© 2014 IJSRSET | Volume 1 | Issue 1 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

# Quantum Cryptography : A Comprehensive Study

**Bhavesh Prajapati**
Assistant Professor, IT Department, L. D. College of Engineering, Ahmedabad, Gujarat, India

## ABSTRACT

Quantum Cryptography is an applied branch of optical physics to establish a cryptosystem, which is future ready. Secrecy is need of today's digitally growing world. Classical cryptography depends on mathematical functions and computational security of those functions. Modern cryptography can be defeated by increasing computing power day-by-day and hence no more future secure. Due to said reason quantum cryptography is gaining much importance among IT security practitioners. Word "Quantum" means the smallest particle of matter and energy, which inhibits some special behavior. This paper discusses basic underlying principles of Quantum Cryptography like Heisenberg's uncertainty principle and different characteristics of photon polarization. Quantum cryptography is combination of dominant physics with mathematics as a key aspect to generate security model.

**Keywords :** Classical Cryptography, Quantum Cryptography, Encryption, Decryption

## I. INTRODUCTION

Let us start with famous quotes of two great scientists. Niel Bohr's quote "Those who are not shocked when they first come across quantum theory cannot possibly have understood it" and Albert Einstein's claim that "God does not play dice". This suggests that one need to think differently from classical way of thinking to digest the behavior of quantum physics. Today quantum cryptography threatening the security achieved by classical cryptography. In 1994, Peter Shor published factoring algorithm for large prime numbers which alerted classical cryptographers and security experts because it can ruin the PKI(Public Key Infrastructure) as it is based on difficulty of factoring out large prime numbers using RSA. Today's cryptosystems are computationally secure and classical computer can take billions of years to break the system. But quantum computer can break such cryptosystems in seconds.

## II. CLASSICAL CRYPTOGRAPHY

Classical cryptography depends on secrecy of key not on secrecy of encryption and decryption process. Key should be long enough and random to guess. The idea of computationally secure means time required to break the system must be longer then the expiry of usefulness of that information. For discussing further let us consider two parties Alice and Bob involved in communication. Eve is the eavesdropper.

One approach of such cryptosystem is Symmetric cryptosystem or Secret key cryptosystem, which uses a single common key for encryption and decryption at both ends. Such systems are simple and fast enough but main problem is secure key transfer.

Another approach is Asymmetrical cryptosystem or public key cryptography in which two keys(public and private) are used to encrypt and decrypt messages. The key is large mathematically related numbers. One

key can be shared with anyone known as public key while other key is kept secret known as secret key.

## III. QUANTUM CRYPTOGRAPHY

Quantum physics inhibits some typical properties which cannot be easily explained by normal physics. For example:

- ✓ The no-cloning theorem states that one cannot create a copy of an unknown quantum state or qubit.
- ✓ One cannot measure a system without disturbing it.
- ✓ The uncertainty principle states that one cannot simultaneously measure two properties (such as position and momentum of a particle) with arbitrarily high precision.

Above characteristics can be considered negative but these drawbacks are turned into positive applications for quantum cryptography. Heisenberg Uncertainty principle says that we cannot measure quantum state of system without disturbing it. So when light particle is polarized, we can know the polarization only at the time of measuring it.

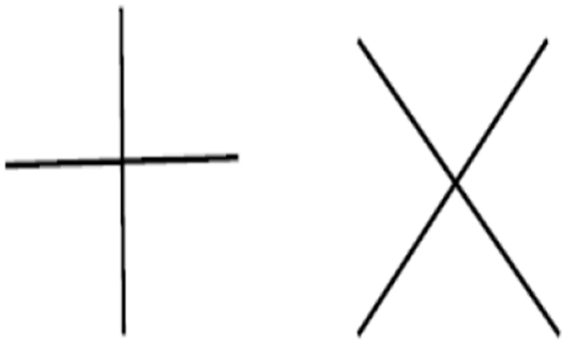

Fig. 1. Rectilinear and Diagonal bases

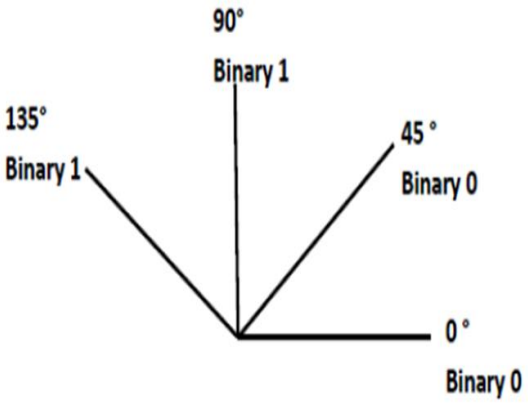


Fig. 2. Polarization of photons to represent bits

Polarization is the direction of electromagnetic field that a quantum bit has as shown in Figure 1 and Figure 2. This uncertainty principle plays a critical role when eavesdropper tries to measure the polarization of quantum bits. Now to detect the polarization of photon we need filter with correct polarization angle else photon will be destroyed. This properties make quantum physics most suitable choice for cryptography.

