International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.04, March 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

A Review Paper on Quantum Cryptography

Daljinder Kaur[1], Astha[2]

[1]*Computer Science and Technology, Central University of Punjab, Bathinda, India*
[2]*Computer Science and Technology, Central University of Punjab, Bathinda, India*

ABSTRACT

Cryptography is the method of hiding the information from unprivileged access to ensure integrity and privacy of the data. It is the strongest tool to meet the security aspects like confidentiality, integrity and availability of data. Cryptography plays the vital role in every secured area like banks, government agencies, telecommunications companies and other corporations who indulge in handling sensitive data. Quantum cryptography is one of the emerging technologies which use quantum physics to generate and share the secret key as opposed to the classical methods that use mathematical formulae to do this between two communicating parties. It addresses the problem of secure key distribution as it offers thoroughly secure communication based on quantum mechanics. This paper is dwelled with the main concepts of Quantum cryptography and the algorithms used in quantum cryptography.

Keywords: BB84 Algorithm, B92 Algorithm, Cryptography, Key Distribution, Quantum Cryptography

I INTRODUCTION

With the emergence of technology and business data has become the most crucial part to be handled. Data is transferred over the internet over insecure channel that make it easy for the adversary to conceal the data and to modify the data. So there is needed to handle and transfer data accurately to ensure the three aspects of security that include confidentiality, integrity and availability. Confidentiality ensures that data is accessed by intended users only. Integrity includes the correctness of data and data to be modified by authorized user. Availability includes the accessibility of data when required[1].

Cryptography in Fig.1 is one of the techniques that include the study and application of methods to hide the data. This helps in meeting the security parameters. Classical cryptography is used to meet this objective by encrypting the plain text into cipher text using mathematical algorithm and calculations, sending the cipher over insecure channel and then decrypting the cipher text at receiver side. The algorithm used for encryption is called cipher. Cryptography includes two processes: encryption and decryption. At the sender side the plain text is encrypted into cipher text using key and encryption and send over the insecure channel. At the recipient side the cipher text is decrypted using the key and decryption algorithm to get the plain text. Different types of

algorithms are available like public key cryptography, secret key cryptography and hash functions. Whatever the algorithm is used for encryption, problem arises during the distribution of the key among communicating parties known as Key distribution problem. These algorithms generate the key which can be broken easily by using powerful computers and inverse mathematical computations. The quantum cryptography can seriously threat the traditional methods of security. The next sections discuss the problems with the traditional methods and the quantum cryptography concepts with algorithm [1].

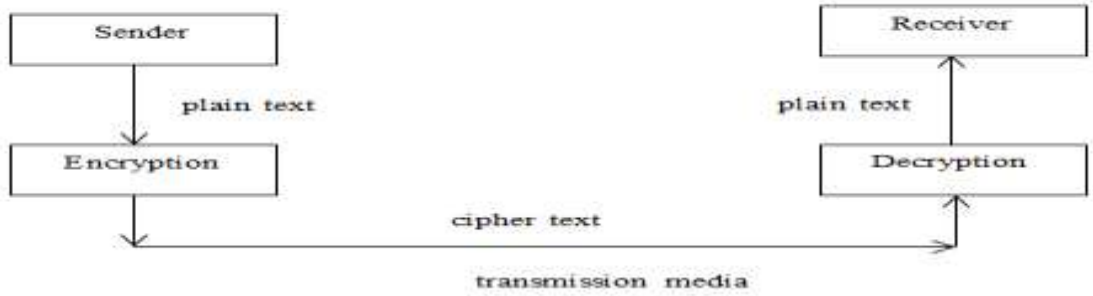

Fig1. Cryptography

II PROBLEMS WITH TRADITIONAL CRYPTOGRAPHY METHODS

Classical cryptography contributes to the number of applications like secure communication, key exchange, identification and authentication, digital signatures and data integrity, electronic commerce, certification authority, zero-knowledge and secret sharing. The security of all these applications relies on some often believable hard problems. All classical cryptographic methods: Substitution methods as ceaser cipher, monoalphabetic and polyalphabetic substitution method, and Transposition methods as rail fence methods are prune to attack of breaking the key.

