Entropy Security in Quantum Cryptography

Hitesh Singh
M.Tech
Department of CSE
KNIT, Sultanpur, UP, India

D.L. Gupta
Assistant Professor
Department of CSE
KNIT, Sultanpur, UP, India

A.K Singh
Associate Professor
Department of ECE
KNIT, Sultanpur, UP, India

ABSTRACT
Quantum mechanics is the basic principle which is applied in the cryptographic scenario of quantum cryptography. Present paper provides a conceptual framework on the high level security protocol in Quantum cryptography. This is used as a base for data security through quantum computing in modern cryptosystem. In this paper first of all a detailed description of BB84 protocol with noise and without noise is explained, then a detailed description of mathematical analysis done by [1] on entropy security is also shown. Finally the result of the experimental work done on Matlab is shown. Our work reveals that at only 37 % bit of the key, we get maximum entropy security in communication network. .In this approach it is also possible to manage security as well as personalize services based on Quantum cryptography in better way.

Keywords
Quantum cryptography, entropic security; information theory; quantum key distribution; Qubits; BB84 protocol.

1. INTRODUCTION
Security is one of the biggest demands for everyone. It is a big concern in wired as well as wireless network also. Quantum Cryptography uses the fundamental laws of quantum physics. The main achievement is that it can solve the problem of key distribution from the practical point of view; it is interesting that quantum cryptography may appropriately be realized by means of quantum optics and the optical fiber serves as a transmission channel. To encode information polarization (divergence, division) or phase can be used. Charles H.Bennett and Gilles Brassard took this approach and brought it in a series of papers that culminated and established the technological feasibility of the concept [2]. In this paper it is possible to create a high- level security protocol allowing to apply the quantum cryptography in communication network.

Rest of the paper is organized as: In section 2 related work has been shown, section 3 depicts a general view of quantum cryptography using BB84 protocol shown, section 4 shows how to measure a new high level security protocol, in section 5 conclusion is shown and future scope is focused in section 6.

2. RELATED WORK
The encrypted work using in the quantum cryptography in the high level security protocol has been done by good researchers which is mention below:

1. M.Niemiec [3] has focused his attention in INDECT: 'intelligent information system is supporting observation, searching and detection for security of citizens in urban environment" in a collaborative research project funded by the EU 7th framework program. Its main aim is to develop cost efficient tools for helping European police service to enforce the law and guarantee the protection of European citizen. This deliverable presents the high level quantum cryptography methods and verification of desired solution.
2. T.Godhavari et al. [4] has shown about a unique quantitative security analysis for the quantum transceiver model proposed for quantum based secure information transmission. In this model follows the same security analysis as BB84 protocol. The advantage of this model is that the less number of Qubits are communicated and also check bits are added. If this model is implemented practically, lesser Qubits may be enough to get the required security level when compared to BB84 protocol. It emphasizes about the different security level to meet the end user requirement and low-level parameters of a typical QC system.

3. QUANTUM CRYOTOGRAPHY
Quantum cryptography is based on the fundamental and unchanging principles of quantum mechanics. In fact quantum cryptography rests on two pillars of 20th century quantum mechanism, the Heisenberg Uncertainty Principle and the principle of photon polarization. Heisenberg Uncertainty principles say that if you measures one thing, you cannot measure another thing accurately. According to the Heisenberg uncertainty principle it is not possible to measure the quantum state of any system without disturbing that system. Thus, the polarization of a photon or light particle can only be known at the point when it is measured. This principle plays a critical role in thwarting the attempts of eavesdropper in a cryptosystem based on quantum cryptography. The photon polarization principle depicts how light photons can be oriented or polarized in specific directions. It is Heisenberg's uncertainty principle that makes quantum cryptography an attractive option for ensuring the privacy of data defeating eavesdroppers

3.1 Polarization
It is the process by which waves of electromagnetic radiation such as light, which would normally vibrate in all directions, are restricted to vibrate in one direction only. When measuring the polarization of a photon, the choice of what direction to measure affects all subsequent measurement. If a photon passes through a vertical filter it will have the vertical orientation regardless of its initial direction of polarization. Polarization can be used to represent either 0 or 1. In quantum cryptography this is called qubit