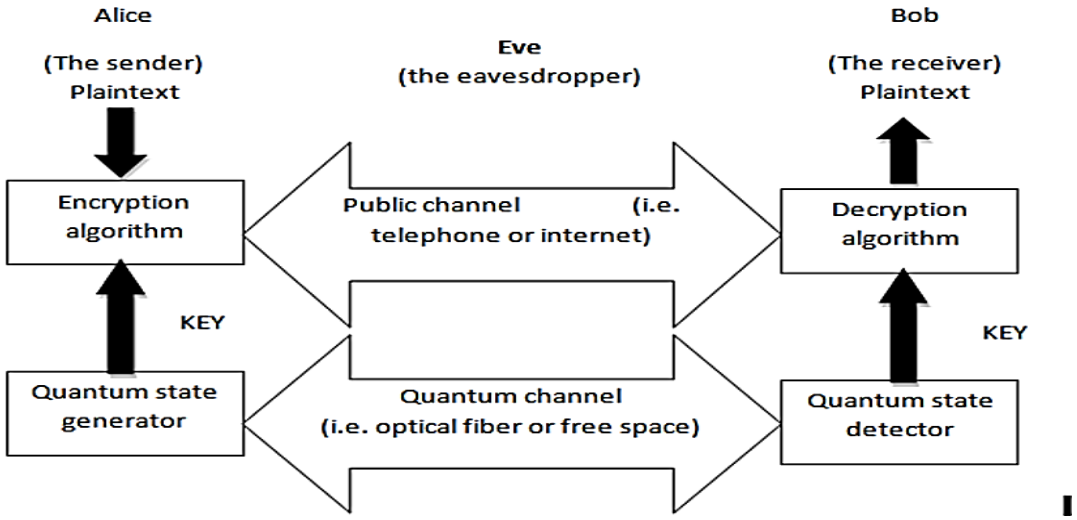


**Figure 3.** Quantum cryptographic communication System for securely transferring Random key

Charles H. Bennet and Gilles Brassard developed the concept of quantum cryptography in 1984. Bennet and Brassad stated that an encryption key can be created depending on the amount of photons reaching a recipient and how they were received. Photons can be polarized for different angles and these orientation can be used to represent information in form of zero and one. In a way a system for producing and delivering key in secure way can be developed. The representation of bits through orientation of polarized bits is base of quantum cryptography. Classical cryptography depends on computational limitations while quantum cryptography depends on basic rules of physics and not on processing power of computations.

Let us understand use of quantum cryptography to distribute keys. This includes a sender, "Alice", a receiver, "Bob". Alice sends a message to Bob using a photon gun to send a stream of photons randomly chosen in one of four polarizations that correspond to vertical, horizontal or diagonal in opposing directions (0,45,90 or 135 degrees).

