

# Quantum Key Distribution System

Sudeshna Ghosh<sup>1</sup>, Abhisinchan Ghosh<sup>2</sup>, Debabrata Sarkar<sup>3</sup>

M.Sc, Department of Computer Science, Visva Bharati, West Bengal, India<sup>1</sup>

M.Sc, Department of Computer Science, Visva Bharati, West Bengal, India<sup>2</sup>

B.Tech, Department of Computer Science and Engineering, Guru Nanak Institute of Technology, West Bengal, India<sup>3</sup>

**ABSTRACT:** The present work would like to highlight in the application and utilization of the quantum cryptography for fully security to transmit the important data. There are two keys in the classical cryptography system, one is public key and another is private key. The receiver only knows the public key. But the encrypted data is larger than the key. So it is too easy to attack. But the quantum key is with the same length as the data which is encrypted. So I generalized quantum cryptography system with the help of distribution of the quantum key, this is hypothetical approach.

**KEYWORDS:** Classical Cryptography, BB84, Quantum key.

## I. INTRODUCTION

Cryptography has many significant importance in our daily life, for example to source internet connections and bank transfers, and in various other critical applications like control satellites. So in many purpose cryptography makes an important role. As there are many successful attacks on classical cryptographic systems, Quantum key Distribution (QKD) systems offer the prospect of a provable secure cryptographic channel. At first there one brief discussion about classical cryptography with its deficiencies and after then how quantum cryptography avoid these that is discussed. The experimental setup of quantum key distribution system is also introduced and at last it is described.

## II. CLASSICAL CRYPTOGRAPHY

Basically Classical Cryptography is one NP-hardness mathematical problem-like example factoring of two very big prime numbers. These problems in one side easy to compute but in another way to compute reverse of it is very difficult without some perfect information. Classical Cryptography has two types

1. Symmetric Cryptography –In this cryptography only one secret key [1] is used in the case of encryption and decryption.
2. Asymmetric Cryptography-It is one type of cryptography used with public key which consists of private and public keys in the case of encryption and decryption.

Deficiencies of Classical Cryptographical problems

As the key is shorter than encrypted data so all classical [2] cryptographic systems can be broken. All the existing cryptographic systems would be easy to attack when one quantum computer was created and they are become practically worthless.

The information is encoded by Quantum key Distribution system in single photons. It will solve the problem of cryptography key distribution with high security and allowing secure communication.

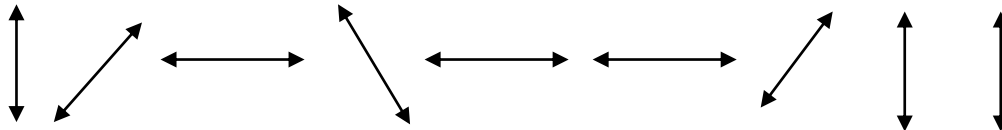
## III. BB84 –PROTOCOL



There are two different basis sets in BB84 protocol. They are linear and circular polarized light and in per basis set there are two orthogonal states. Vertical and horizontal polarised light for first basis and for second basis there's left and right handed circular polarized light. Between two people, "Alice"[3] select one basis sets randomly and

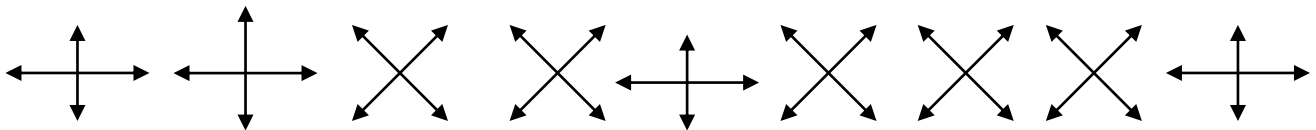
transmitted bit. In other side “Bob”[3] randomly chooses basis set and polarization set is measured in this basis set. Here Bob tells Alice about his used basis set for decoding and the position of the bits is told by Alice such that Bob can use same basis set to decode. And encoding is done by Alice.

