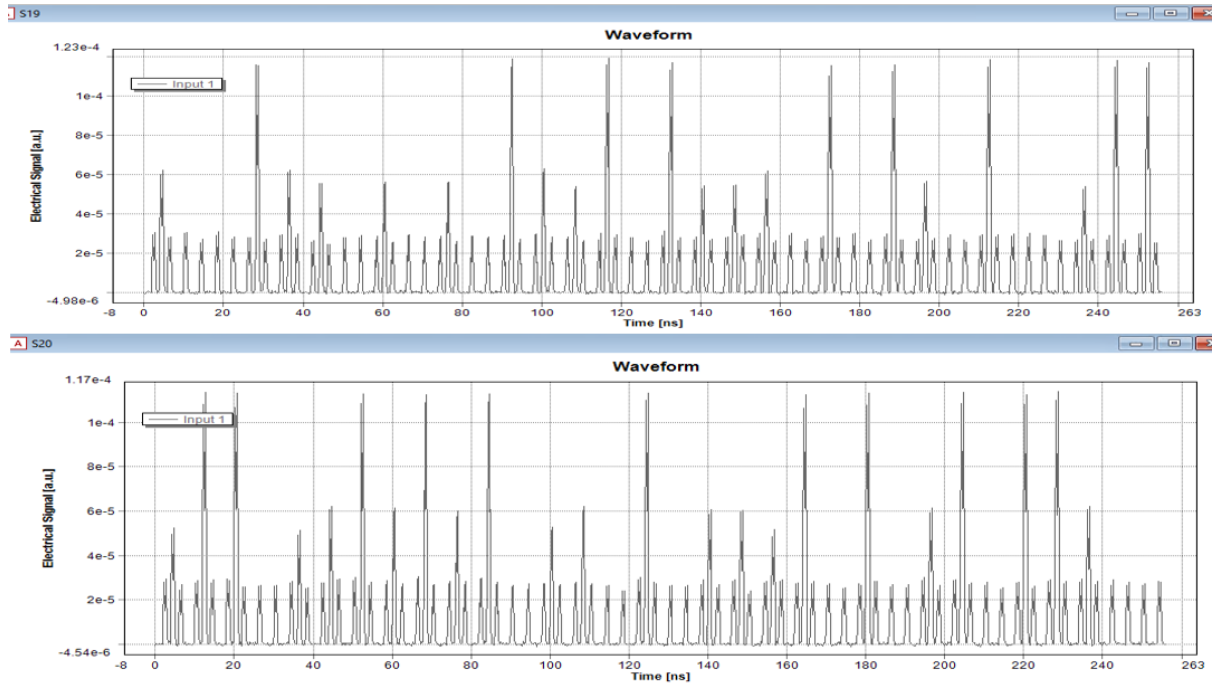


Figure 3-3 : Photo-Detectors Output for 1-km real fibre

The statistical analysis has been performed at the receiver side in order to obtain the Alice key information as shown in Table 3-2.

Table 3-2 : Key distillation of 1-km Real Fibre number of samples 64

Key Information (Xk)	0	1	0	0	0	1	1	0
Alice Basis (Yk)	1	1	1	0	1	0	0	1
Bob Basis (Yk1)	0	0	0	0	0	0	0	0
PD1- (S19)	0.5	0.5	0.5	0	0.5	1	1	0.5
PD2 – (S20)	0.5	0.5	0.5	1	0.5	0	0	0.5
	✘	✘	✘		✘			✘

Shared Key 011

We can observed from that out of 8 bits 5 are rejected and only 3 bits results in shared key. As per BB84 protocol 50% of information will be lost but in this analysis more than 50% key information has been lost because the key sequence is too short for statistical analysis. In order to verify our observation we generate long key with number of samples 256 .After performing key distillation process we obtain following key

Shared Key 1110101100000

We generated 48 bits, 35 are rejected and only 13 bits results in shared Key. So we can conclude that the classical design of BB84 QKD protocol when tested in realistic condition**, more than 50% of information has been lost**.

3.3 20-km Real Optical Fibre

In this analysis we increase the optical fibre length up to 20 km. We used the same random pulses for as input as shown in Figure 3-2.The output of Photo Detectors PD1 and PD2 are shown in Figure 3-4.

