Implementation of Noise Immune QKD using BB84 Protocol In Time Division Multiplexing – Passive Optical Networks

Archana.B
M.E-Communication System
Electronics and Communication Engineering
Kumaraguru College of Technology
Coimbatore, India
archana.bala7@gmail.com

Ms.Krithika.S
Assistant professor
Electronics and Communication Engineering
Kumaraguru College of Technology
Coimbatore, India
krithika.s.ece@kct.ac.in

***Abstract*—**This paper proposes a cryptographic method know as quantum cryptography. Quantum cryptography(QC)uses quantum channel to exchange key securely and keeps unwanted parties or eavesdroppers from learning sensitive information. A technique called Quantum Key Distribution (QKD) is used to share random secret key by encoding the information in quantum states. Photons are the quantum material used for encoding. QKD provides an unique way of sharing random sequence of bits between users with a level of security not attainable with any other classical cryptographic methods. In this paper,BB84 protocol is used to implement QKD, that deals with the photon polarization states used to transmit the telecommunication information with high level of security and by random change of photons in case of any eve's interruption using optical fiber. In this paper we have implemented BB84 protocol with eve's attack detection using photonic simulator OptSim 5.2.

Keywords: *Quantum Mechanism(QM),QuantumKey Distribution (QKD), Quantumcryptography(QC), BB84protocol, photonpolarization , OptSim5.2.*

*****

I. Introduction

Quantum Cryptography is one of the latest methods of security in the cipher world and has been proclaimed as the ultimate security. It involves the laws of Quantum Mechanics (QM) to create new cryptographic techniques. Quantum Key Distribution (QKD) is one quantum cryptographic primitive which is achievable with today's technology [1]. Secret key distribution is one of the interesting researches in the network security field. Digital cryptographic system provides a unique solution based on computational security. Technology growth in today's world is capable of breaking the security by a simple technique called brute force attack. Furthermore the impended product from quantum mechanics principle is the quantum computer and its algorithms are capable of solving the non polynomial problem in polynomial time. On the contrary, quantum cryptography from QM offers an unconditional security by the principle of uncertainty, photon entanglement and no-cloning theorem.

II. Quantum Mechanics

Quantum Mechanics (QM) deals with the motion and interaction of subatomic particles, incorporating the quantization concepts such as wave particle duality and uncertainty principle. Quantum key distribution uses QM to provide secure communication.QKD implies on quantum properties to detect eavesdroppers in one of two ways: either by relying on the Heisenberg Uncertainty Principle or by the violation of Bell's Inequalities in entanglement based schemes.

A. Theorms

- *Heisenberg's Uncertainty Principle* -There is a complication to quantum observations, when we measure the quantum position, let the quantum be a photon, electron or any other particle, you cannot know its velocity exactly and the complication is similar for the measurement of photon velocity and the position. This is the Heisenberg Uncertainty Principle exists to protect quantum theory.
- *Quantum Entanglement*-A quantum property consistent to QKD is quantum entanglement. Pairs of quanta can be produced which pretends to be a single entity and so called as EPR pairs following the work of Einstein, Podolsky and Rosen[2]. For example, quanta possess a property called the"spin": one quantum could have spin up, one spin down, so that the total spin is zero but until a measurement is made it is not clear to identify which of the pair it belongs to. If the EPR pair is separated, measuring one of the pair causes the other's wave function to collapse in the opposite state. It appears to know instantaneously that its partner has been measured, apparently contradicting Einstein's finding, that nothing can travel faster than light. This is known as the EPR paradox.
- *Quantum No-Cloning Theorem*-Quantum No-Cloning Theorem specifically prevents copies of an unknown quantum state from being created and was first identified by [3] Wooters, Zurek and Dieks. It is another 'protection' mechanism for quantum theory, in that copying unknown quantum states would enable an observer to measure the copies exactly and avoids the restrictions of Heisenberg's Uncertainty Principle. So, backup copies of quantum states cannot be taken and used in quantum computing error correction routines. And also eavesdropper cannot create copies of quantum information sent along a quantum channel. It also means that a quantum signal cannot be amplified along a quantum channel.