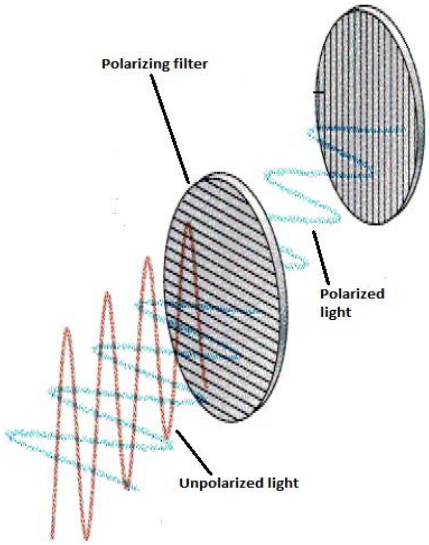

Fig 1. Light Polarization using filter

3.2 Qubits

A standard bit is in one of two states, '0' or '1' at the same time. A quantum bit or qubit can hold not only the states '0' or '1' but a linear superposition of both states, $\alpha|0> + \beta|1>$. This special notation is called the Dirac Notation (or ket notation) and is the standard notation for states in quantum mechanism. A qubit might be |0>, a horizontally polarized photon; or itmight be |1>, a vertically polarized one, or it might be $1/\sqrt{2}$ (|1> +*i*|0>), a right circularly polarized one, or any other linear combination with appropriate normalization. The Qubit cannot be copied because of the no cloning theorem of Diekes, Wootters, and Zurek [5][6]. A qubit is denoted by

$$|\Psi> = \alpha|0> + \beta|1>$$

A bit represents one of two points, but a qubit represents any point on the unit circle in the complex plane

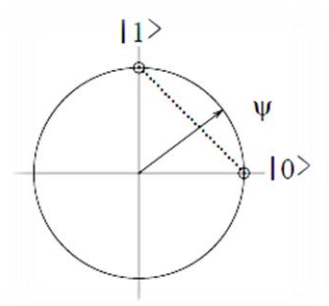

Fig 2. The Interpretation of qubits [16]

The state of qubit can be |0>, |1> or it can be an arbitrary mixture of |0> and |1>.

3.3 Quantum key distribution

Key distribution using quantum cryptography would be almost impossible to steal because Quantum key distribution (QKD) [7][8][9] systems continually and randomly generate new private keys that both parties shares automatically. A compromised key in a QKD system is able to decrypt only a small amount of encoded information because of continuously changes in private key. A secret key can be build from a stream of a single photon where each photon is encoded with a bit value of 0 or 1, typically by a photon superposition state such as polarization. These photons are emitted by a conventional laser as pulses of dim light so that most pulses do not emit a photon. This approach ensures that few pulses contain more than one photon travel through the fiber-optic line. In the end only a small fraction of the received pulses actually contains a photon [10]. The photons that are reached to the receiver are used. The key is generally encoded in either the polarization or the relative phase of the photon.

3.4 BB84 Protocol

The BB84 is the first quantum cryptographic communication protocol formulated in 1984. This protocol is capable to work for a transmission over 30 km of fiber optics cable, and also over free space for a distance of over one hundred meters [11]. The transmission is started from the quantum channel up to the communication over the public channel. In fig 3 one can see the abstract sequence diagram of BB84, where the first phase is the shifting phase in which client A and client B negotiate which bits are used and which bits are discarded.

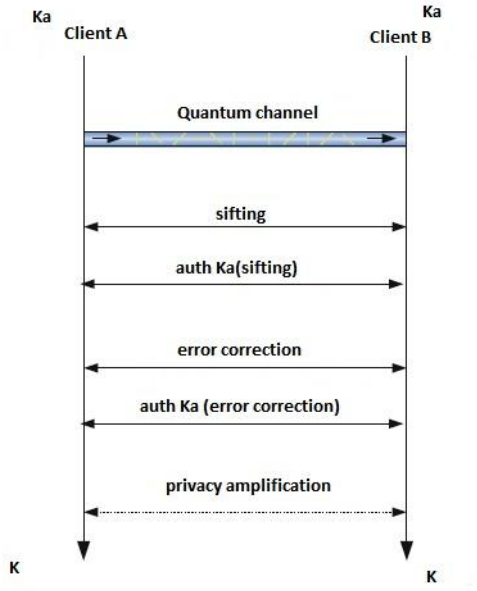

Fig 3. BB84. K_a is the pre-shared key. K is the generated key after protocol execution [15]

