Quantum Cryptography and Polarization Control Mechanisms of the Entangled Photons

[1]Namit Garg, [2]Nafisur Rahman

[1]M.Tech. Scholar, [2]Assistant Professor, Department of Computer Science and Engineering, School of Engineering Sciences and Technology, Jamia Hamdard, New Delhi, India.

[1]namitgarg.1991@gmail.com, [2]nafiis@gmail.com

Abstract: Modern cryptography algorithms are based on the basic process of the one-way functions in which large integer numbers are factorized into the prime numbers, which is said to be UNCONTROLLABLE. These are prone to the advancement in computing field and mathematics to reverse the basic process of one-way functions. Quantum Cryptography is one of the latest and advanced cryptography technique, which is different from all other cryptography techniques and is more secure. The main objective of this research is to understand the working of Quantum Cryptography and the issues associated with it. The problem observed during the study of Quantum Cryptography was how to control a real-time state of polarization (SOP) of entangled photons which was caused due to channel parameters. This study proposes how to completely control the multiple polarization states caused due to birefringence by deploying the polarization controllers in a closed loop configuration, or by studying the DWDM on how the data/photons transmitted should be received at the receiver end without any BER (Bit Error Rate).

Keywords — Quantum Cryptography (QC), BB84, BBM92, State of Polarization (SOP), Quantum Key Distribution (QKD), Dense Wavelength Division Multiplexing (DWDM), BER.

I. INTRODUCTION

The concept of quantum was first introduced by Max Planck, a German physicist, in 1900. Since then, the study of quantum physics has advanced through many physicists' efforts. Quantum cryptography (QC) [4], first proposed by Stephen Wiesner, in 1968, relies on the fundamentals of quantum mechanics, whereas, the conventional public key cryptography, relies on evaluating complex mathematical functions leading to computational difficulties in solving them. These traditional methods cannot yield any sort of indication/traces of eavesdropping at any point in the communication channel or any mathematical proof to the actual complexity of reversing the one-way functions used.

Quantum encryption (done using BB84 protocol) [1] can be conducted by measuring the quantum state of the singular photons ejected from weak coherency/consistency laser source. However, this system is affected by the attacks that divide the photons and measures the state of them incorrectly.

In 1991, Artur Ekert developed a varied approach to solve the problem of quantum key distribution based on quantum entanglement, an unusual quantum correlation. In order to compensate for the vulnerabilities of the BB84 protocol, a new protocol called BBM92 protocol [1] was developed by Bennett, Brassard, and Mermin in 1992. In this, QKD protocols [10] were further extended to use entangled quantum bits, that are interrelated [9] so that if there is any change in the quantum state of one of them, the other photon changes the quantum state instantaneously. The BBM92 protocol used entangled polarized photons to implement QKD. It has a large number of advantages over other cryptographic methods to increase the security of data/key transmission.

II. PROBLEM STATEMENT

Polarization Mode Dispersion (PMD) [5] is one of the known limitations in optical transmission systems. It arises due to the communication channel (optical-fiber) parameters like birefringence which causes random fluctuations. These fluctuations cause State of Polarization (SOP) of the signal to change randomly and in an unpredictable way over a period of time, leading us to the below problem statement:

"The photons which are used to create a Quantum Key or Secret Key are prone to change the SOP which can cause issues in generating the secret key. The change in polarization can be due to birefringence [2][3]."

III. PROPOSED SOLUTIONS

If we wish to have some sort of relation between the SOP of input and output signal in the communication channel, then we need to have some kind of polarization controlling mechanism. The complex situation arises when we have

 DOI : 10.18231/2454-9150.2018.0286

different polarization states mapped into corresponding polarization states at the receiver. The scenario of optical-fiber systems where a quantum bit is allocated to the SOP of the transmitted single photon is called polarization coding. In such cases, the measurement base which the sender and the receiver of the message should choose should be orthogonal and be any of two independent non-orthogonal bases. Hence, it will be difficult to transmit the quantum key unless and until we achieve full control on the polarization states (states change due to random polarization rotations over the communication channel) of the photons.

The suggested solutions have been discussed in the sections that follow.