III. Quantum Key Distribution

Quantum key distribution is a key exchange technique implemented in quantum cryptography to generate a perfectly random key which is shared between the sender and receiver.

The keys are highly prohibited towards eavesdropping [4].QKD brings the higher level of security over the transmission in telecommunication channel.

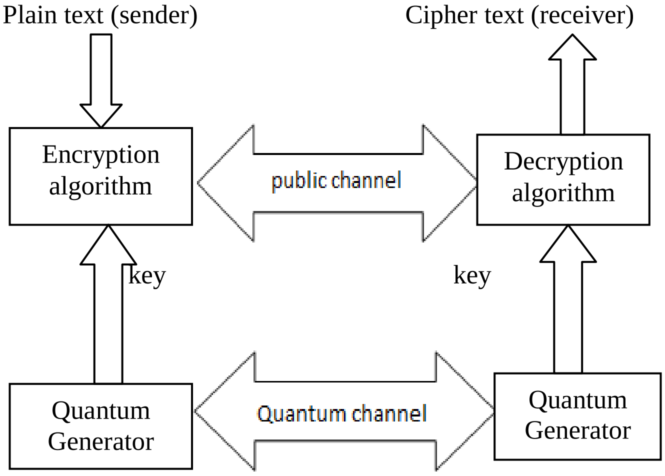

Fig. 1. Block diagram of Quantum Cryptsystem

A. Methodology Of QKD

Quantum mechanical effects can be used to transfer information from sender(Alice) to receiver(Bob) and any attempted eavesdropping by intruder(Eve) will always be detectable. Three different phases are needed to provide secure key exchange such as raw key exchange, key sifting and key distillation, with the guarantee to discard the secret key at any of the three stages.

- *Raw Key Exchange Principle*-This is the only quantum part of Quantum Key Distribution. Alice and Bob exchange quantum states using QC. Quantum information is passed along a quantum channel from Alice to be measured by Bob with or without the presence of eavesdropper. In all subsequent exchanges in a protocol, only a secure classical channel will be used. This is known as 'classical post-processing'.
- *Key Sifting*-Alice and Bob decide between them which of the measurements will be used for the secret key. The decision making rules depend on which protocol is being used, and some measurements will be discarded e.g. if the settings used by Alice and Bob did not match.
- *Key Distillation*-When reviewing experimental results protocol needs to be workable even in the presence of error transmission .Thus error correction and privacy amplification are required, which are the first two steps in the key distillation phase of the classical post-processing of remaining secret key bits. The third and final process is the implementation authentication, which impede man-in-the-middle attacks.

B. Need Of QKD

Quantum key distribution is a key establishment protocol which creates symmetric key material by using quantum properties of light to transfer information from Alice to Bob. Incontrovertible results of quantum mechanics[5] are obtained using QKD. It will highlight any eavesdropping in adversary. This can be used to derive a key, and the resultant key material can then be used to encrypt plaintext using a onetime pad encryption via a Vernam Cipher to provide unconditional security.

C. Photon Polarization

Electromagnetic waves such as light have an electric field associated with them, which vibrates as the wave travels. The direction of this vibration is known as polarization and polarized photons can be created by passing a normal beam of light (which contains photons of many differing polarizations) through a filter set for a specific angle of polarization.

Two bases are conjugate if the measurement of the polarization of one randomizes the other, and thus are subject to the Heisenberg Uncertainty Principle: measuring one photon affects the value of the other, so its impossible to know both values simultaneously. For example, filters set at 0^o and 90^o form one basis, and its conjugate basis has filters set at 45^o and 135^o.Photons passing through the polarization beam splitter(PBS) first will emerge with vertical or horizontal polarization, which will then be changed to diagonal polarization once they have been filtered by the conjugate basis, but 45^o or 135^o polarizations will occur with random probability of ½ as shown in Table I.