This message exchange must be authenticated to avoid the man-in-the-middle attack by the third person. After agreeing on the bits and being sure that the third person has not modified message by using an authentication scheme, Client A & client B go on to the error correction phase because the quantum channel is not a noiseless channel. Client A & client B do not share the same identical string. There is a small portion of errors in client B string which is corrected in this phase. Again the third person has the possibility to modify messages during this phase to her interest. Therefore client A & client B must authenticate this phase. After the authentication client A & client B shares a string, which is identical with very high probability, but this string cannot be used as a key yet. The third person information about the string must be considered. Client A has gained information

during the error correction and may be also during the quantum transmission. Hence Client A and Client B must map their string via a function to a smaller subset, so that the third person's knowledge decreases to zero. This stage is called privacy amplification and afterward client A and client B share a secret key only know by them.

3.4.1 The BB84 protocol without noise

The photons are very suitable for Quantum Key Distribution (QKD) because photons hardly interact with each other and they can overcome long distances with low loss in optical fibers. The polarization types are given below:-

- Rectilinear polarization

Horizontal Polarization	|↔>	0
Vertical Polarization	|↕>	1

The rectilinear polarization is denoted with the symbol +.

- Diagonal Polarization

Clockwise ($+45^o$)	|↗>	1
Anticlockwise ($+135^0$)	|↖>	0

The diagonal polarization is denoted with the symbol ×.

These two types are chosen because the Heisenberg uncertainty principle implies that the observation with respect to the + is incompatible to the ×.

To exchange the secret key in the BB84 protocol [12], client A and client B must do as follow:

STAGE 1 PROTOCOL: Communication over quantum channel

- Client A prepare photon randomly with either rectilinear (+) or diagonal polarization (×) therefore Client A transmit photons in the four polarization states \|↔>, \|↕>, \|↗>, and \|↖>.
- Client A records the polarization of each photon and sends it to Client B.
- Client B receives a photon and randomly records its polarization according to the rectilinear or diagonal basis. The Client B records the measurement type (basis used) and the resulting polarization measured. Client B doesn't know which of the measurement are deterministic, i.e. measured in the same basis as the one used by client A. Half the time Client B will be lucky and chose the same quantum alphabet as the third person. In this case, the bit resulting from his measurement will agree with the bit sent by Client A. However the other half time he will be unlucky and choose the alphabet not used by client A. In this case, the bit resulting from his measurement will agree with the bit sent by client A only 50% of the time. After all these measurement, client B now has in hand a binary sequence

Client A and Client B now proceed to communicate over the public two-way channel using the following stage 2 protocol.

STAGE 2 PROTOCOL: Communication over a public channel

Phase 1. Raw Key extraction

- Over the public channel, client B communicates to client A which quantum alphabet he used for each of his measurements.
- In response client A communicate to client B over the public channel which of his measurement were made correct alphabet.
- Client A and Client B then delete all bits for which they used incompatible quantum alphabet to produce their resulting raw keys. If the third person has not eavesdropped, then their resulting keys will be the same. If the third person has eavesdropped their resulting key will not be in total agreement.