IV. Polarization Controllers

By configuring the polarization controllers in a closed loop. Introducing a polarization control system just before the receiver will nullify the effect of the channel parameter so that when the signal is received, the Jones matrix is identity [5][6]. This method will help control the SOP of the photons which can be used in generating the key. In this solution, let us consider 2 non-orthogonal polarized signals, viz S_1 and S_2 which are communicated to the receiver over optical-fiber. At the receiver's end, we have the 2 signals which are having some sort of transformation or rotation due to channel parameters. Let the transformation over the channel be represented by Jones matrix T and the signal received can be expressed in Eq. 1. To nullify the effect of the transformation and get the original signal, we introduce the polarization controller which do a set of rotation: R_1 and R_2.

$$R_1TS_1 = S_1$$
$$R_2S_1 = S_1$$
$$R_2R_1TS_2 = S_2 \quad (1)$$

Rewriting first 2 equations of Eq.1 as Eq.2.

$$R_1 = \begin{pmatrix} 1 & 0 \\ 0 & e^{j\phi} \end{pmatrix} T^{-1}$$

$$R_2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{j\phi} \end{pmatrix} \quad (2)$$

Combining the Eq.2 with Eq.1 to write third equation Eq.3.

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{j(\theta+\phi)} \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix},$$

iff, $\theta + \varphi = 0$ modulo 2π. (3)

By this, we mean that R_1R_2T must be equivalent to 1, or $R_1R_2 = T^{-1}$, which implies that the rotations which are due to the effect of T are neutralized by the use of the polarization controller. Hence, state of polarization of the signal will be preserved. In spite of the fact that the above method can control the state of polarization of the signals sent over the optical fiber, the co-propagation of these signals is still a concern. The photons count should not be impacted by the extinction of the photons over the communication channel. Alternatively, we can have multiple signals carrying the important information over the optical-fiber multiplexed using as many wavelengths so that both the sender and the receiver are synchronized.

To control the polarization of the signal at a wavelength λ_0, we employ S_1 and S_2 at different wavelengths, expressed by $\lambda_1 = \lambda_0 - \Delta\lambda$ and $\lambda_2 = \lambda_0 + \Delta\lambda$. Rewriting Eq. (1) by replacing $T = T(\lambda)$.

$$R_1\,T(\lambda_1)S_1 = S_1$$
$$R_2S_1 = S_1$$
$$R_2R_1\,T(\lambda_2)S_2 = S_2 \quad (4)$$

From monochromatic case, we know $T(\lambda_2) = T(\lambda_1) + 2\Delta\lambda(\partial T/\partial\omega)$,

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{j(\theta+\phi)} \end{pmatrix} \left(I + 2\Delta\omega T^{-1}\frac{\partial T}{\partial\omega}\right)\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad (5)$$

For monochromatic case, $\theta + \varphi = 0$ modulo 2π is valid if and only if,

$$2\Delta\omega T^{-1}\frac{\partial T}{\partial\omega} << 1 \quad (6)$$

We can see Eq. (6) is half of $\tau/2$, we can rewrite it as $\tau\Delta\lambda<<1$ which depicts that the SOP of the photon is preserved. Below is the experimental set-up.

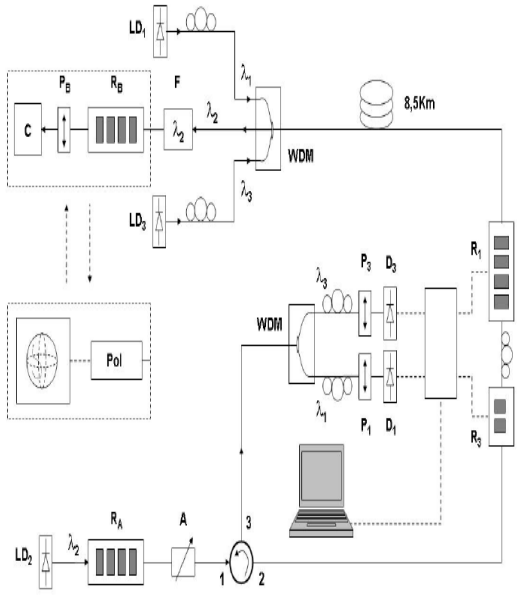

Fig. 1. Experimental set-up: The three loops represent manual polarization controllers, R: electrically driven polarization controllers, P: linear polarizers, D: classical photodetectors, C: single photon counting module, LD: Laser diodes, A: attenuator and Pol: polarimeter.