TABLE I. POLARIZATION STATUS

Sent Photon	**Receiver**		**Status**	***Bit***
	1st Photon	***2nd Photon***		
H	V	Unpolarized	Accept	0
V	H	Unpolarized	Accept	0
H	Unpolarized	V	Accept	1
V	Unpolarized	H	Accept	1
H	H	Unpolarized	Ignore	-
V	V	Unpolarized	Ignore	-
H	V	-	Ignore	-
V	H	-	Ignore	-

IV. PROPOSED KEY DISTRIBUTION SYSTEM

The paper deals with the QKD [6]system, which provides secured communication between two parties by the exchange of secret key using quantum channel (eg: optical fiber).This system deals with the implementation of BB84 protocol using simulation package OptSim. OptSim software provides variety of optical communication modeling and simulation. OptSim consist of variety of components related to photonic telecom components.

A. Basic QKD setup

The main objective of the paper is to model QKD experiments using OptSim which looks simpler in shallow, but their in-built components are not correlated with QKD operation. Polarization beam splitter (PBS) is one of the prime passive components of the QKD, its functionality is to pass the incoming light based on its angle. Unfortunately, in OptSim PBS splits the incoming light of photons to two different angles (Horizontal or Vertical).Some of the available components in the OptSim library does not execute as QKD components. For these cases, an alteration or creation of components is required.

OptSim has some other built in libraries can be utilized for simulation called visualizers. In this library, polarization analyzer and power meter components can be used for photon counting and also detectors can be used. There are three major classifications in the telecommunication system; they are transmitter, channel, and receiver. In transmitter block, photon source is the prime component and OptSim offers wide variety of optical sources with many inseparable properties. Attenuation is an indispensable mechanism in QKD to extract a single photon level from photon pulses. A polarizer is used for the polarization of photon extracted to the desired direction angle.

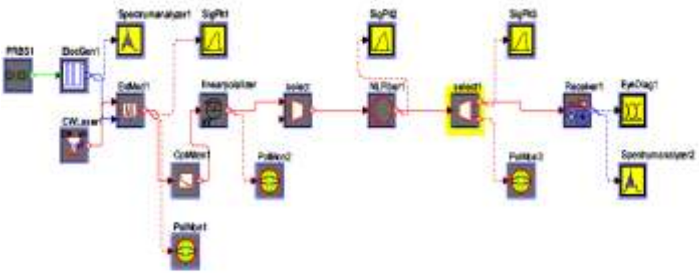

Fig. 2. Implementation of QKD setup

B. Implementation of BB84

The implementation of BB84 protocol[7] using the four polarization states of the form that defines the quantum key exchange in the quantum channel. In OptSim, optical fiber is standard component well known for the channel classification. To overcome the problem of PBS, OptSim offers a simple solution. The component called 'select' can be used as PBS as well as random selection of the incoming photons. Random choice of polarization is made to send the photons to receiver in QKD experiments. Receiver also picks random polarization for measuring the incoming photon. Finally based on the polarization, detectors will trigger. All photon values being recorded by the Alice and Bob are discussed in the public channel, this explains the basic operation of the QKD scenario. To obtain randomness discrete function consisting of random index, minimum value, maximum value and delta parameters are used. By carefully choosing the right values of the parameters correct randomness could be achieved. The evaluation parameters of the QKD components are listed in Table II.The implementation of BB84 protocol using QKD is shown in Fig.3. below.