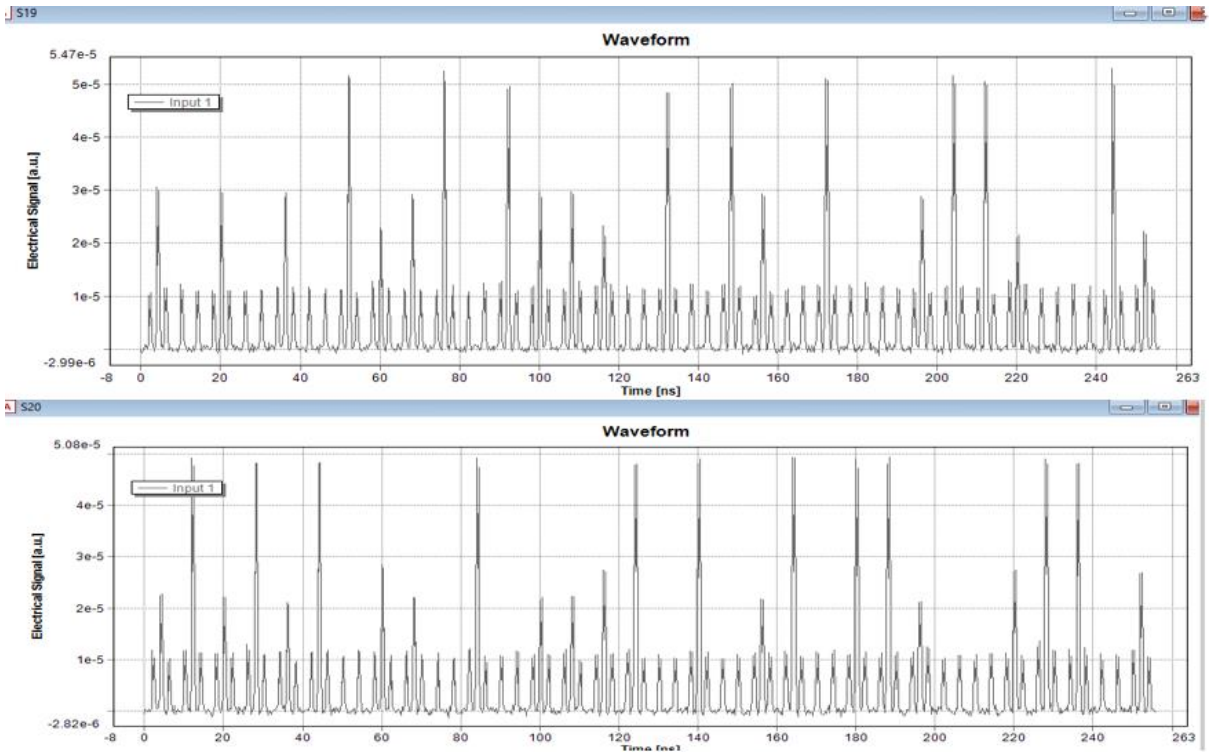


Figure 3-4 : Photo-Detectors Output for 20-km real fibre

After performing the key distillation process we obtained following key as shown in Table 3-3.

Table 3-3 : Key distillation of 20-km Real Fibre number of samples 64

Xk	0	1	0	1	0	1	0	0	0	1	1	1	1
Yk	1	1	0	1	1	0	1	0	1	0	0	1	1
Yk1	0	0	0	0	0	0	0	0	0	0	0	0	0
PD-1	0.5	0.5	0	0.5	0.5	1	0.5	0	0.5	1	1	0.5	0.5
PD-1	0.5	0.5	1	0.5	0.5	0	0.5	1	0.5	0	0	0.5	0.5
	✖	✖		✖	✖		✖		✖			✖	✖

In this analysis we retrieve 13 bits key, 8 are rejected and only 5 results in shared key. Finally we can conclude that when classical design tested in real fibre with dispersion and attenuation, more information will be lost. The reason is synchronization or key sequence is too short.

3.4 Dispersion Compensation Techniques

Since when we tested our Classical design of BB84 QKD protocol in realistic condition, the main limitation is to obtain key information at the receiver to the desired level. In order to reduce dispersion factor several compensation techniques were proposed in the literature including DCF (Dispersion Compensating Fibre), FBG (Fibre Bragg Gratings) and HOM (High Order Mode) Fibre.

3.4.1 Dispersion Compensating Fibre

DCF techniques has been considered one of the suitable method for dispersion compensation. DCF is not affected by the wide bandwidth and temperature. Single Mode Optical Fibre (SMF) has positive second and third order dispersion value. On the other hand dispersion value in DCF is negative. By adding DCF the average value of dispersion is close to zero [25]. DCF negative dispersion value is range between -70 to -90 ps/nm.km. There are three DCF strategies has been proposed including pre-compensation, post-compensation and mix-compensation. In pre-compensation technique the DCF is place before the SMF. In post-compensation the DCF is place after the conventional single mode fibre. In mix-compensation both post and pre-compensation is comprised. [26] The disadvantage of this method is it can insert high insertion losses and also increase the impact of nonlinear effects.

3.4.2 Fibre Bragg Gratings

The problems of high insertion loss and nonlinear effects can be reduced by utilizing Fibre-based Bragg Gratings for dispersion compensation. In this technique, the refractive index changes in periodic manner inside the core along the grating length. Due to this behaviour Fibre Bragg Gratings act as optical filter. This form the stop band in the spectral region where most of incident light is reflected back. The stop band is centred at the Bragg wavelength. The periodic behaviour of refractive index couples the backward and forward propagation at Bragg wavelength. This yield a frequency dependent reflectivity over a bandwidth determined by grating strength to the incident signal. This fibre grating act as reflection filter. There is another technique in extension to this method is chirped fibre grating [27]. This method has wider stop band and consider more suitable for dispersion compensation. Chirped fibre gratings also work as a reflective filter. The major drawbacks are the bandwidth of this filter is very small and the transfer function shows a single peak.

3.4.3 Fibre Bragg Gratings

HOM is another technique used for dispersion compensation [28]. This technique offer very large negative dispersion value in very shorter length of DCF. This shorter length helps to reduce the insertion loss and nonlinear effects.

3.5 Summary

This chapter describes the different experiment conducted for the testing of phase-encoding BB84 QKD protocol classical design in realistic condition. First analysis is 10000-km dispersion and attenuation free optical fibre. It shows that when there is no dispersion in fibre, the key can be obtained easily even in very long fibre. Another analysis is for 1-km and 20-km real fibre with dispersion and attenuation. The results show that key distillation is still possible but more information will be lost.

4. Eavesdropping Analysis

When the two legitimate users communicate with each other through public channel then illegtimate user may try to intercept the communication without showing his presence to legitimate users .This technique is called Eavesdropping. For example if Alice (transmitter) want to send inforamtion to Bob(reciever) then there is third person (Eva) who is using different techniques to steal the information.

4.1 Types of Eavesdropping

We have mentioned some eavesdropping types [29] aims to break the security of phase encoding BB84 QKD protocol.