V. DWDM Based Technique

By setting up a DWDM in such a way that the BER comes out to be 0: DWDM [11][12] is a technique for signal transmission over optical fiber. The process involves n number of signals that are multiplexed using n wavelengths and are sent over the single optical-fiber just

 DOI : 10.18231/2454-9150.2018.0286

like a multi-mode. Every optical-fiber will be carrying multiple signals with minimal difference in the wavelength. When the photons are sent to the optical fibers, they are multiplexed using DWDM method, so that we get the same SOP of photons at the receiver's end. This method basically depends on a couple of factors like the transmission rate and the wavelength [13].

DWDM consists of few parameters which are important for its configuration, related to each other using the formulae [14]:

1. $\Delta T_{disp} = D*\Delta\lambda*L$ where,
   D = Dispersion
   $\Delta\lambda$ = max. Wavelength spacing
   L = Length of the channel.
2. $\Delta T_{disp} \leq 0.15*T$ where,
   T = rate at which data is to be transmitted.

We have designed a DWDM having transmission rate as 1Gbps and 10 Gbps and found the BER for each scenario.

VI. Simulation Results

The experimental set up of DWDM involves multiplexing of multiple signals using an ideal multiplexer. This multiplexed signal is transmitted over the communication channel of particular length along with the amplifiers as shown in the Fig2 and Fig3. The multiplexed signal is then de-multiplexed using ideal de-multiplexer and then each signal is received using the optical receiver and analyzed using Eye Diagram Analyzer.

The length of the eye depicts the quality of the output. Eye length is inversely proportional to BER, larger the eye length, lesser the BER and smaller the eye length, more the BER, depicting that the SOP of the photons changes.

For the transmission rate of 1 Gbps over 60 km, the output eye length observed in eye Diagram Analyzer, Fig4, is more and the BER is 0, depicting that the output and input SOP is similar.

For the transmission rate as 10 Gbps over 20 km, the output eye length observed in eye Diagram Analyzer, Fig5, is less and the BER is more which depicts that there is a slight change in the SOP of the photons.