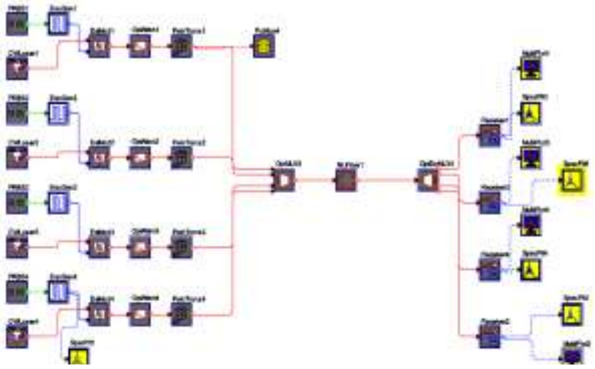

Fig. 3. Implementation of BB84 protocol

C. Algorithm Of BB84

Step1: Photons are polarized using conjugate bases, either a rectilinear basis (vertical/horizontal polarizations) or a diagonal basis (45^o and 135^o polarizations).

Step2: These polarized photons can be used to send information if each polarization generated by a basis is allocated the value '0' or'1' (i.e. one photon can carry one quantum bit (qubit) of information), and these encodings are agreed between Alice and Bob before they attempt to exchange quantum states.

Step3: Alice can produce photons with 4 different polarizations and (using a trusted random number generator) the basis for each photon is chosen at random and sends a stream of randomly polarized photons to Bob for measurement. This style of protocol is thus termed prepare and measure (P & M).

Step4: Bob now has to detect and measure these polarizations.[8] Receiver passes the photons through filters potentially changing their original polarizations and the photon counter records the results. As Bob does not know which basis Alice has used for each photon, he can only set his receiving bases randomly too. If he chooses correctly, the polarization is recorded accurately, if he chooses wrongly then the result is a random polarization matching his (not Alice's) choice of basis, with all information about the initial photon polarization lost. This is the **Raw Key Exchange** stage.

Step5: The **Key Sifting** stage is done over a public classical channel, where Alice and Bob each broadcast their choice of basis for each photon. As it is only the basis which is being publicly discussed, no key information can be gained by an eavesdropper at this point. The bases are compared, and any photon which had been processed using non-matching bases is dropped from the raw key material. The sifting process on an average leaves half of the exchanged qubits still available for use in the final secret key.

TABLE II. EVALUATION USING OPTSIM

QKD components	Evaluation	
	Availabilty-optisystem	*Modifications*
CW Laser	YES	NO
Bit sequence generator	YES	NO
Modulator	YES	NO
Optical attenuation	YES	NO
Polarization Monitor	YES	YES
Fiber channel	YES	NO
PBS	YES	YES
Select	YES	YES
Receiver	YES	YES

D. Eve's attack in BB84Algorithm

Eve could ever perform against the quantum channel, assuming Eve has absolutely no technological limits, i.e. she can do everything that quantum physics does not explicitly forbid. But clearly, Eve's attacks are not limited to the quantum communication channel. For instance, Eve could attack Alice or Bob's apparatuses, or she could exploit weaknesses in the actual implementation of abstract QKD. Our simulation utilize simple model of combination of attacks.

Mostly, Eve's attacks are classified as individual, coherent and incoherent attacks. For our experiment we generalize the Eve's attack mostly based on Intercept-Resend attack strategy and man-in-middle attack. Further, Denial of Service (DoS) attack is performed in our simulation. We assumed DoS carried out by Eve by simply abort the transmission line between Alice and Bob. This scenario particularly suits in fiber optic channel. In our experiment scenario, Eve is the connection hub between Alice and Bob.Eve can do intercept on incoming qubits and measure with rectilinear, diagonal polarizers, phase shift, photon rotator. She can send a new qubit to Bob. Further, she can also send null qubit or Alice's qubit to Bob.