4.1.1 Beam Splitting Attack

One of the basic and simplest technique to decode the information by Eavesdropper is beam splitting attack.In this method Eve tries to decode information by intercept the transmitter signal. In quantum cryptography ,this technique is not efficient because In QKD protocol the photons tranmitted by Alice will not reach to Bob and no security key generated from both the transciever.In case of strongly attenuated laser light, there is chance Eve can leak small information but this problem can be eliminated by using privacy amplification technique.

4.1.2 Intercept Resend Attack

Another technique in which Eve can intercept the Information tranmistted between Alice and Bob is Intercept resend attack.In this attack when Alice sends information to Bob through public channel Eve measure the state and resend fake state to Bob.This is very difficult because Alice encode the information based on four states. As a result Eve is unable to send exact copy of Alice signal to Bob. The reciever Bob creates the key from Eva signal and this key will not match with the Alice key bits.In this way both legitmate users Alice and Bob know that there is eavesdropper trying to decode the information.There is very less probability Eve can send the same signal to Bob as Alice but if some bits matches then we can consider this eavesdropper attack.To eliminate this attack we can set BER (Bit Error Rate) threshold. If BER incereases from certain threshold we can know the eavesdropper attack.

4.1.3 Photon Number Splitting (PNS) Attack

When the Alice transmits signal consisting of two photons,Eve extract one photon and keep it save and let another photon pass through loss less transmission.In this case Bob unaware from the presence of Eavesdropper and Both Alice and Bob share the phase information.Eva silencely listen this information and able to decode the secret key.This attack is unrealistic because for this case Eva have to perform quantum nondemolition (QND) in order to split the photon from the transmitted signal and also need to install loss less fiber [30].As a security anlysis we have to considere all the cases because Eva can do anything unless its contradict the law of physics.This PNS attack limit the transmission distance.In case of long distance tranmission the Bob probability to receive exact number of photons is very less because of large transmission lossed.This type of attack can be eliminated by using single photon source which can only emits only one photon.

4.2 Eavesdropping of Phase-Encoding BB84 QKD Protocol Design

In this section we will discuss the eavesdropping attack on our Phase-Encoding QKD Protocol design. We split this into two section, in first section we describes the strategy used by the Eva and two legitimate users are unaware of his presence. In the next section we will show how eavesdropper steal the key information.

4.2.1 Eavesdropping Strategy

There is no modification in our transmitter and receiver design. The only difference is that Eva use the beam splitter between optical fibres in order to intercept the communication as shown in Figure 4-1.

