IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.7, Special Issue.1, Jan 2019 E-ISSN: 2347-2693

Quantum Mechanics Inside Quantum Communication and Quantum Bit Error Rate(QBER)

Susmita Nayek[1*], Utpal Roy[2]

[1,2]Department of Computer & System Sciences, Visva-Bharati, Santiniketan -731235, INDIA

[*]*Corresponding Author: sush08@gmail.com*

Available online at: www.ijcseonline.org

***Abstract*—**The quantum cryptography has changed the landscape of the conventional cryptography theory and the field of security itself. The Quantum cryptography differs from the classical cryptography in the sense that data and the information are kept secret by the properties of quantum mechanics without importing any extra formulation. In case of classical cryptography the security is based on the conjecture difficulty of factoring and computing a special mathematical function. The first Quantum Key Distribution (QKD) protocol was proposed by C H Bennet and Brassard in 1984[1](BB84). In course of time many variants of QKD protocols have been proposed, all are basically based more or less in the same principle. In this paper role and the beauty of the Quantum Mechanics behind the QKD protocol have been unfolded and explained. The pros-and cons of the protocol have been analyzed in details. The quality of the QKD protocol is measured through a factor called QBER (Quantum Bit Error Rate). The bit error rate is an essential phenomena during the transmission of quantum bit along the quantum channel. Both quantum mechanical and mathematical analysis of QBER have been discussed in the paper. An empirical formula for QBER has been proposed too.

***Keywords*—**Quantum mechanics, quantum cryptography, light(photon), eavesdropping, quantum bit error rate(QBER)

I. INTRODUCTION

Long time ago it was also necessary to send encoded messages to distant place. The intended person was the only target to receive messages. To others the messages was just like noise. The encoding was done by the recipient of the message through some encoding key. There are several protocols for encoding and decoding messages into its understandable form. RSA (Rivest-Shamir and Adleman) algorithm is the most popular modern technique for encoding messages. It basically depends on the conjecture difficulty of factoring some mathematical function. The public key is developed with a product of two large prime numbers. If the factoring of this product is done within the range of a time then RSA algorithm cannot come into use. Till date theoretically the quantum computers are able to factorize large numbers. Fortunately, the quantum world supplies a solution for it.

Quantum physics has changed the landscape of cryptography in last two decades. Basically the quantum Cryptography exploits quantum phenomena such as uncertainty principle and quantum entanglement to secure the distribution of quantumcryptographic keys. In the Key Distribution process two legitimate users establish two exact copies of random bit string with the communication channel. Quantum cryptography is probably secure against eavesdropping attack as a matter of fundamental principle of quantum mechanics so that the secret data cannot be compromised unknowingly to the legitimate users of the channel. The first QKD protocol was proposed by CH Bennett and G Brassard in 1984[1] after that various studied on its security proof and power have been made [1-27]. Recently Kumar and Prabhakar[12] have made the study of QBER using Frequency coded quantum key distribution. A considerable amount of studies have been made on field of Quantum Key Cryptography [1] and based on the BB84 QKD many variants of it have been proposed in literature. Out these following are important ones E91[2], BB92[13], SSP [16][17], DPS [21][22], SARG04[15], COW [19][20], KMB09[23] and S09[24]. The nature of the all the protocols have been discussed in survey work of Singh, Gupta and Singh [25].

It has already been stated that QKD protocols are very novel. The novelty resides in the fact that working principle of QKD protocols are governed by quantum mechanical principal. The quality of the QKD protocols are governed by QBER. The discussions and analysis of the QBER has been described in the following sections.

II. QKD in the light of Quantum Mechanics:

In the quantum cryptography data are kept secret with the fundamental properties of quantum mechanics. But classical cryptography security relies on the fact of conjecture difficulty

of computing some mathematical function. The quantum mechanics is the basis on which the quantum key distribution protocols rely to transfer and share keys.
The quantum key distribution protocols are based on two quantum mechanical properties

1. **Heisenberg Uncertainty Principle**
It states that a (conjugate) pair of quantum observables of a quantum mechanical object (subject to Heisenberg Uncertainty Principle) measuring one of the observables necessarily randomizes the other. The key security of a protocol over an open channel relies onHeisenberg Uncertainty Principle. Suppose if we want to measure the position and momentum; energy and time of a quantum mechanical object then accurate measurement of position and energy will lead to error in measurement of momentum and time respectively. The product of the error of two variable is subject to some limit. The BB84, BB92, SARGO4 are QKD protocols based on Heisenberg Uncertainty Principle.