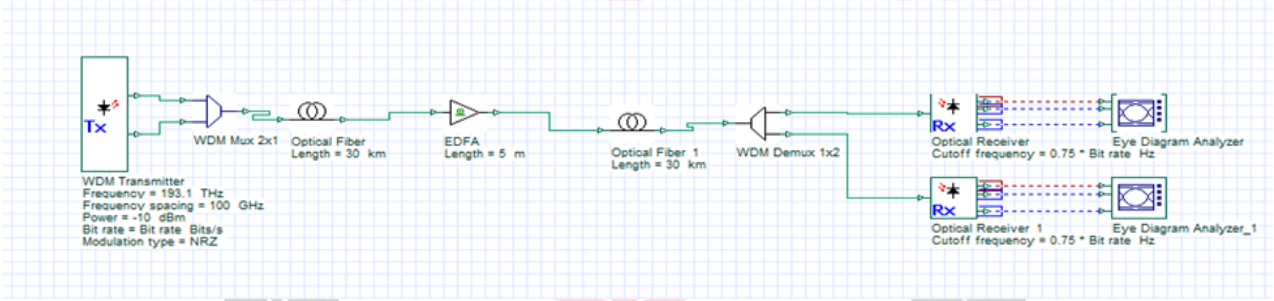

Fig.2 Experimental DWDM set-up for Transmission Rate of 1 Gbps

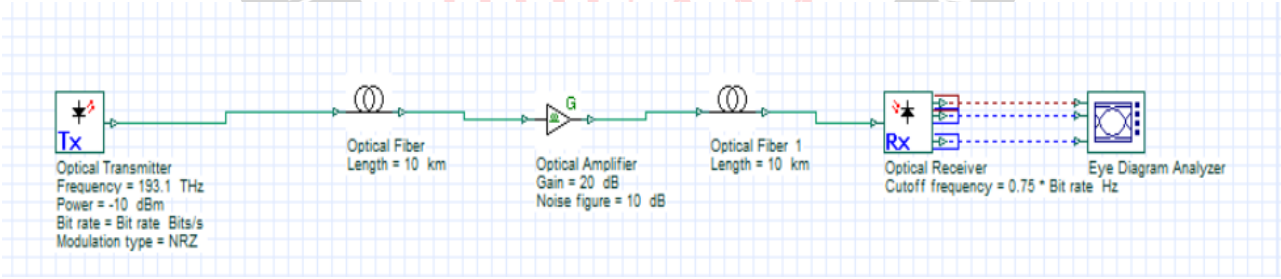

Fig.3 Experimental DWDM set-up for Transmission Rate of 10 Gbps

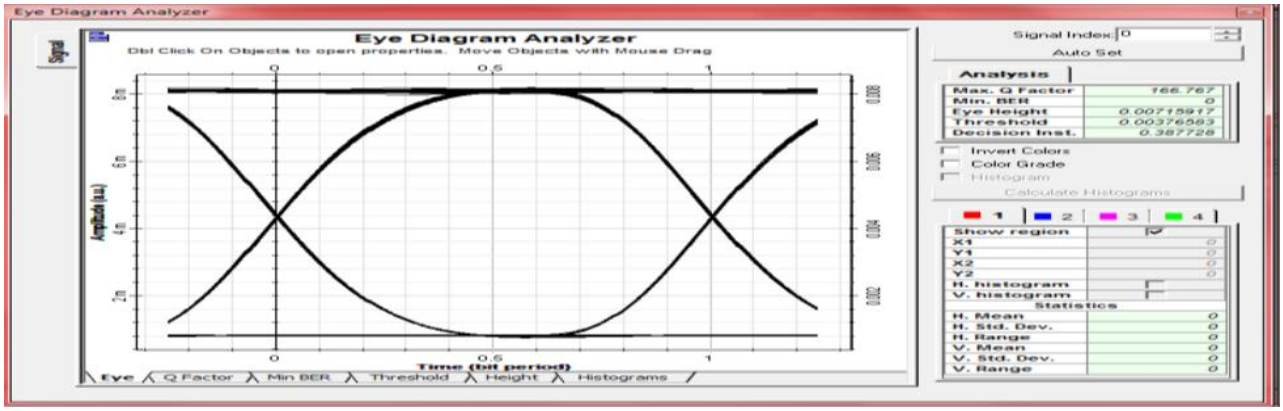

Fig.4 Output eye at the receiver end for a transmission rate of 1 Gbps

 DOI : 10.18231/2454-9150.2018.0286

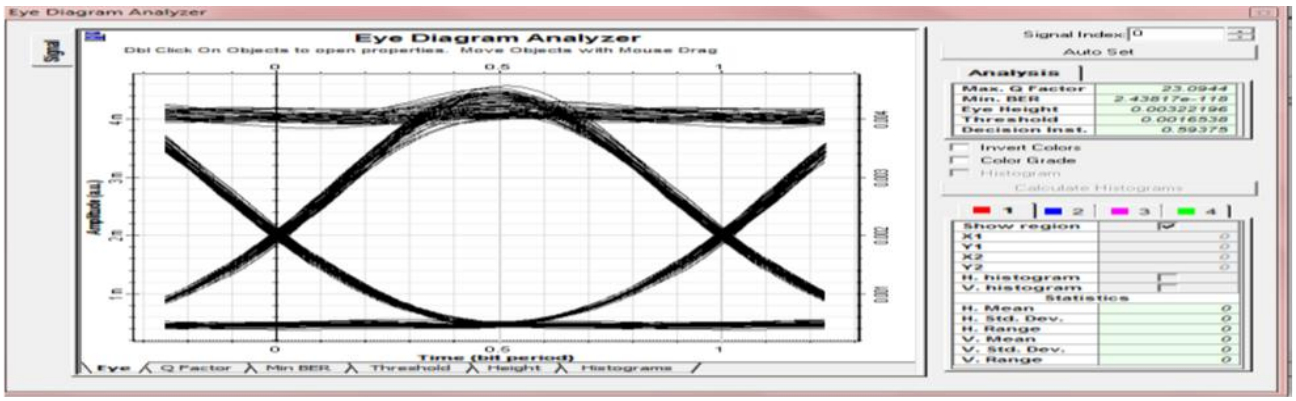

Fig.5 Output eye at the receiver end for a transmission rate of 10 Gbps

V. CONCLUSIONS

Based on the above study, we can conclude that quantum cryptography is more secure than other methodologies and is based on the quantum of physics i.e. photons which are used for key generation. The photons are prone to change their state when they are transmitted between sender and receiver for key generation. We demonstrated DWDM set up using Opti System for the transmission rate of 1 Gbps & 10 Gbps and found the BER for 1 Gbps is 0 and for 10 Gbps is $2.43x10^{-118}$. This shows that for a transmission rate of 1 Gbps, the SOP of the photons has not changed during transmission whereas, for the transmission rate of 10Gbps, the SOP has changed during transmission.

We also conclude that DWDM set-up should have less transmission rate. If we increase the transmission rate, then the BER will increase which will lead to change in the SOP of the photons which makes the key generation difficult.

For higher transmission rate, we can use a system which can control the polarization using the wavelength multiplexing of 2 non-orthogonal inputs signals at the regular interval so that the polarization does not change at the receiver end.

REFERENCES

[1] Cangea, O, Oprina, C.S. and Dima, M.O., "Implementing Quantum Cryptography Algorithms for Data Security", Electronics, Computers and Artificial Intelligence, 30 June -02 July 2016.

[2] Ojha, V., Sharma, A., Goar, V., Trivedi, P., "Limitations of Practical Quantum Cryptography", International Journal of Computer Trends and Technology- March-April 2011.

[3] Aditya, J., Shankar Rao, P., "Quantum Cryptography".