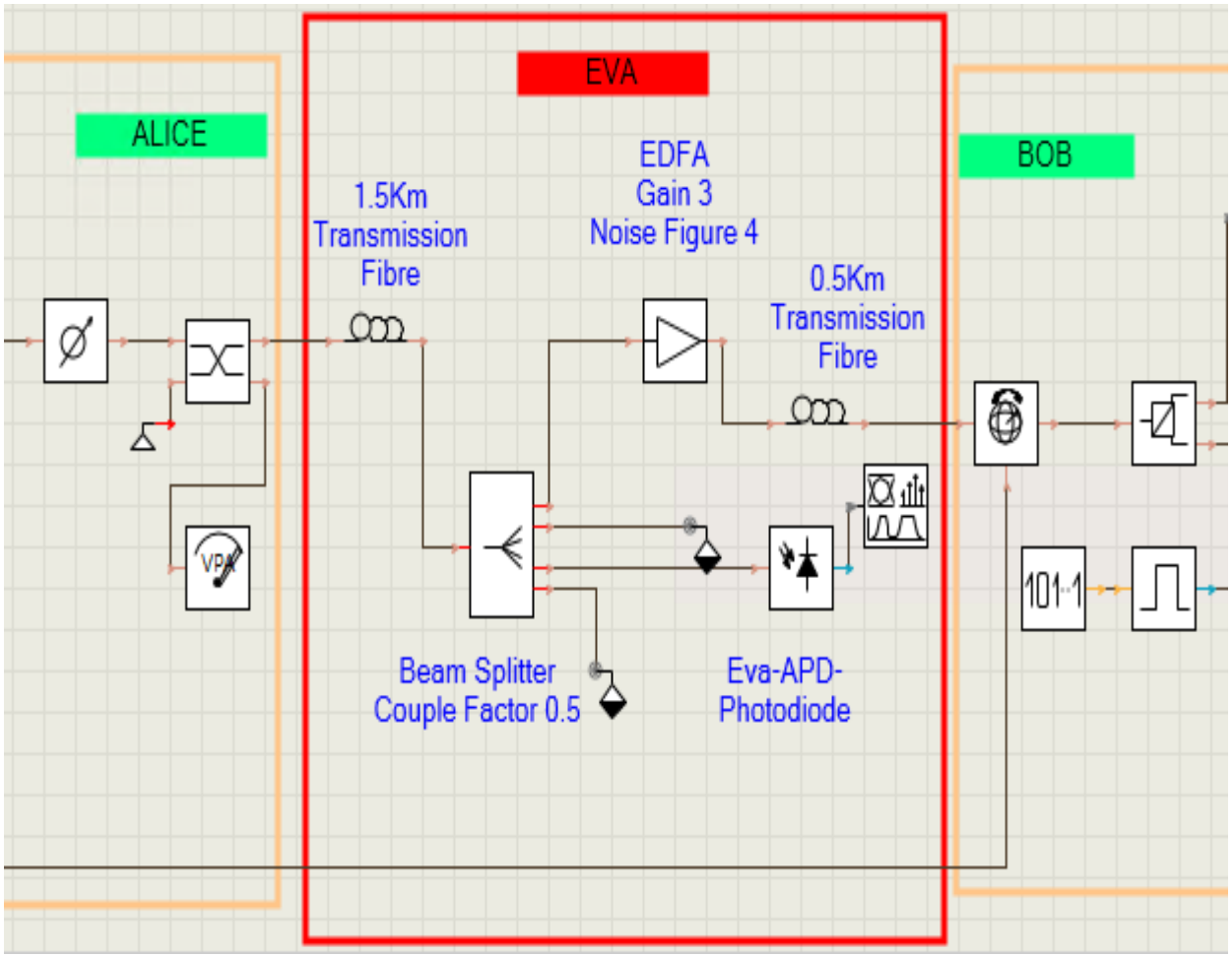


Figure 4-1 : Schematic of Eavesdropping Analysis

Eva used 0.5 coupling factor beam splitter to take half of the power of optical pulses. After that Eva placed EDFA amplifier with gain 3dB in order to amplify the power of optical pulses. In this case Bob will receive the same power as before and unaware of the presence of Eavesdropper.

When there is no eavesdropper the output power of optical pulses received by the Bob is around 1.40 µW as shown in Figure 4-2.

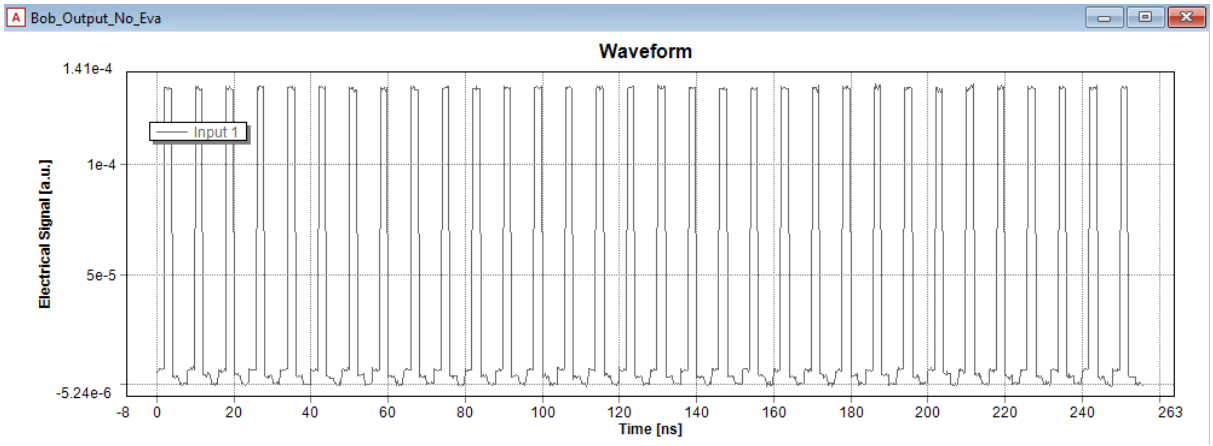


Figure 4-2 : Bob Output with No Eavesdropper

When there is eavesdropper the Bob optical pulses power is same around 1.40µW as shown in Figure 4-3. So the receiver Bob cannot distinguish between output optical pulses and **unaware from the presence of eavesdropper**.

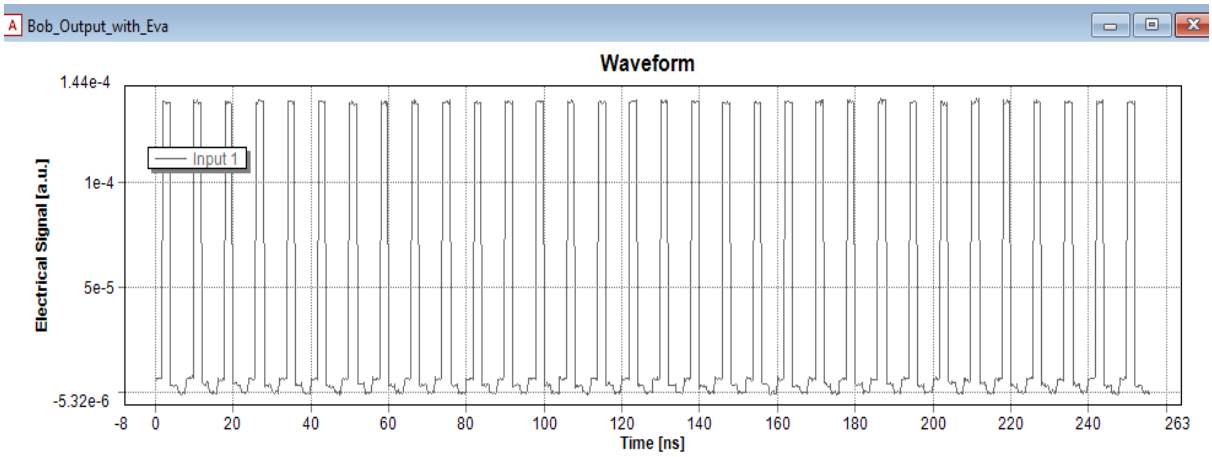


Figure 4-3 : Bob Output with Eavesdropper

Eavesdropper used EDFA amplifier to increase the output of stealing optical pulses as shown in Figure 4-4. Eva can increase up to Bob level so that he can perform key distillation and after obtaining the key, decode the Alice information. This optical amplification cannot be applied to the actual QKD transmission!