2. **Quantum Entanglement**
Quantum mechanics allows entangled states of two distant systems. Measuring the properties of one system can instantly change the properties of the other system. Precisely, quantum entanglement is a physical phenomenon which occurs when pairs or groups of quantum particles are generated, interact, or share spatial proximity in ways such that the quantum state of each particle cannot be described independently without affecting the state of the other(s), even when the particles are separated by a large distance.

No-Cloning theorem:
The no-cloning implies that it is not possible to create an identical copy of an arbitrary quantum states. The quantum information cannot be kept copied whose states are not explicitly known. Summarily the theorem states the inaccessibility of the quantum information. It actually means that quantum states and the quantum information as well cannotbe amplified at all. Thus no such unitary operator can exit which can copy arbitrary quantum state.
Let C be an unitary coping operator that can exactly copy a normalized quantum state $|\varphi>$, represents a qubits
$|\varphi>=\alpha|0>+\beta|1>$where
$1=\alpha^2+\beta^2$applying coping operator
$C|\varphi>=\alpha|0>+\beta|1>$then

$$<\varphi|C|\varphi>=\alpha\alpha^*|00>+\beta\beta^*|11>$$
$$+\alpha\beta^*|01>+\beta\alpha^*|10>$$

It indicates that the cross terms should be zero which contradicts the probability condition
.
The Heisenberg principle based QKD protocols uses the fact that while a quantum state is measured it changes from its original. So the eavesdroppers may inject error in the quantum information transfer while operating through quantum channel. This error must be detected by the QKD protocol.

On the other hand, in the entangle based protocol eavesdropper may inject the extra quanta into the qutantum channel to disrupt the quantum information. Here the information only springs into existence when the entangled quanta are measured. The extra quanta violates the Bell's inequalities and so the eavesdroppers will be detected in the entangle based protocols also.
Quantum no-cloning theorem also further do not allow the eavesdroppers to take copy of information quanta for further processing.

Quantum Key Distribution protocols
Quantum cryptography based on quantum principle has provided unconditional security in data transfer. Quantum mechanical principles are used to quantum key distribution for transferring and sharing data. In order for this to be translated into working Quantum Cryptographic Protocol a combination of quantum processing and classical processing of data is essential.
In the QKD protocol two classical users Alice and Bob they communicate among themselves through
1. A quantum channel and
2. A classical channel

Security of both the channel is based on the nature of protocol using quantum mechanical principle. In any QKD protocol following are the various phases:
1. Use of Random Number Generator by Alice
2. The Transfer of quantum bits through quantum channel (raw key exchange)
3. Key shifting
4. Key distillation
5. Estimation of Eve's presence
6. Privacy amplification
7. Discussion over public channel
8. Confirmation of Key

In the first phase Alice uses her Quantum Random Number generator to generate the random quantum states and allow to pass them through quantum channel.
Alice begins her communication by choosing a random string of bits and for each bit Alice will randomly choose a basis (polarizer for photon communication) to encode the qubit. When the photon source is used the Alice will transmit a photon for each qubit with the corresponding polarization to Bob. For the photons Bob receives he will measure the polarization with a randomly used bases.

If Bob choose a same basis as used by Alice she will get the exact polarization state of photon and she will correctly infer the qubit Alice intended to send. If Bob chooses the wrong basis, his results, thus the qubit she reads will be random. The qubits sting corresponding to signal detected by Bob is known as *Raw Key*.

In the next phase Bob will notify Alice over a public channel what basis she has used to measure each photon. In discussion with Alice, Bob will come to know how much percentage of correct basis she has used. At this point Alice and Bob will discard those qubits which have been measured by Bob with a different basis. NowAlice and Bob has identical qubits of string which is called a *shifted key*.

In the next phase Alice and Bob choose a random subset from the shifted Key to compare and to ensure the consistency. If the bits agrees they discarded the subset of the key.