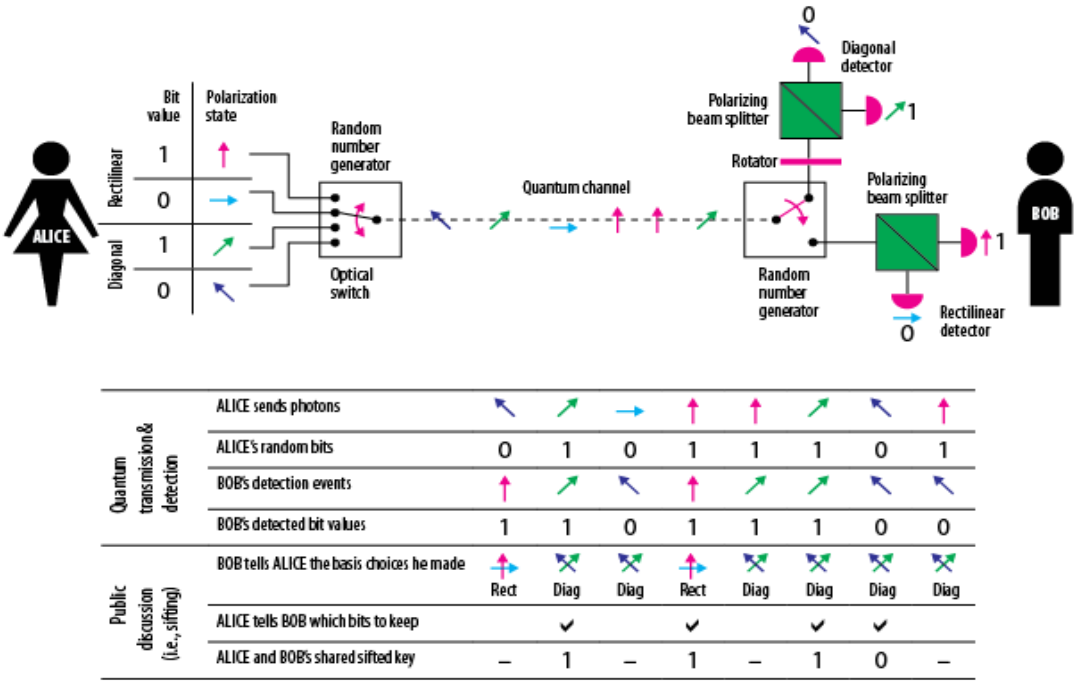


**Figure 4.** Key generation process Image source: UNS Nice (France), Department of Physics

Bob receives each photon from stream and chooses a random filter to measure the polarization of received photon, whether it is in rectilinear (0 or 90 degrees) or diagonal (45 or 135 degrees) bases. Bob also keeps record of results of which measurements are correct with reference to Alice's selection. All photons will not reach to Bob due to distance and noise.

Alice and Bob discusses over pubic channel about types of measurements done, which bases are used and which photons are registered. The in correctly measured photons were discarded. While correctly measured photons are converted in to bits based on their polarization.

Here Alice and Bob cannot determine the key in advance as key is generated based on their random choices of polarization angles and correctly received bits. In a way quantum cryptography makes secure distribution of keys possible.

So far, so nice. But what about attacker? Let us assume the obvious possibility of attacker try to gain the key from quantum key distribution system. Let us name this malicious attacker "Eve". When Eve tries to measure , she have equal chance of selecting the correct filter as Bob have but will not be able to confirm with Alice regarding her choice of bases. Eve may try when Alice and Bob are confirming with each other about the matching bases used for measurements. But still this information is of no use as Eve does not know the exact polarization used by Alice for each photon. Due to this Eve will never be able to gain the correct key.

As per Heisenberg Uncertainty principle, we cannot copy quantum bit as when we try to measure it, its state will be changed. Alice and Bob need to fix the number of photons required to be communicated to generate a key before starting a procedure. Mathematically Bob should receive at least twenty five percent of photons correctly if they are not sniffed in between. If Eve detects a photon she cannot pass the same to Bob as she cannot copy the photon. And if Eve sends her own photons with randomly chosen orientation error rate will increase suggesting presence of malicious attacker.

## IV. CONCLUSION

Classical cryptography is computationally secure and depends on advances on technology to remain secure. Quantum cryptography is secure technique based on laws of physics. There are still some short comings like point to point link and denial of service, losses in quantum channel, high bit error rate, low key distribution rate, photon detectors inaccuracy, sending of one single photon of light at a time, classical authentication and distance limitation. This paper discusses fundamentals of quantum cryptography and in future low cost implementation of quantum cryptography will be feasible with relatively less short comings.

## V. REFERENCES


[1]. Vittorio, S., 2002, "Quantum Cryptography: Privacy Through Uncertainty" http://www.csa.com/discoveryguides/crypt/overview.php

[2]. Id Quantique White Paper, 2005, "Understanding Quantum Cryptography" http://www.idquantique.com/products/files/vectis-understanding.pdf

[3]. Ford, J., 1996, "Quantum Cryptography Tutorial" http://www.cs.dartmouth.edu/~jford/crypto.html#1

[4]. Bennett, C.H., Brassard, G., 1984, "Quantum Cryptography: Public Key Distribution and Coin Tossing"

[5]. Bennett, C.H., 1992,"Quantum Cryptography: Uncertainty in the Service of Privacy"

[6]. Papanikolaou, N., 2004, "Techniques For Design And Validation Of Quantum Protocols"

[7]. Goldwater, S., 1996, "Quantum Cryptography and Privacy Amplification" http://www.ai.sri.com/~goldwate/quantum.html
[8]. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H., 2004 , "Quantum cryptography"
[9]. Fuchs, C. A., Gisin, N., Grıffiths, R. B., Niu, C. S., Peres, A. , 1997, "Optimal Eavesdropping In Quantum Cryptography. I. Information bound and optimal strategy"
[10]. Petra Pajic, 2013, "Quantum Cryptography"
[11]. D.J. Bernstein, 2009 Post-Quantum Cryptography, Springer,