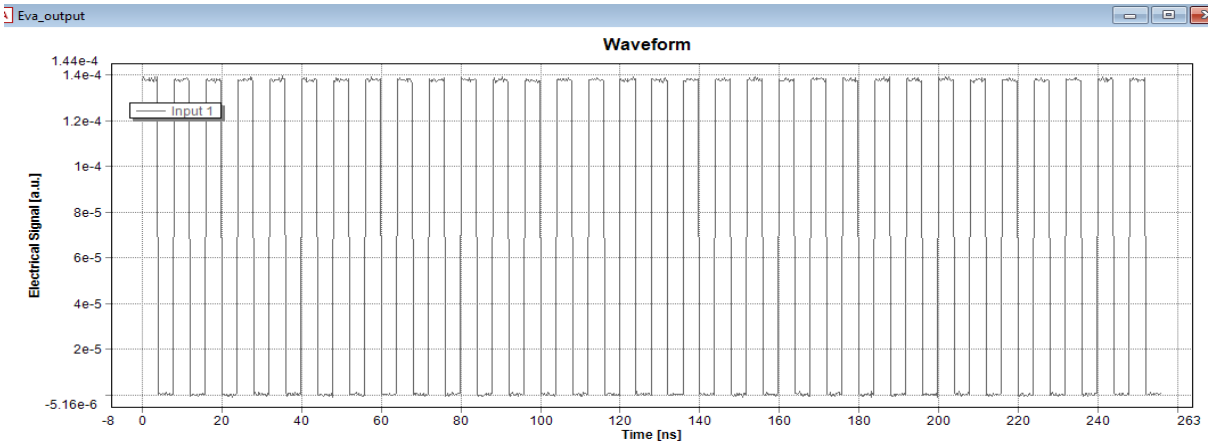


Figure 4-4 : Eavesdropper Output

4.2.2 Eavesdropping Key Stealing

In the previous section we observed that both Alice and Bob are unaware from the presence of Eva. In this section we describe how Eva steal the Key and decode the information. For the key stealing we used copy of Bob as shown in Figure 4-5.

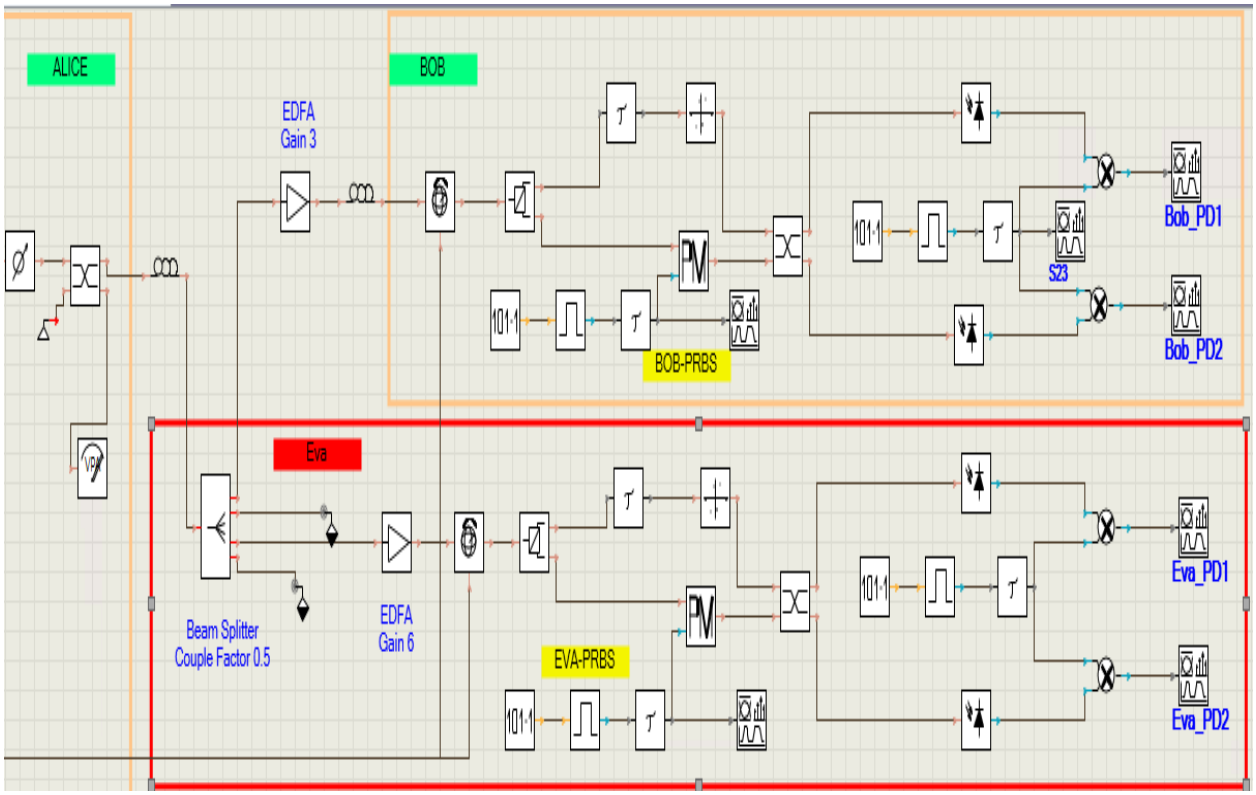


Figure 4-5 : Schematic of Eavesdropping Key Stealing

In this process the Eva does not have the knowledge of Bob basis. Bob randomly generate optical pulses as shown in Figure 4-6. These pulses woks as a basis in QKD protocol. If the Bob basis match with Alice basis, he keep this bit and reject which does not match. In this way Bob successfully retrieve the key and decode the Alice information.