A	+	×	×	×	+	×	+	×	+
	↕	↖	↖	↗	↕	↖	↔	↗	↔
	1	0	0	1	1	0	0	1	0

B	×	×	+	×	+	×	+	+	+
	1	0	1	1	1	0	0	0	0

Raw key		0		1	1	0	0		0

Fig 4. The BB84 protocol without the third person presents (No noise)

Phase 2**.** Error estimation

Over the public channel, Client A and client B compare small portion of their raw keys to estimate the error-rate R, and then delete the disclosed bits from their raw keys to produce their tentative final keys. If through their public disclosures Client A and Client B find no errors (i.e., R=0), then they know that the third person was not eavesdropping and that their tentative keys must be the same final key. If they discover at least one error during their public disclosures (i.e., R>0), then they know that the third person has been eavesdropping. In this case, they discard their tentative final keys and start all over again

3.4.2 The BB84 protocol with noise

Client A continues her presentation by addressing the issue of noise. "We must assume that client B's raw key is noisy. Since client B cannot distinguish between errors caused by noise and those caused by the third person's intrusion, the only practical working assumption he can adopt is that all errors are caused by the third person's eavesdropping. Under

this working assumption, the third person is always assumed to have some information about bits transmitted from client A to client B. Thus raw key is always only partially secret". We need a method to distill a smaller secret key from a larger partially secret key. We call this privacy amplification

STAGE 1 PROTOCOL: Communication over a quantum channel

This stage is exactly the same as before, except that errors are now also induced by noise.

STAGE 2 PROTOCOL: Communication over a public channel

Phase 1. Raw key extraction

This phase is exactly the same as in the noise free protocol, except that client A and client B also delete those bits locations at which client B should have received but did not receive a bit. Such "non-receptions" could be caused by the third person's intrusion.

Phase 2. Error estimation

Client A and Client B now use the public channel to estimate the error rate R in raw key and then delete the disclosed bits from their raw key to produce their tentative final keys. If R exceeds a certain threshold R_{max} then privacy amplification is not possible. If so clients A client B return to stage 1 to start over. On the other hand, if $R \leq R_{max}$ then client A and client B proceed to phase 3.

Phase 3. Extraction of reconciled key

Client A and client B remove all errors from what remains of raw key to produce an error free common key, called reconciled key [13].

Phase 4. Privacy amplification

Based on their error estimate R, Client A and Client B obtain an upper bound k of the number of bits Known by the third person of their n bits of reconciled key. Let s be a security parameter that client A and client B adjust as desired. Then they publicly select n-k-s random subsets of reconciled key, without revealing their contents, and without revealing their parities. The undisclosed parities become the common final secret key.

4. MATHEMATICAL ANALYSIS

In section 3.4 an eavesdropper may cause and injects some error due to the quantum states and may also from other cause i.e. the disturbance of quantum channel, optical misalignment or noise in the detector. In QC we refer to this Quantum Bit Error Rate (QBER). It is defined as following formula:

$$\text{QBER} = \frac{Number\ of\ errors}{Total\ number\ of\ bits} * 100\% \qquad (1)$$

As we also that error may also caused by technical, therefore QBER expressed as:

$$\text{QBER} = \text{QBER}_{opt} + \text{QBER}_{det} + \text{QBER}_{acc} \qquad (2)$$

The QBER_{opt} arises due to polarization or interference in the optical channel [14]. The QBER_{det} arises from the detector dark count and error counts can arise from uncorrelated photons i.e. QBER_{acc}

4.1 Measure of security

The QBER estimation process is crucial for the security of the QC system but we can't specify the level of security. In this section the security of QC in a quantitative way is considered. Let us assume we have a string of bits B which is an encryption key distributed by means of QKD protocol

$$B = [b_1, b2, b3 \ldots b_n] \qquad (3)$$

The key is distributed by means of quantum states of photons. Client A and Client B have to uncover some bits to know that nobody was eavesdropped. They uncover one bit the info about the security of key B is growing because the key length is n, the probability that we uncover bit b_i equal to $\frac{1}{n}$. Now assume J is a function which indicates the probability that key was not eavesdropped during the QKD process. Such function J could be measure the security of the binary string B because it directly influences data confidentiality.

Assume k is the number of uncovered bits the function J (k) is monotonously growing i.e. if k is growing than J (k) is also growing. It also implies that more bits are compared and we know about the security of distribute encryption key.