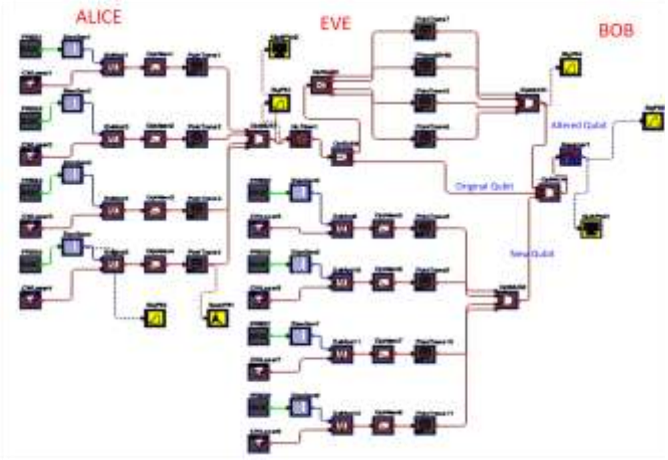

Fig. 4. BB84 with EVE's attack

E.Noise immune QKD

Noise is one of the biggest challenge in QKD. Distinguishing noise from eavesdropping is an intrigue research. Noise occurs due to various effects such as birefringence, polarization dispersion and free space issues i.e. scattering, absorption, diffraction, etc. Further, detectors problems like dark count and detection efficiency also adds noise to the system.Noise has various triggering factors which results in poor performance in QKD especially in secure key generation rate and distance. There have been several solutions proposed by researches.

Bob sends a rectilinear basis photon to Alice. Alice passes the incoming qubit to faraday rotator and forwards the verified qubits to Bob. Alice also sends unpolarized photon to Bobif it chooses a wrong rectilinear basis. The information about photon is calculated by the polarization basis and time delay between adjacent photons. The property of faraday rotator is :

Hin → Faraday Rotator → Vout

Vin → Faraday Rotator → Hout

Here H and V refer to horizontal and vertical basis. In our simulation, we use polarization rotator which is an inbuilt component.

The property of polarization rotator is:

0○ – 90○ = -90○

90○ – 90 = 0○

Here 0○ and 90○ refer to rectilinear angles. We have used two 'Time Delay' components for introducing time delay between photons. The simulation setup for noise immune QKD is shown in Fig.5.

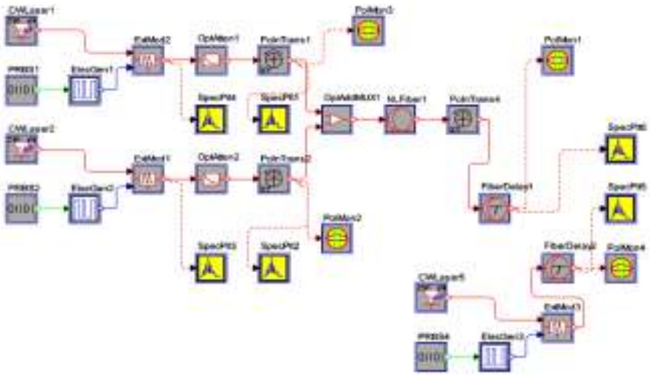

Fig. 5. Noise immune QKD

F.BB84 implementation in TDM

The main objective of this paper is to connect a pair of QKD devices, transmitter and receiver, as subscribers in the network and to enable a direct path between them without disturbing the network. Both systems are assumed to be connected to a branch, thus isolating them from subscribers in the rest of the network. Since only the narrow passband around the quantum channel is reflected, the rest of signals remain unaltered and the setup does not impose any kind of modification on the subscribers and other network devices. In this setup it could be possible to transmit single photons under the assumption that TDM slots are assigned to the QKD devices, hence synchronized to emit and detect single photon pulses only when there is no upstream traffic in their branch. This synchronization can be, avoided by performing a collision detection based solely on the QKD post-processing steps.

The technique is general enough to be applied in networks that by design have a chance of low noise periods. . If a TDM-PON channel is used, the performance would be reduced, since quantum and classical channels cannot operate simultaneously in the same device. On the other hand, using a wavelength separated well enough to avoid disturbing the quantum channel and outside of the classical channel plan, there would be no performance loss.