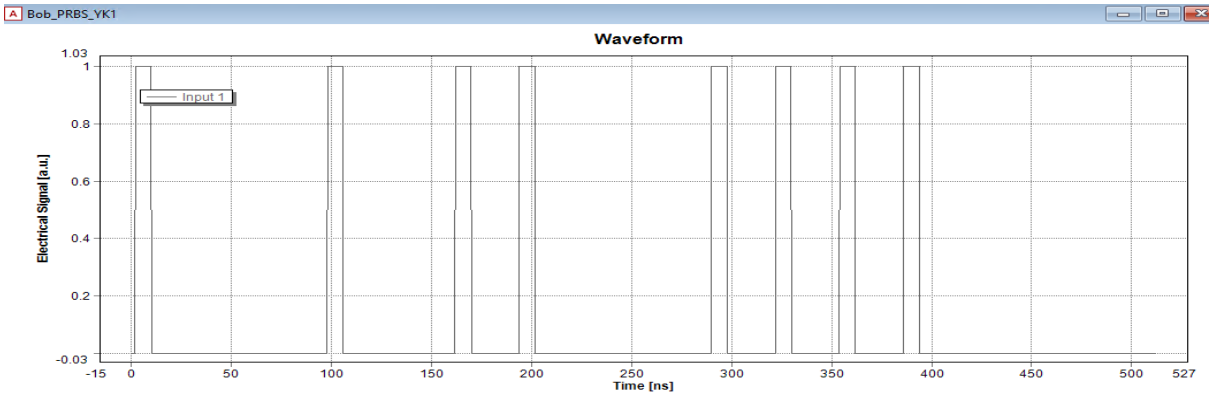


Figure 4-6 : Bob random pulses to define basis

In order to retrieve the key information Eva will also generate random optical pulses as shown in Figure 4-7. We can observed that Eva has almost 50% same basis as Bob

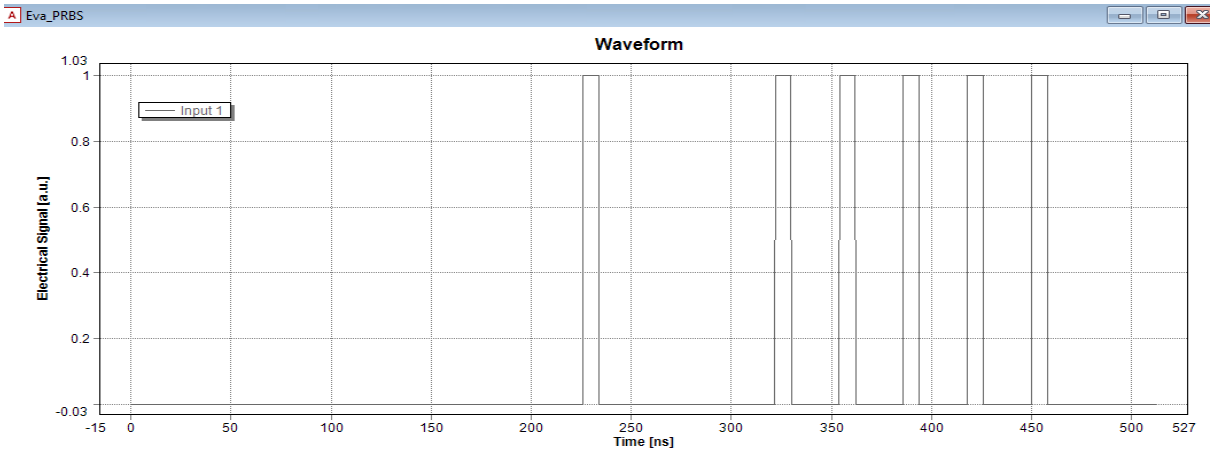


Figure 4-7 : Eavesdropper random pulses to define basis

We performed the key distillation process (mentioned in chapter 2) and retrieve the key information for both Bob and Eva as shown in Table 4-1 and 4-2.

Table 4-1 : Bob Key with Eavesdropper

Xk	1	0	1	1	0	0	1	1	1	1	0	1	0	1	1	0
Yk	0	1	0	0	0	1	1	1	1	1	1	0	0	0	1	0
Bob-PRBS	1	0	0	1	0	1	1	0	0	1	1	1	1	0	0	0
BOB-PD1	0.5	0.5	1	0.5	0	0	1	0.5	0.5	1	0	0.5	0.5	1	0.5	0
Bob-PD2	0.5	0.5	0	0.5	1	1	0	0.5	0.5	0	1	0.5	0.5	0	0.5	1

Bob Key: 10011010

Table 4-2: Eavesdropper Key

Xk	1	0	1	1	0	0	1	1	1	1	0	1	0	1	1	0
Yk	0	1	0	0	0	1	1	1	1	1	1	0	0	0	1	0
Eva-PRBS	0	0	0	0	0	0	0	1	0	0	1	1	1	1	1	0
Eva-PD1	1	0.5	1	1	0	0.5	0.5	1	0.5	0.5	0	0.5	0.5	0.5	1	0
Eva-PD2	0	0.5	0	0	1	0.5	0.5	0	0.5	0.5	1	0.5	0.5	0.5	0	1

Eva Key: 11101010

4.3 Comparison between Bob and Eva Key

From the Table 4-3 we can observed that 5 out of 8 bits of Eva key are similar to Bob key. So we can conclude that **Eva generate almost 50% correct key.**

Table 4-3 : Comparison between Bob and Eva Key

Bob-Key	1	0	0	1	1	0	1	0
Eva-key	1	1	1	0	1	0	1	0

In order to support our results we also performed another experiment with long key.