If there be no measurement error, no noise in the channel if any disagreement occurs on the qubit(s) during comparison then it indicates the presence of eavesdropper in the quantum channel. This reveals that the eavesdropper had attempted to measure the key. This could only be done (by Eve) by measuring the photons sent by Alice before reaching it to Bob. Importantly no-cloning theorem states that a quantum state cannot be replicate. It is impossible to know for Eve which basis Alice has used to encode the bit until after Alice and Bob discuss their measurement. Eve will be forced to guess.
With his guess if Eve chooses the incorrect basis according to Heisenberg principle message encoded on the other basis will be lost.

So in presence of Eve the information reaches to Bob her Measurement will be random and she will read thequbit 50% time wrong on an average. This implies that Eve will use the incorrect basis incorrectly 50% of time. So 25% of time Bob's measurement bits will differ from Alice. Now if Eve has affected all the n qubits then after the comparison of all bits by Alice and Bob then the Eve will go undetected on$\left(\frac{3}{4}\right)^n$. For a long qubit n the error will be less.
At the end of the above process the Alice and Bob has the sifted Key. Main objective is that in practice the practical channels are lossy, and the QKD protocolsare needed to be workable with in this scenario. The remaining secret key qubits will be more filtered with classical post-processing, this is called Key Distillation. It has two phases:

- Error correction and
- Privacy amplification

Error Correction

In this stage Alice and Bob will generate a more corrected shifted key. The corrected shifted key is shorter than the raw key and perfectly correlated qubits. The fraction of perfectly correlated shifted key that is to be extracted from the partially extracted shifted key is given by the equation.

$I(A:B) = H(A) + H(B) - H(AB)$……. (1)

This equation physically corresponds to that fact that sender (Alice) reveal an amount of information at least as large as the uncertainty the receiver (Bob) has on the shifted key.

Explanation of the error correction part is as follows: it actually estimates the actual error rate in the transmitted qubit string. This is known as Quantum Bit Error Rate (QBER). The error in the quantum channel occurs mainly due to Noise or due to the presence of eavesdropper. Generally due to security reason it is considered that all the errors have occurred due to eavesdropping. If the QBER is less than a fixed value as defined earlier than the shift key passes to the Privacy Amplification stage. If the Error Rate is greater than that predefined value that it is concluded that the amount of information lost to the eavesdropper is too large to guarantee the secrecy of the key. So eventually the secret key is discarded and a new round of QKD is initiated.

Privacy Amplification (PA)

It is the other part of the post processing of the sifted key. The main objective of this part is to eliminate the information that Eve has already gained from the sifted key. The PA is designed in such a way to counteract any knowledge that Eve has gained from the Quantum Channel during the transmission of the Raw Key. The PA compresses the qubit string (sifted key) by an appropriate factor. This factor is determined from the QBER as calculated earlier. The sifted key having high value QBER needs more compression. In this manner it removes at least the same number of qubits from the sifted key from which Eve may have gleaned the information from Raw Key.
The fraction of the Key that is to be discarded is equal tomin$(I_{EB,}I_{EA})$ where I_E is Eve information about the sifted key of Alice and Bob. A PA procedure that works in a probable manner is based on Two-universal hash functions. The extractable fraction of the key using one way post processing is as follows:

$r = I(A,B) - \min(I_{EA}, I_{EB})$…… (2)

The other form of post-processing is the two-way post processing in which both Alice and Bob could be the senders. Thus the bound on the extractable portion of the shifted key can to be improved to an amount.

Authentication:

Considering previous stagesof a QKD protocol it is the jest that classical authentication should ensure that Alice and Bob are not under the Man-in-Middle attack. An adverse effect may occur as Bob to Alice and Alice to Bob: this means that all traffic between Alice to Bob has been routed through a third party, without the knowledge of them. This situationcannotbe detected with the help of any quantum mechanical process. Now the secret key is to be pre-shared between Alce and Bob for the use in authentication of very first quantum exchange.

BB84 Protocols

Photons are the most popular carrier of quantum key bits. The photon quanta has a zero rest mass and integral spin having intrinsic polarization property. The light has wave particle duality i.e. both particle and wave nature. Most of the QKD

protocols use polarization states of photons for the key qubits. Considering its wave form the light composed of photon is an electromagnetic wave. The light wave is described by electric field and magnetic field perpendicular to each other and the propagation of light is perpendicular to both electric field and magnetic field. Light considering its wave naturelight exhibit the polarization. While considering the polarization state of light, one component of light either electric field or magnetic field is to be considered. As both the electric and magnetic fields are correlated the knowledge of either electric field or magnetic field is sufficient to describe the electromagnetic wave. Usually electric field is considered when talking about polarization state of light.