#### IV. QUANTUM KEY DISTRIBUTION SYSTEM

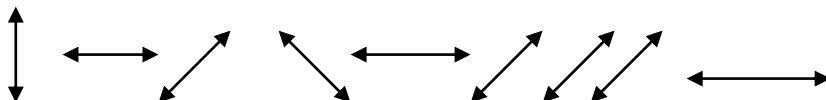
In this cryptography system two people are allowed, “Alice” and “Bob”, exchange a secret key. A transmitter is used by Alice for sending photons in one of four polarizations :  $0^{\circ}, 45^{\circ}, 90^{\circ}, 135^{\circ}$ . Bob uses a receiver to compute each polarization n either the rectilinear basis which is 0 or 90 or which is 45 or 135; according to the laws of quantum mechanics he cannot simultaneously make both measurements. There are several steps [4] in key distribution. Alice sends photons with one of four polarizations, which she [5] chooses as random.



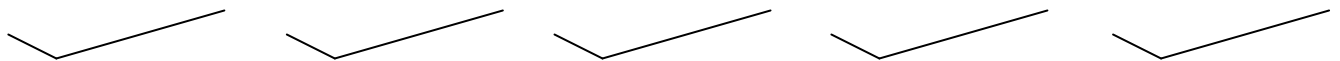
[6] In case of every photon, Bob measures randomly : either the rectilinear type (  ) or diagonal type (  )



The measurement of result is recorded by Bob but it is kept secretly.



When the transmission is over, Alice does not get any result by Bob, only get the measurement types and Bob only get which were correct for photons. This is an overhead exchange.



Alice and Bob keep all cases and in between them the correct polarization should be measured by Bob. And to define the key the cases are translated these convert into bits. At random to reveal some bits are chosen by Alice and Bob. If they support it, the remaining have not been prevented with assurance. The behaviour of photons sent through a series of polarizer's that is described below:

- Let,
- R = An apparatus measures rectilinear polarization
  - V = Vertical polarization
  - H = Horizontal polarization
  - C = Circular polarization measurement device
  - L = Circular polarization (Left)
  - R = Circular polarization (Right)

1. At first through a rectilinear (R) measurement apparatus a photon is sent and it is polarized vertically or horizontally with equal probability[7].

**International Journal of Innovative Research in Science, Engineering and Technology**

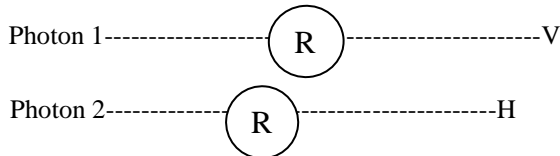
An ISO 3297: 2007 Certified Organization

Volume 4, Special Issue 9, July 2015

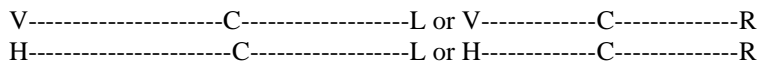
**National Conference on Emerging Technology and Applied Sciences-2015 (NCETAS 2015)**

**On 21<sup>st</sup> & 22<sup>nd</sup> February, Organized by**

**Modern Institute of Engineering and Technology, Bandel, Hooghly-712123, West Bengal, India**



2. A photon that was measured in vertical or horizontal which is polarized and sent through an apparatus to measure its circular polarization. The photon has equal probability of being polarized in either left-circular or right-circular.



3. When one circular polarized photon was sent through a rectilinear measurement Apparatus then analogous [8] result would occur.