Bob Generate 38 bit key

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

Eva generate 32 bit key

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

As we can see, Bob and Eva has different length of key. In order to find same key we accept only those key which is accepted by both Bob and Eva at the same time. We can observe from the Eva key the first bit is 1 and Bob first key is also 1 generated at the same time we accept this bit. Next two bits of Eva 1, 1 are not same as Bob we reject these bits and so on.

Table 4-4 : Long Key Comparison between Alice and Bob

Bob-Key	1	0	0	1	1	0	1	0	0	0	0	1	1	1	1	1	0	0	1	0	1	0	1	0	0	1	1	1	0	1	0	1	0	1	1	1	0	0
Eva Key Similar to Bob	1	0	-	-	-	0	-	0	0	-	-	-	1	-	1	-	0	0	1	0	1	0	-	0	-	1	-	1	-	-	-	-	0	-	-	1	-		

Since Bob generated 38 bit key, we can observe from the Table 4-4. Eva able to generate 18 bits same as Bob which proof our previous results. We can conclude that by using this Eavesdropping method Eva can steal 50% of information.

Eva steal the key information before the Alice and Bob announced their basis information via classical channel. This classical design of BB84 QKD model is easily breakable because Eva know 50% of key information.

4.4 Future Work

Studying the classical analogue of phase encoded BB84 QKD protocol give us the opportunity to delve into its key practical points with the help of VPI software. Next I will compare these classical protocol with the QKD VPI module when this will be available.

4.5 Summary

In this chapter we do analysis of our classical phase-encoding BB84 QKD protocol in case of Eavesdropper. First we describes different eavesdropping techniques used to intercept the communication between legitimate users. In the next section we applied beam splitting technique. It shows that both legitimate user Alice and Bob are unaware of the presence of Eavesdropper. The last section describes how Eva can obtain the key information of Bob by stealing some portion of optical pulses and then performing key distillation. The comparison of Bob and Eva key shows that Eva can steal 50% of Bob key information. Then we proposed a Decoy State techniques which can be helpful in order to detect eavesdropper. This will be implemented in Future work.

5. CONCLUSIONS

Since the development of first BB84 Quantum Key Distribution (QKD) protocol in 1984, a huge progress has been achieved in the encryption field. QKD is different from traditional cryptography by providing secure distribution of secret key in data communication. QKD protocol is very effective for the detection of eavesdropper. In addition, QKD protect individual and corporate date information infrastructure.

To achieve the maximum efficiency of QKD protocol the ideal photon source is not available. The source acts in a probabilistic way in contrast to the generation of coherent states. In this thesis first we presented mathematical equations of phase-encoding BB84 QKD protocol with coherent states and single photon. Secondly we introduced a classical version of phase-encoded BB84 QKD protocol on VPI-Photonics software. The results of this classical design has clearly depicted successful communication between transmitter (Alice) and receiver (Bob) in case when Bob decode the key information in the same basis as Alice basis used to encode key. Key portion is discarded when Bob measure the key in different basis as Alice basis. These results are similar to original BB84 QKD protocol.

Third we performed key distillation at the Bob side. The results show that 50% of key information is successfully retrieved which is again same with original BB84 protocol. Fourth we tested our classical model on real fibre with dispersion and attenuation, we observed that key information obtained at the receiver side is less than 50%. The reason is synchronization issues and key sequence being too short. If we use dispersion and attenuation free fibre we can retrieve key information at receiver side successful.

Fifth we performed eavesdropper analysis of our classical design. If an eavesdropper steal the optical pulses between the fibre, we demonstrated that Alice and Bob is unaware from his presence .With this stealing information eavesdropper can easily retrieve 50% of Bob key information which proved that this classical protocol is easily breakable.

ABBREVIATIONS - ACRONYMS

QKD	Quantum Key Distribution
CV-QKD	Continuous Variable Quantum Key Distribution
DV-QKD	Discrete Variable Quantum Key Distribution
MZM	Mach-Zehnder Modulator
MZI	Mach-Zehnder Interferometer
PM	Phase Modulator
PBC	Polarization Beam Combiner
PBS	Polarization Beam Splitter
DCF	Dispersion Compensating Fibre
FBG	Fibre Bragg Gratings
HOM	High Order Mode
BER	Bit Error Rate

ANNEX I

Parameters Setting

Emission Frequency	1550nHz
Average Power	1mW
Line Width	10M
Symbol Rate	0.3e9
Centre Frequency	193.1e12
Number of Symbol	16 to 512
Couple Factor	0.5
Optical Delay	2ns
Fibre length	1km to 10000km
Attenuation	0.25e-3
Dispersion	16e-6
PMD Coefficient	2.2e-12/31.62
Channel frequency	1e9
Responsivity	0.7
Photodiode Type	APD
Avalanche Multiplication	1
Thermal Noise of PD	10e-12

ANNEX II

List of Components:

1. Continuous-Wave Laser source
2. Mach-Zehnder modulator (MZM)
3. Pseudorandom data sequences (PRBS)
4. Rectangular pulses generator
5. Optical Coupler
6. Phase Modulator (PM)
7. Polarization Beam Combiner (PBC)
8. Polarization Beam Splitter (PBS)
9. Polarization Controller (PC)
10. Avalanche Photo Diode (APD)
11. Attenuator
12. Delay
13. Signal Analyser
14. Beam Splitter (BS)
15. Erbium-Doped-Fibre Amplifier (EDFA)
16. Multiplier
17. Optical Fibre

REFERENCES

[1] Gisin, N., et al., Quantum cryptography. Reviews of modern physics, 2002. **74**(1): p. 145.

[2] W.Shor, Peter (1995). "Scheme for reducing decoherence in quantum computer memory". Physical Review A. **52** (4): R2493–R2496.