Considering the projection of electric field vector on the plane of perpendicular to the direction of travel of light the state of polarization of light is described. Thus considering the direction of electric state vector the state of polarization could be linearly polarized, circularly polarized or elliptically polarized. So choosing two linearly orthogonal polarization axes one can denote (considering Dirac notation) the vertically polarized photon as $|\uparrow>$ and horizontally polarised photon as $<\rightarrow|$. The qubitstate prepared by the polarized light is described the wave function

$\varphi = \alpha|\uparrow> + \beta|\rightarrow>$ where $\alpha^2 + \beta^2 = 1$ ……(3)

Unconditional Security of QKD

The novel idea behind the QKD is the fact that it can achieve unconditional security. The novelty resides in the fact that data in QKD are kept secret by the properties of quantum mechanics where as in case of classical cryptography the security is preserved by the conjecture difficulty of computing certain mathematical function. The most popular QKD protocol is BB84 proposed 1984 named after the inventors (C H Bennett and G. Brassard). Jest of the protocol is that the participants Alice and Bob wish to agree on secret key about which no eavesdropper can obtain significant information. Alice sends each qubits of secret key in one of the set of conjugate bases which Eve does not know, this key is protected by the impossibility of measuring the state of a quantum system simultaneously in conjugate bases (governed by no-cloning theorem).

But in case QKD the unconditional security does not mean absolute security. The unconditional security of QKD is restricted under certain conditions, these are discussed below.

1. Eve cannot intrude the Alice's and Bob's devices. In addition he/she cannot tamper with their setting choices, such as basis choice.
2. The quantum random number (QRNG) generator used in the photon pulse generator must be fully trusted by Alice and Bob. This QRNG is used to send the quantum state from Alice side and to select the bases towards the Bob side.
3. In QKD transmission one classical channel is also used, that classical channel should be authenticated by the unconditionally secure authentication protocol.
4. Eve should obey the quantum mechanical laws.

Failure of these requirements would compromise the security of QKD protocol. However it should be noted that stated conditions only promise theoretical security.

Limitation of Quantum Key Distribution (QKD)

The field of quantum computer and quantum computing is the significant development in the field of future technology in general and in the field of security in special. But this is the only way of securing communication in the era of quantum computer. However this impressive field of science is still in its immature stage and has several restrictions mainlydue to the non-availability of quantum hardware and quantum programming environment. Limitations associated to system implementing QKD Protocols are pointed as follows:

Single Photon Source

Single photon source is the key factor for the security implementation of QKD using BB84 protocols. But it is difficult to have a single photo source due to photon source implementation reason. For multiple photon transmission eavesdropper will launch the PNS attack (Photon number splitting attack). Thus eavesdropper will access the additional photons generated by Alice and will have information after analysis. This type of attack will go undetected. Now a day faint laser pulses are used to achieve single photon source. As a result most of the time the slot will remain empty, a few would have single photon and most are of multi photon.

Distance

Due to lossy and nosey quantum channel the present QKD distribution is restricted to 60 to 100 km.

Data Rate

In the Fiber Optics Communication data rate, now a day, is of the Gigabits order very common. But due to single photon pulse, even in the case of ideal QKD, the data rate is very low.

Security

Though the QKD's unconditional security has been proved in many ways, any implementation of QKD will be susceptible to attacks at device level.

Quantum Bit Error Rate (QBER):

The Quantum Bit Error Rate (QBER) denotes the Quality quantum signal transmitted in QKD communication. Mathematically it is defined as the number of bits under error to the total number of detected bits.

$$QBER = \frac{B_{error}}{B_{error}+B_{shift}} \quad \text{…….. (4)}$$

QBER depends on the various factors mainly on the QKD protocol used for the transmission. The value of QBER varies from protocol to protocol used. The nature of quantum channel also affect bit error rate. The cannel noise and imperfection of the components in the link affect the QBER to an extent. The nature and the power of the QRNG also influences the **bit error** factor.