In the other words we describe the quantum key distribution using BB84 Scheme given bellow in the tabular form:

Left circular=0 Right-circular=1  
Horizontal=0, Vertical=1

Using online demonstration program the following table was generated considering the Alice sends twelve photons

Step	Description	1	2	3	4	5	6	7	8	9	10	11	12
1.	Apparatus used by Alice to prepare photons	R	R	C	R	C	C	C	R	R	R	C	C
2.	Alice send the Polarization of photons	V	H	L	H	R	L	R	V	H	H	R	L
3.a	Bob makes Measurement types	R	R	R	R	C	C	C	C	R	C	C	R
3.b	Bob's measurement Result	V	H	H	H	R	L	R	L	H	L	R	H
4.	Bob informs Alice Publicly which type measurement he makes on each photon	R	R	R	R	C	C	C	C	R	C	C	R
5.	Alice publicly tells Bob which measurement type is correct	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes	No	Yes	No
6.	From correct measurement Each of Alice and Bob keeps the data and it converts binary	1	0		0	1	0	1		0		1	

Here if eves dropping is occurred during Alice and Bobs transmission, eaves dropping does not compromised the security of keys of development using quantum cryptography because transmission between Alice and Bob take place on two separate channels. Transmission of photons are quantum in nature and take place on a quantum channel, such as optical fibre. The conversation between Bob and Alice about the measurement types is made on classical channel, such as telephone or email.

Without detection Eve can cut off transmitted information. It is not a problem in Quantum Cryptography because in this protocol the information Bob and Alice exchange is the measurement type they made not result of the measurement and therefore nothing about the key that was developed.

Suppose Eve hears on a quantum channel. She performs this by reading some photons from the burst send from Alice to Bob. Now ,Eve has photon which are same in polarization with those received by Bob, and she randomly choose her own

## International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization

Volume 4, Special Issue 9, July 2015

National Conference on Emerging Technology and Applied Sciences-2015 (NCETAS 2015)

On 21<sup>st</sup> & 22<sup>nd</sup> February, Organized by

Modern Institute of Engineering and Technology, Bandel, Hooghly-712123, West Bengal, India

measurement type as she does not know what measurement type Bob is going to use. Assume Alice sends circularly polarized photon, which are received by Bob and Eve. Eve and Bob decide to use rectilinear and circular bases for measurement respectively. Here Bob and Alice record the resulting data as they both use same basis but Eve does not know their result since she used the wrong basis. Now Eve decided to handle the circular basis and Bob the rectilinear basis to measure it, then Eve would have the same result that Alice sent and Bob would throw the results out since Bob did not choose the correct basis. So Eve will not finish up with anything resembling to the string of bit that Alice and Bob create.

### V. ADVANTAGE AND DISADVANTAGE

**Advantage:** Lasers and optical attenuators are commercially available at affordable and can operate at high bit rates.

**Disadvantage:** A QKD system commits that only single photons are transmitted, otherwise the system is vulnerable to beam-splitting attacks.

### VI. CONCLUSION

Although a fair amount of research was done on the single photon sources, little real progress could be achieved within the scope of this project. Probably, future growth in the work of individual photon sources other than weak coherent sources will improve the security of the QKD systems. In the field of data analysis, this project can be considered to be rather successful.

### REFERENCES

- [1] High Bit Rate Quantum Key Distribution Systems 5<sup>th</sup> Year Project Report qkd-lenz.pdf
- [2] A SURVEY OF QUANTUM AND CLASSICAL CRYPTOGRAPHY <http://www.ccsc.org/southcentral/E-Journal/2008/Papers/P-0006-final.pdf>
- [3] Computer Networks & Computer Security <http://www4.ncsu.edu/~kksivara/sfwr4c03/lectures/lecture10.pdf>
- [4] University of Cambridge. [www.qi.damtp.cam.ac.uk/node/38](http://www.qi.damtp.cam.ac.uk/node/38)
- [5] Quantum Cryptography and Privacy Amplification <http://www.ai.sri.com/~goldwate/quantum.html>
- [6] Released October 2002. [www.csa.com/discoveryguides/crypt/overview.php](http://www.csa.com/discoveryguides/crypt/overview.php) Quantum Cryptography : Privacy through Uncertainty
- [7] Quantum Cryptography <http://www.scienceintegration.org/concepts/quantumcryptography.pdf>
- [8] Quantum Cryptography <http://www.scienceintegration.org/concepts/quantumcryptography.pdf>