[4] Bhandari, Sandepak, "A New Era Of Cryptography: Quantum Cryptography".

[5] Xavier,G.B., Vilela de Faria, G., Temporão, G.P., and Von der Weid, J.P., "Full polarization control for fiber optical quantum communication systems using polarization encoding", Pontifical Catholic University of Rio de Janeiro - Optoelectronics & Instrumentation Group Center for Telecommunications Studies – Rio de Janeiro – Brazil.

[6] Xavier,G.B., Vilela de Faria, G., Temporão, G.P., and Von der Weid, J.P., "Experimental polarization encoded quantum key distribution over optical fibres with real-time continuous birefringence compensation", Pontifical Catholic University of Rio de Janeiro, Brazil.

[7] Nagali, E., Sciarrino, F., De Martini, F., Piccirillo, B., Karimi, E., Marrucci, L., Santamato, E., "Polarization control of single photon quantum orbital angular momentum states", Compl. Univ. di Monte S. Angelo, 80126 Napoli, Italy.

[8] Wu, G., Chen, J., Li, Y., Zeng, H., "Stable polarization-encoded quantum key distribution in fiber", Key Laboratory of Optical and Magnetic Resonance Spectroscopy, Department of Physics, East China Normal University, Shanghai, China.

[9] Bethune, D.S., Risk, W.P., "An Auto-compensating Fiber-Optic Quantum Cryptography System Based on Polarization Splitting of Light", IEEE JOURNAL OF QUANTUM ELECTRONICS, VOL. 36, NO. 3, MARCH 2000.

[10] Tang, X., Ma, L., Mink, A., Nakassis, A., Hershman, B., Bienfang, J., Boisvert, R.F., Clark C., Williams, C., "High Speed Fiber-Based Quantum Key Distribution using Polarization Encoding", National Institute of Standards and Technology, 100 Bureau Dr., Gaithersburg, MD 20899.

[11] [MUKHERJEE97] BiswanathMukherjee, "Optical Communication Networks", McGraw Hill, July 1997, 575 pages, http://networks.cs.ucdavis.edu/users/mukherje/book/toc.html.

[12] [GREEN93] P.E.Green, "Fiber-Optical Networks", Prentice-Hall 1993.

[13] [GERARD98] Gerard Lachs, "Fiber-Optical Communications, McGraw-Hill Telecommunications 1998.

[14] [KEISER 03] Gerd Keiser, Optical fiber Communications, McGraw-Hill 2003.

 DOI : 10.18231/2454-9150.2018.0286