Ekert in his seminal paper [2] used quantum entangle photon for QKD between Alice and Bob. It is his demand that during transmission no information is carried by photon thus no chance of eavesdropping but if eaves dropper inject extra photon in the quantum channel then its presence could be detected through Bell's Inequality at either end.

SARG04 protocol has sifted key rate of 25 % as compared to the 50% of BB84 [1] protocols. But the attenuation increases specifically for pulses with one and two photons, thus indicating the presence of eavesdropping even in case of week coherent pulses.

Following the format of the Tables of the article [26] the operation of BB84 protocol with and without eavesdropping has been analyzed in our study with Tables 1 and Table 2. The symbols used in the tables having their usual significance. Alice generate the random number with the QRNG and basis are encoded accordingly and she transmit the photons to Bob. Bob measures the polarization of each received bit by choosing a random basis for each bit. On an average, statistically in 50% of cases Alice and Bob has chosen the same basis. So even in ideal case the QBER is maximum 50%. But the presence of eavesdropper increases the QBER.

From Table I, it is clear that the QBER is less than 50% [$\frac{12}{29}$ .100 = 41.37%] (considering transmission errors), which is acceptable. Thus Alice and Bob can decide to continue the communication. In such case the shifted keys of both the parties will be partially correlated due to transmission errors. These errors can easily be removed by reconciliation process of 'parity check'.

Table 2, depicts the case of presence of eavesdropper and transmission errors. Here the QBER is very high [$\frac{24}{29}.100 =$ 82.75%] which is much greater than 50%. This indicates the presence of eavesdropping in the communication. Both the parties can abort the transmission now and can set a new round.

III. TECHNOLOGICAL ASPECTS

The Technological setup is an important aspect for the measurement of the QBER. The QKD is very useful for application when the distance between A and B is very small. The medium, detector and sources are important factors for QKD experiment. Faint laser pulse is used normally as photon source. The distribution of photon from the source is described as Poisson distribution.

$P(n,\mu) = \frac{\mu^n}{n!} e^{\mu}$……..(5)

For very small (mean number) it has low probability ($n > 1$) $\approx \frac{\mu}{2}$. The problem is that for

$P(n=0) \approx 1-\mu$……(6)

Implies detector dark count. For the photon gun ideally single photon source is not yet available. Normally optical fiber is used as quantum channel. The associated refractive index is $n(x,y)$ and attenuation is 2dB/km at 800 nm, 0.dB/km at1550 nm. The ideal quantum detector should have high quantum efficiency over a large spectral range with low dark counts, good timing resolution and short recovery time. But in practice it is difficult to have such an ideal detector. The experimentalists always compromise with the quality. Currently as a detector APD(Avalanche Photodiodes) is the best choice. In free space and fiber communication silicon APD is best suited for QKD.

Considering all technological aspects

$QBER = \frac{R_{error}}{R_{error}+R_{shift}}$; $R_{shift} = \frac{1}{2}R_{raw}$…….(7)

where

$R_{raw} = q.f_{pulse}.t_{ana}.\mu.p_{pdet}$……(8)

q correction factor for the setup, . f_{pulse} number of laser pulses per second, t_{ana} probability of a photon arriving analyzer, μ mean number of photon per pulse and p_{pdet} probability of detecting a photon correctly.

The error in the QBER measurement, R_{error} depends on mainly three parameters Detector quality, optical quality and the quality of the photon source.

From the knowledge and property of the QBER are provided an empirical formula for QBER in terms of μand distance d between the receiver and transmitter has been developed. This formula approximately estimates the QBER valid for the distance up to 160 km.

The empirical formula for the QBER is as follows:

$QBER = A_0 + A_1 e^{\frac{d-x_0}{\mu}}$ ……(9)

A_0=0.0022

A1=-4.78 x 10^{-4}

X_0=-28.9981

It also agrees with the results that available in literature [27, 28]. The nature of QBER is depicted in Figure 1. It has been found that the QBER varies from protocol to protocol but the overall variation is maximum 1%. With the increase of distance d the QBER increases exponentially. The QBER is less for a certain distance (d) for lower value ofμ. With the increase of $\mu$for a fixed distance the QBER increases. Here in the Figure 4.1 the variation of QBER has been shown for μ= 0.95 and μ=2.6.