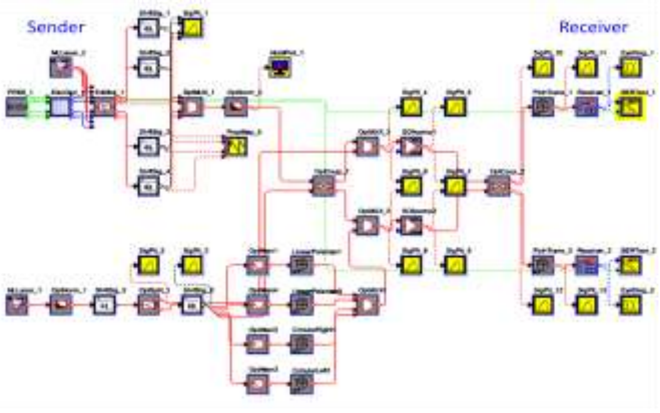

Fig. 6. Implementation of QKD in TDM

V. RESULTS

The spectrum of signal as seen in spectrum analyzer 1 of Fig 2 and Fig 3 implemented using simulation software OptSim [9] at the input of the optical fiber propagating is as follows

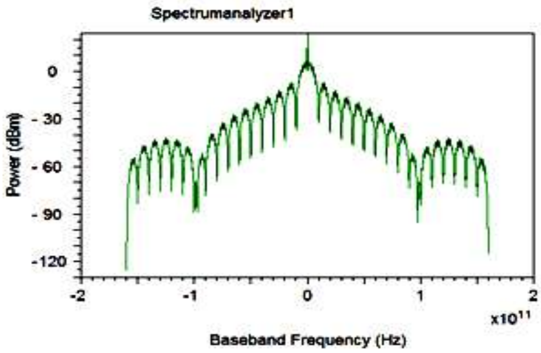

Fig. 7. Input spectrum of QKD and BB84 protocol

Fig 5 shows the input spectrum before the polarization of the input signal.

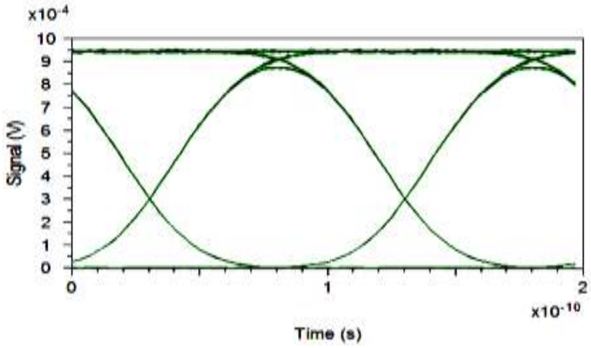

Fig. 8. Eye diagram of QKD

From the eye diagram shown in Fig6, it can be infered that the level of inteference is low and the total internal reflection happens inside the quantum channel after polarization of the photons.