The function J (k) defined is as follows:

1) If we uncover 0 bits (minimum knowledge about security)
2) If we uncover all bits (maximum knowledge about security)

The function J (k) [14] can be defined in log function.

$$J(k) = \log_e \frac{k}{n} \qquad (4)$$

Where log represent the natural logarithm (with base e) and the constant e is called Euler's number (i.e. e = 2.71828). The Matlab code for the function J (k) where key is n=10000 bits as shown below.

```
n =10000;
K = [1: n];
J (k) = log (k/n);
Plot (k,J,'');
xlabel ('k');
ylabel ('J (k)');
```

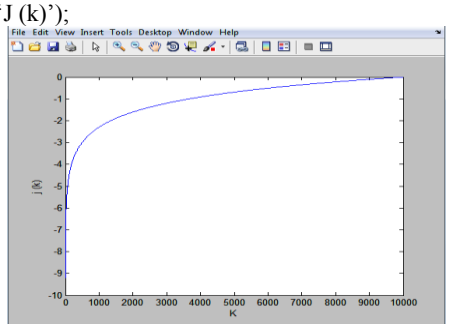

Fig 5. An example of function J (k) for key length: 10000 bits

In the Fig 5. It has following domain X and codomain Y:

$X \varepsilon \{1, 2, 3\ldots n\}$ and $Y \varepsilon \{ -\infty, 0 \}$ (5)

Now modify the function J (k) because of codamin. It is not be negative number. Therefore the function J (k) should be lie between 0 and 1 i.e. range is between 0% to 100%.

$$J(k) = \frac{\log(k+1)}{\log(n+1)} \quad (6)$$

Or it can be written as:

$$J(k) = \log_{n+1} k + 1 \quad (7)$$

The Matlab code for the function J (k) in equation (7) where key is n=10000 bits as shown below.

```
n =10000;
K = [1: n];
J (k) = log 1p (k) / log 1p (n);
Plot (k, J,'');
xlabel ('k');
ylabel ('J (k)');
```

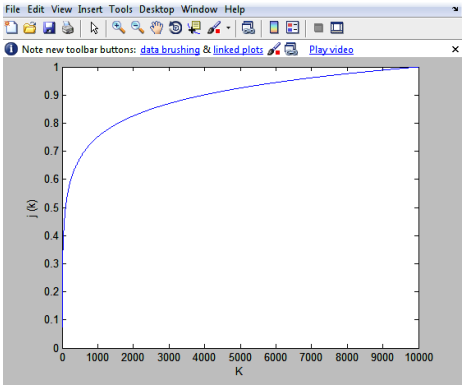

Fig 6. An example of function J (k) for key length: 10000 bits

It show that security of QC depend on the number of uncovered bits and compared bits (k).

4.2 Entropy of security

By analogy to the Shannon's entropy of security is defined as

$$S(\varphi) = -\sum_{k=1}^{n} p_k * J(k) \quad (8)$$

Or it can be written as

$$S(\varphi) = -\sum_{k=1}^{n} \frac{k}{n} * \log \frac{k}{n} \quad (9)$$

S (φ) defines the average security of the key when we uncover and compare k bits. Negative sign in equation (9) indicates the positive value of S (φ). Also the function of the entropy of the security is defined as

$$S(k) = -p_k * J(k) = -\frac{k}{n} \log \frac{k}{n} \quad (10)$$

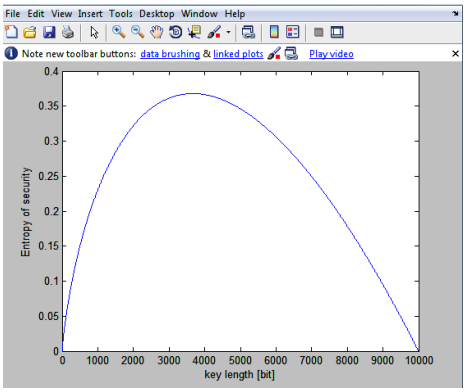

Fig 7. An example of function S (k) for key length 10000 bits

The Matlab code for the function S (φ) in equation (10) where key is n=10000 bits as shown below.

```
n =10000;
J =Zeros (1, n);
a = [1:n];
K = 1;
While k<=n;
J (k) = (-1) * (k/n) * log (k/n);
k = k + 1;
end
Plot (a, J,'');
xlabel ('key length [bit]');
ylabel ('entropy of security');
```

The function S (k) defined in Equation (10) has one global maximum i.e.