[3] Nielsen, Michael A.; Chuang, Isaac L. (2010). Quantum Computation and Quantum Information. Cambridge University Press. p. 13. ISBN 978-1-107-00217-3.

[4] J.R. Klauder and B. Skagerstam, *Coherent States*, World Scientific, Singapore, 1985.

[5] Scarani, V., et al., The security of practical quantum key distribution. Reviews of modern physics, 2009. **81**(3): p. 1301.

[6] B. Yan, Q. Li, H. Mao and X. Xue, "High-Speed Privacy Amplification Scheme Using GMP in Quantum Key Distribution," in *IEEE Photonics Journal*, vol. 12, no. 3, pp. 1-13, June 2020, Art no. 7600213, doi: 10.1109/JPHOT.2020.2987611

[7] C. H. Bennett and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing". In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York, 1984.

[8] Ivan B. Djordjevic - Physical-Layer Security and Quantum Key Distribution (2019).

[9] Yan, Hui & Zhu, Shi-Liang & Du, Shengwang. (2010). Efficient Phase-Encoding Quantum Key Generation with Narrow-Band Single Photons. Chinese Physics Letters. 28. 10.1088/0256-307X/28/7/070307.

[10] Zhu Cao *et al* 2015 *New J. Phys.* **17** 053014.

[11] Paul D. Townsend & I. Thompson (1994) A Quantum Key Distribution Channel Based on Optical Fibre, Journal of Modern Optics, 41:12, 2425-2433,DOI: 10.1080/09500349414552271.

[12] Coppersmith, D., D.B. Johnson, and S.M. Matyas, *A proposed mode for triple-DES encryption.* IBM Journal of Research and Development, 1996. **40**(2): p. 253-262.

[13] Lim, C.C.W., et al., Concise security bounds for practical decoy-state quantum key distribution. Physical Review A, 2014. **89**(2): p. 022307.

[14] Ma, X., et al., Practical decoy state for quantum key distribution. Physical Review A, 2005.**72**(1): p. 012326.

[15] Lucamarini, M., et al., Efficient decoy-state quantum key distribution with quantified security.Optics express, 2013. **21**(21): p. 24550-24565.

[16] Yicheng Shi, Hou Shun Poh, Alexander Ling, and Christian Kurtsiefer, "Fibre polarisation state compensation in entanglement-based quantum key distribution," Opt. Express 29, 37075-37080 (2021).

[17] Amaresh Mahapatra and Edmond J. Murphy, “Electrooptic Modulators,” in Optical Fiber Telecommunications IVA, Chapter 6, pp.258–294, Eds. Ivan Kaminow and Tingye Li. Academic Press, San Diego, 2002.

[18] Fumio Koyama, Kenichi Iga, “Frequency chirping in external modulator,” J. Lightwave Technol., vol. 6, no. 1, Jan. 1988.

[19] R. Coates, G. Janacek, and G. Lever, “Monte Carlo simulation and random number generation,” IEEE J. Selected Areas Communication, Vol. 6, pp. 58–66, 1988.

[20] M. C. Jeruchim, P. Balaban, and K. S. Shanmugan, Simulation of Communication Systems, Kluwer Academic, 2nd ed., 2002.

[21] R. März, Integrated Optics: Design and Modeling, Artech House, Boston, 1994, p. 183.

[22] Gobby, C., Z. Yuan, and A. Shields, Quantum key distribution over 122 km of standard telecom fiber. Applied Physics Letters, 2004. **84**(19): p. 3762-3764.

[23] Bujang MA, Sapri FE. An Application of the Runs Test to Test for Randomness of Observations Obtained from a Clinical Survey in an Ordered Population. Malays J Med Sci. 2018 Jul; 25(4):146-151. doi: 10.21315/mjms2018.25.4.15. Epub 2018 Aug 30. PMID: 30914857; PMCID: PMC6422539.

[24] Dr. Hossein Arsham: Randomness of statistical Sampling: The Run test,2022 https://home.ubalt.edu/ntsbarsh/Business-stat/otherapplets/Randomness.htm. [Accessed 05/07/2022]

[25] Ajeet Singh Verma, A. K. Jaiswal, Mukesh Kumar, An Improved Methodology for Dispersion Compensation and Synchronization in Optical Fiber Communication Networks, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 5, May 201, 769-775.

[26] Gurpreet Kaur, Navdeep Kaur, Use of Dispersion Compensating Fiber in Optical Transmission Network for NRZ Modulation Format, International Journal Of Engineering And Computer Science ISSN: 2319-7242 Volume 3 Issue 5, May 2014, 5839-5842.

[27] K. O. Hill, F. Bilodeau, B. Malo, T. Kitagawa, S. Thériault, D. C. Johnson, J. Albert, and K. Takiguchi, "Chirped in-fiber Bragg gratings for compensation of optical-fiber dispersion," Opt. Lett. 19, 1314-1316 (1994).

[28] S. Choi, W. Shin, and K. Oh, "Higher-Order-Mode Dispersion Compensation Technique Based on Mode Converter using Hollow Optical Fiber," in *Optical Fiber Communications Conference*, A. Sawchuk, ed., Vol. 70 of OSA Trends in Optics and Photonics (Optica Publishing Group, 2002), paper WA6.
[29] Inoue, Kyo. (2006). Quantum key distribution technologies. Selected Topics in Quantum Electronics, IEEE Journal of. 12. 888 - 896. 10.1109/JSTQE.2006.876606.
[30] *A A Gaidash* et al *2016* J. Phys.: Conf. Ser. ***735*** *012072.*