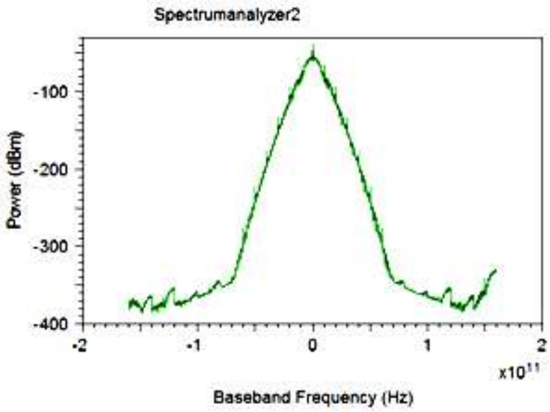

Fig. 9. Output spectrum of QKD

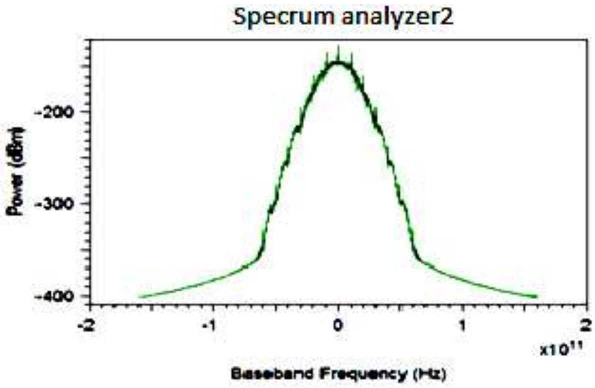

Fig. 10. Output spectrum of BB84 protocol

The spectrum at the output of the quantum channel after key distribution is shown in fig.6 and key disstribution with BB84 protocol is shown in fig.7.Comparing both the spectrums it can be infered that the effect of noise on the input is low after implementing BB84 protocol in the key distribution process.

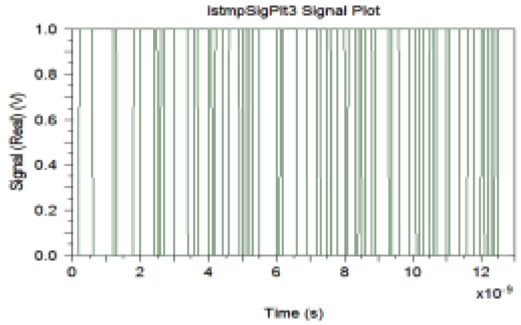

Fig. 11. Spectrum before EVE's attack

The signal in the Fig.4 is inferred from the sigplt1 as shown in the Fig.10 before eve's attack and the output spectrum in Fig.11 shows the spectrum after the detection of eve during the transmission between the sender and the receiver.

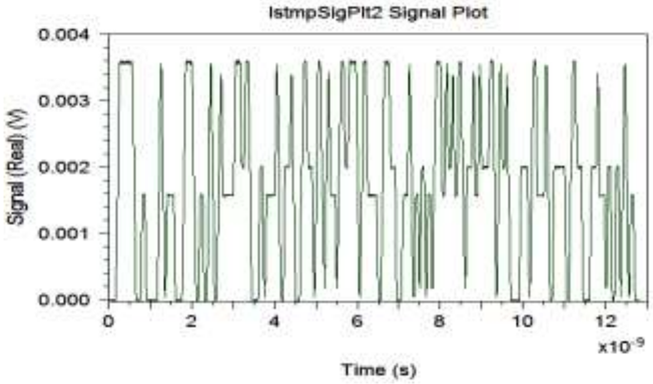

Fig. 12. Spectrum after EVE's detection

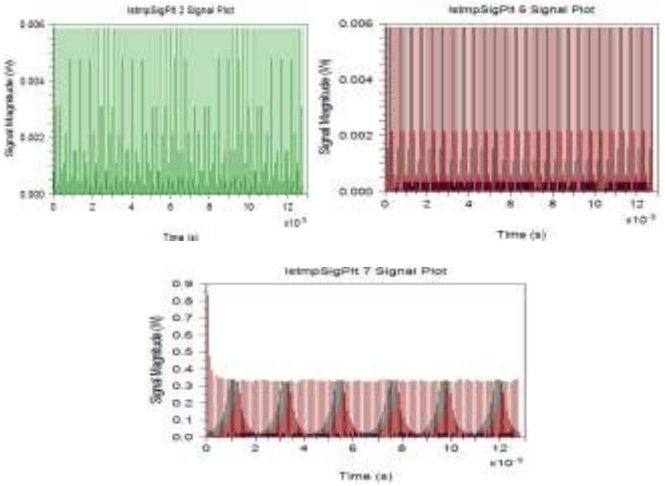

Fig. 13. Output spectrum of QKD implementation in TDM

The input spectrum derived from the block1 in the multiplot1in Fig 6 and the spectrum after the application of BB84 protocol in block 2 is shown in Fig 13.