$$S`(k) = \frac{d}{dk} S(k) \quad (11)$$

By solving equation (11) we get

$$S`(k) = -\frac{1}{n} - \frac{1}{n} \log \frac{k}{n} \quad (12)$$

And equate this derivative to 0;

$S`(k) = 0$

We get $K = ne^{-1}$

$$K = \frac{n}{e} \quad (13)$$

Therefore we able to define that the maximum of the function of entropy of security is always equal to $\frac{n}{e}$. Now divide the maximum of the function by n (The number of bits).

$$K \sim \frac{1}{e} = 0.3678$$

It means that maximum function corresponding to this situation when we uncover and compare 37% bits of the key.

5. CONCLUSION

Nowadays, the interest in Quantum cryptography is rapidly growing. Securing data and data communication is a top priority on both economy and national security. Quantum cryptography provides more security level then any classical

cryptosystem. This paper reveals on the security level that only 37% bits is enough to collect information about security of a distributed key for maximum security in quantum cryptographic communication network.

6. FUTURE WORK

In general cases in Quantum key distribution, distance is limited to tens of kilometers because in optical communication data amplification destroys qubit state, and there is a paramount need of such a device which may generate detect and to guide photons too. One can add further advance functions to enhance the security and can also add hash function to the privacy amplification to reduce the probability of occurrence of error bits.

7. REFERENCES

[1] M.Niemiec, "Design Construction and Verification of a High-level Security Protocol Allowing to Apply the Quantum Cryptography in Communication Networks", 2011, Ph.D. Thesis, AGH University Of Science and Technology, Poland.

[2] 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.

[3] M.Niemiec, "D8.6 specification & Evaluation of quantum cryptography for security & privacy assurance"2012, AGH University of Science and Technology, Poland.

[4] T.Godhavari and N.R.Alamelu, "Quantum based secure information transmission", European journal of scientific research, ISSN 1450-216X, Vol.66.No2 (2011) pp243-254

[5] D.Dieks,"Communication by EPR Devices", Physics Letters A, vol.92, No.6, 1982 pp.271-272.

[6] Wootters, W.K., and W.H. Zurek, "A Single quantum cannot be cloned", Nature, 299, pp.982-983, 1982.

[7] G. Brassard and L. Salvail "Secret key reconciliation by Public discussion", Advances in Cryptology: Eurocrypt 93 Proc. Pp.410-23, 1993.

[8] C. Gobby, Z. L. Yuan and A. J. Shields, "Quantum key distribution over 122 km telecom fiber", Appl. Phys. Lett. 84, pp.3762–3764, 2002.

[9] D. Gottesman, H. K. Lo, N. Lutkenhaus and J. Preskill, "Security of quantum key distribution with imperfect devices", Quantum Information Computation. 4, pp.325–360, 2004.

[10] K. J. Gordon, V. Fernandez, G. S. Buller, I. Rech, S. D. Cova and P. D. Townsend, "Quantum key distribution system clocked at 2 GHz," Optics Express 13, pp.3015–3020, 2005.

[11] C. H. Bennett: "Quantum cryptography using any two non orthogonal states", Physical Review Letters, Vol.68, No.21, 25, pp.3121-3124, 1992.

[12] F. Henle, BB84 online demo <http://monet.mercersburg.edu/henle/bb84/>. An online demonstration of the original BB84 algorithm from, Bennett et al. 1991.

[13] Jacobs, B.C and J.D Franson, "Quantum cryptography in free space", Optics Letters, Vol. 21, pp.1854-1856, 1996.

[14] R.J. Hughes, G.G. Luther, G.L.Morgan, C.G. Peterson and C. Simmons "Quantum Cryptography over underground optical fibres", Advances in Cryptology: Proceeding of CRYPTO'96.

[15] C. Kollmitzer, M. Pivk, "Applied Quantum Cryptography", Lect. Notes Phys. 797, Published in Springer, Berlin Heidelberg 2010.

[16] R. Pike and B. Labs, "An Introduction to Quantum Computation and Quantum Communication", Published by Lucent Technologies.

[17]MathWorkswebside.http://www.mathworks.com