Table 1. Working of BB84 protocol without eavesdropping

Alice's Random bits	1	1	0	1	0	0	1	1	1	0	1	0	0	1	1	0	0	0	1	1	1	0	0	1	0	1	0	0	1
Alice's Random basis	+	×	×	+	×	+	+	×	×	+	+	+	×	×	+	×	+	+	×	×	+	×	+	+	×	+	+	×	+
Alice's Photon With Polarization	|	\	/	|	/	%	|	\	\	%	|	%	/	\	|	/	%	%	\	\	|	/	%	|	/	|	%	/	|
Assuming transmission errors at some random bits (e.g. bit number 4,24)																													
Bob's random basis	+	×	+	+	×	×	+	+	×	+	×	+	×	×	×	+	+	+	×	×	×	+	+	+	+	×	+	+	+
Bob's measurements (raw key)	1	1	-	-	0	-	1	-	1	0	-	0	0	1	-	-	0	0	1	1	-	-	0	1	-	-	0	-	1
Bob reveals his basis for received bits to Alice on a classical channel																													
Alice verifies the basis	C	C	W		C	W	C	W	C	C	W	C	C	C	W	W	C	C	C	C	W	W	C	C	W	W	C	W	c
Alice's shifted key	1	1			0		1		1	0		0	0	1			0	0	1	1			0	1			0		1
Bob's raw key is correlated with Alice's for some bits and now include errors due to transmission impairments																													
Bob's shifted key after public discussion	1	1			0		1		1	0		0	0	1			0	0	1	1			0	1			0		1
A simple parity check (reconciliation) will be used for rectifying this decorrelation																													

w- Wrong, c- Correct

Table 2. Working of BB84 protocol with eavesdropping and Transmission Errors

Alice's Random Bits	1	1	0	1	0	0	1	1	1	0	1	0	0	1	1	0	0	0	1	1	1	0	0	1	0	1	0	0	1
Alice's Random Basis	+	×	×	+	×	+	+	×	×	+	+	+	×	×	+	×	+	+	×	×	+	×	+	+	×	+	+	×	+
Alice's Photon With Polarization	|	\	/	|	/	%	|	\	\	%	|	%	/	\	|	/	%	%	\	\	|	/	%	|	/	|	%	/	|
Assuming transmission errors at some random bits(e.g. bit number 4,24)																													
Eve's random basis	+	+	+	×	×	×	×	+	+	×	+	×	+	+	+	×	×	+	×	+	+	×	×	+	+	+	×	×	+
Eve's measurements	1	-	-	0	0	-	-	-	-	-	1	-	-	-	1	0	-	0	1	-	1	0	-	0	-	1	-	0	1
Eve's bits (assuming random bits at nil measurements)	1	0	1	0	0	1	1	0	0	0	1	0	1	0	1	0	1	0	1	1	1	0	0	0	1	1	0	0	1
Eve's random basis	+	+	+	×	×	×	×	+	+	×	+	×	+	+	+	×	×	+	×	+	+	×	×	+	+	+	×	×	+
Eve's photons with polarizations	|	%	|	/	/	\	\	%	%	/	|	/	|	%	|	/	\	%	\	|	|	/	/	%	|	|	/	/	|
Assuming transmission errors at some random bits (e.g. bit number 1, 18)																													

Bob's random basis	×	×	+	+	×	×	+	+	×	+	×	+	×	×	×	+	+	+	×	×	×	+	+	+	+	×	+	+	+
Bob's measurements (raw key)	0	-	1	-	0	1	-	0	-	-	-	-	-	-	-	-	-	0	1	-	-	-	-	0	1	-	-	-	1
Bob reveals his basis for received bits to Alice on a classical channel																													
Alice verifies the basis	W		W		C	W		W										C	C					C					C
Alice's shifted key					0													0	1					1					1
Bob's raw key is correlated with Alice's for some bits and now include errors due to transmission impairments																													
Bob's shifted key after public discussion					0													1	1					1					1
Alice and Bob conclude that this transmission is not secure due to very high QBER (82.75%) and abort the transmission																													