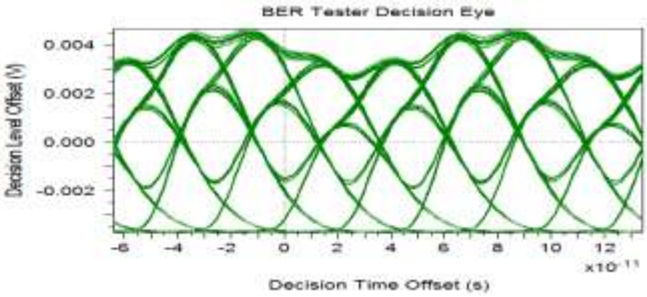

Fig. 14. Eye diagram

From the eye diagram shown in Fig 14, it can be infered that the level of inteference is low and the total internal reflection happens inside the quantum channel after polarization of the photons.

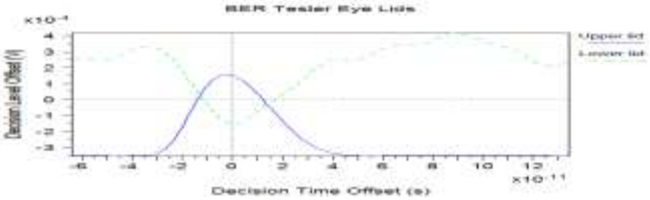

Fig. 15. Eye lids of eye diagram

VI. Conclusion

In this paper we have focused on hardware setup based on OptiSystem^{TM}.A combination hardware and protocols required to achieve unconditional security in key distribution is QKD. Both hardware and software should be evaluated correctly to analyze the performance of QKD protocols. In this paper we have used Optsim 5.2 to emulate the practical experiments with slightly modified components. The parameter settings of the components can be varied to find the optimum value. Thus, this simulation framework reduces the implementation cost by choosing appropriate components properly. The main advantage is that the integration is straightforward and does not require any modification including the network devices and protocols. This simulation can be further improved by including sophisticated Eve’s attack and detectors problems.

References

[1] Jesus Martinez-Mateo, Alex Ciurana, and Vicente Martin” Quantum Key Distribution Based on Selective Post-Processing in Passive Optical Networks” *IEEE photonics technology letters,* vol. 26, no. 9, may 1, 2014.

[2] Abudhahir Buhari, Zuriati Ahmad Zukarnain, Shamla K.Subramaniam” An Efficient Modeling and Simulation of Quantum Key Distribution ProtocolsUsingOptiSystem” *Industrial Electronics and Applications, IEEE Symposium*,pp.83-89,sept2012.

[3] Patryk Winiarczyk, Wojciech Zabierowski ”BB84 analysis of operation and practical considerations and implementations of quantum key distribution systems” *CADSM’2011, Polyana-Svalyava (Zakarpattya), Ukraine*, pp.23-25, feb2011.

[4] Wang Yong, Wang Huadeng, Li Zhaohong ,Huang Jinxiang “Man-in-the-middle Attack on BB84 Protocol and its Defence” *IEEE International Conference*, pp.438 – 439, 2009.

[5] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,”*Rev. Modern Phys.*, vol. 74, pp. 145–195, Jan. 2002.

[6] P. Eraerds, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, “Quantum key distribution and 1 Gbps data encryption over a single fiber,” *New J. Phys.*, vol. 12, no. 6, p. 063027, 2010.

[7] Sharma. A, Lakshmangarh, Ojha, V,Lenka, S.K.”Security of entanglement based version of BB84 protocol for Quantum Cryptography” *Computer Science and Information Technology (ICCSIT), IEEE International Conference* ,pp.83-89, july 2010.

[8] Q.Y. Cai, “Eavesdropping on the two-way quantum communication protocols with invisible photons,” *Physics Letters A,* vol. 351, no. 1-2, 2006, pp. 23-25.

[9] http://optics.synopsys.com

[10] http://www.optiwave.com