w- Wrong, c- Correct

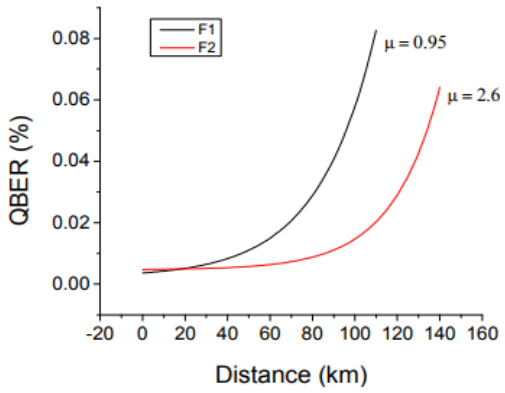

Figure 1. Variation of QBER with and distance d.

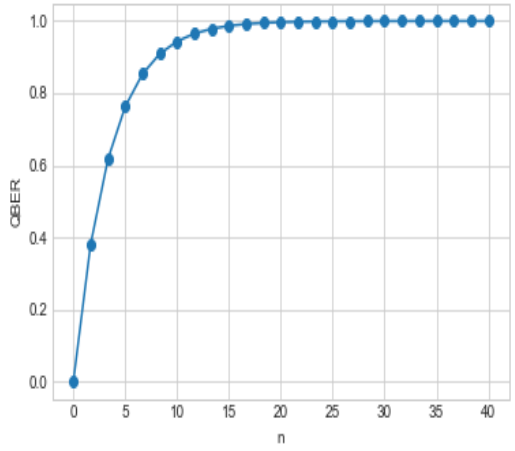

Figure 2. Nature of QBER Vs. length of the key n

The probability that Eve choses the incorrect basis is 50% while Alice choses her basis randomly. If Bob measures this intercepted Photons he gets the incorrect result with probability 50%. The probability guarantees an error in the key is $50\% * 50\% = 25\%$

If Alice and Bob publicly compare n key bits and pthe probability they find in disagreement is

$$QBER = 1 - \left(\frac{3}{4}\right)^n \ldots\ldots\ldots\ldots(10)$$

This is QBER. The nature of QBER is shown in Figure 2 with increasing no of n QBER initially goes increasing and with increasing value of n it gets stable.

IV. ACKNOWLEDGEMENT

Authors wishes to acknowledge sincere help and cooperation of Mr. Debjyoti Ghosh, Research Scholar of the department for his help, cooperation and interest.

REFERENCES

[1]. C. H. Bennett and G. Brassard, "*Quantum cryptography: public key distribution and coin tossing*," Proc. of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175-179, 1984.
[2]. [Ekert, A.k. "Quantum cryptography based on Bell"s Theorem", Physical Review Letters vol.67.no6 5th august 1991, pp.661-663.
[3]. D.Mayers, Journal. of ACM 48, 351 (2001), preliminary version in Mayers, D. Advances in Cryptology-Proc. Crypto 96, vol 1109 of Lecture Notes in Computer Science, Kobiltz, N.Ed.(Springer-Verlag, New York, 1996) pp. 343-357.
[4]. E.Biham, M.Boyer, P.O.Boykin, T.Mor and V.Roychowdhury, in Proc of the thirty second annual ACM symposium on theory of computing (Portland, Oregon, United States, 2000), pp. 715-724
[5]. H.K.Lo and H.F.Chau Science 283, 2050 (1999)
[6]. P.W.Shor and J.Preskill, Phys.Rev. Lett 85,441(2000), arXiv: quant-ph/0003004.
[7]. D.Gottesman, H.K.Lo, N.Liikenhaus and J.Preksill, „Quantum Information and Computation 5, 325 (2004), arXiv: quant-ph/0212066.
[8]. H.Inamori, N.Liikenhaus, and D.Mayers (2001), arXiv.quant-ph/0107017.
[9]. W.Y.Hwang, Phys.Rev. Lett. 91, 057901 (2003).
[10]. H.K.Lo, X.Ma and K.Chen, Phys.Rev. Lett 94, 230504 (2005)
[11]. H.k.Lo, in Proc of IEEE International Symposium on Information Theory (ISIT) (2004), p.137, arXiv.quant-ph/0509076.
[12]. Pradeep Kumar and A. Prabhakar,Bit error rates in a frequency coded quantum key distribution system,Optics Communications 282 (2009)3827-3833.

[13]. C.H. Bennett Quantum cryptography using any two non orthogonal states, Physical Review Letters 68 (21) (1992) 3121-3124
[14]. Mart Haitjema, "A Survey of the Prominent Quantum Key Distribution Protocols "http://www.cs.wustl.edu/~jain/cse571-07/ftp/quantum/index.html#b92
[15]. Scarani, A.Acin, Ribordy, G.Gisin.N."Quantum Cryptography protocols robust against Photon number Splitting attack." Physical Review Letters, vol.92.2004 http://www.qci.jst.go.jp/eqsi03/program/papers/O26-Scarani.pdf
[16]. N.Gisin. talk presented at the workshop on Quantum Computation, Torino. July 1997; D.bruss. Physical review letter. Vol 81.no3018 (1998)
[17]. Bechmann-Pasquinucci, H and Gisin.N "Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography." Physical Review Letter A59, 4238-4248; (1999).
[18]. N.Gisin, G.Ribordy, W.Tittel, H.Zbinden, "Quantum Cryptography", Review of Modern Physics, Vol 74 No 1, pp145-194, 2002
[19]. D.Stucki et al., Appl. Phys. Lett.87, 194108 (2005)
[20]. [Gisin N, Ribordy G, Zbinden H, Stucki D, Brunner N and Scarani V 2004, " Towards practical and fast quantum cryptography", arXiv:quant-ph/0411022
[21]. K.Inoue, E.Waks and Y.Yamanoto." Differential-phase-shift quantum key distribution using coherent light." Phys.Rev. A 68.022317 (2003).
[22]. E.Waks, H.Takesue and Y. Yamamoto, "Security of differential-Phase-Shift quantum key distribution against individual attacks." Phys.Rev.A 73,012344 (2006).
[23]. Muhammad Mubashir Khan et al. "High error-rate quantum key distribution for long distance communication" New J.Phys. 11 063043 http://iopscience.iop.org/1367-2630/11/6/063043/
[24]. Eduin Esteban, Hernandez Serna, "Quantum Key Distribution protocol with private- public key" arXiv: 0908.2146v4 quant-ph 12th may 2012.
[25] Hitesh Singh,D.L. Gupta,A. K. Singh,Quantum Key Distribution Protocols:AReview,IOCR Journal of Computer Engineering(IOSR-JCE),e-ISSN:2278-0661,p-ISSN:2279-8727 Volume 16,Isuue 2,Ver.XI(Mar-Apr.2014),PP 01-09
[26] M. Lopes and N. Sarwade, Cryptography from Quantum Mechanical View Point, Int. Jour. Of Cryptography and Information Security, Vol. 4. No.2 Page 13(2014).
[27] L. Lydersen, Practical security of quantumcryptography, Ph.D. thesis, Norwegian University ofScience and Technology, 2011.
[28] M. E. Rifai, Quantum secure communication usingpolarization hopping multi-stage protocols, Ph.Dthesis, University of Oklahoma, 2016.

Authors Profile

SusmitaNayek received B. Sc. Degree in Computer Science from Vidyasagar University in 2003 and M.Sc. Degree in Computer Science from Visva-Bharati in 2005. She has more than 12 years of teaching experience in the field of Computer Science.

She has submitted her Ph. D. thesis under the supervision of Prof. Utpal Roy, Department of Computer & System Sciences, Visva-Bharati. She has published seven research articles in various conferences and journals of national and international level. Her research interests include Quantum Computation and Quantum Cryptography.

Dr. Utpal Roy completed his Ph.D. from Department of Mathematics, Visva-Bharati and went to LAVAL University, Quebec, Canada for Post Doctoral work in 1994. He worked at IndianAssociation for the Cultivation of Science, Jadavpur, Kolkata as CSIR Scientist Pool during 1996-1997. He Joined the Visva-Bharati at the end of 1997 as Asst. Prof in Computer Science to teach theMCA course. He worked as Visiting Scientist in Academia Sinica, Taipei, Taiwan during 2001-2002.He worked as Professor in IT in Assam University Silchar, Assam during 2008-2009. Presently he is aProfessor and Former Head of the Department, Department of Computer & System Sciences, Visva-Bharati. He has been guiding Ph.D. students since long time and many students have been awardedPh.D. under his supervision.