Therefore, the concept of one time pad is used as in vernam cipher. The key is kept as long as plain text and key generated once is never used again. Key is very difficult to break. The one pad key method also suffer from a problem called key distribution problem [2]**.** Communicating users have to agree in advance and secretly on the key. When this is shared key can be used for enciphering and deciphering. The resulting cipher information can be transmitted publicly, for example: broadcasting by radio without compromising the security. The foremost work is establishment of key over a secure for example: a private meeting, a very secure telephone line. A Secure channel is usually available at specific times and under certain circumstances. Although a secure channel is available, this security can never be fully guaranteed. This is because, in principle, the classical private channel can be monitored passively, without in the knowledge of the sender or receiver that eavesdropping has taken place. This is due to classical physics - the theory of ordinary-scale bodies and phenomena such as magnetic tapes, radio signals- allows all physical to measure the physical properties of the object without disturbing those properties. All the information, including cryptographic keys, is encoded in

measurable physical properties of object or signal. Thus classical theory provides the possibility of passive eavesdropping. This is not the case in quantum theory that forms the basis for quantum cryptography [3].

III QUANTUM CRYPTOGRAPHY

Quantum cryptography also known as Quantum Key Distribution(QKD), is the method where quantum systems are used to do cryptographic tasks for example: - quantum key distribution (QKD) which makes use of quantum mechanics for secure communication. It allows two communicating parties to generate a shared random bit string, known only to them and used to encrypt and decrypt messages [2].

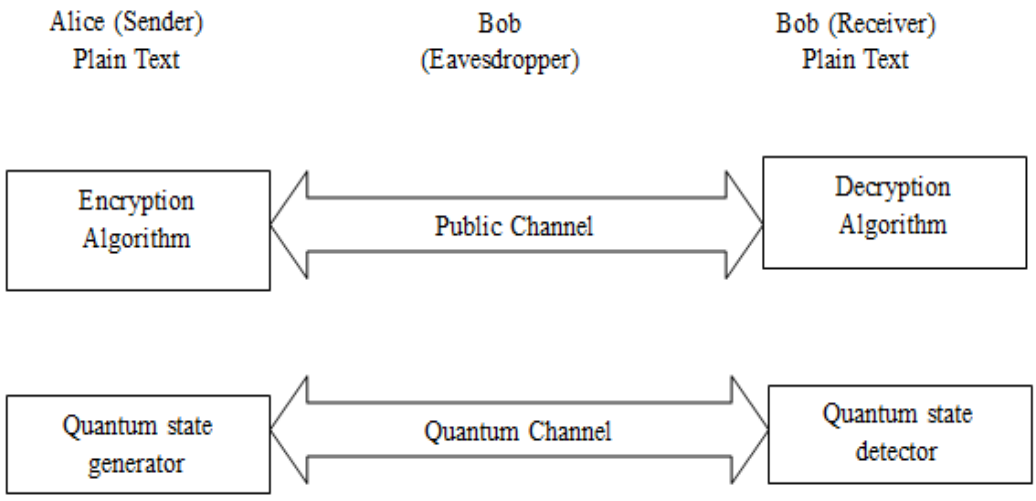

Fig2. Quantum communication [4]

The most significant and unique property of quantum cryptography lies in the fact that it detects the intervention of any third party to gain knowledge of the key. This is the fundamental aspect of quantum mechanics that is the process of measuring a quantum system in general disturbs the system. The adversary eavesdropping on the key is trying to measure it, thus generating detectable anomalies. The use of quantum super positions and transmitting information in quantum states allows developing a communication system as in Fig2. capable of detecting eavesdropping. If the level of eavesdropping falls below some threshold value then key produced is guaranteed to be secure otherwise secure key is not possible and communication is aborted. Quantum cryptography is used to produce and distribute a key but not to transmit any message data. This key is used with chosen encryption and decryption algorithm and then message is transferred over the secure communication channel. One-time pad algorithm is commonly used with QKD as it is certain secure when used with a secret and random key. In this the term qu-bits is used instead of bits. This is done by using polarizers that are bit readers, which allow the photons of certain polarization to enter and block the others [9]. If a photon

enters the wrong decoder then it is interpreted as a 0 or else 1. Thus, a photon can be assumed to be in two states simultaneously. Quantum cryptography is based on two major principles: Polarization of light and Heisenberg's uncertainty principle [5].

Polarization: Light waves are composed of millions of discrete quanta known as Photons. These photons are mass less and have energy, momentum and angular momentum called spin. Polarization is carried by spin. These photons are indivisible like atoms. These can be polarized from 0^0 to $360^0$and intermediate spin positions like 45^0 or 90^0can be detected using filters inclined to certain directions.

Heisenberg's uncertainty principle: This states that it is not possible to know the position and momentum of particle simultaneously. When the information is encoded in the properties of a photon, any attempt to monitor the photon will change the properties and are detectable. It is based on quantum theory that suggests certain pairs of physical properties are complementary such that measuring one will change the other.

Different basis are used to secure the secret key. Basis is the pair of polarization states that describe polarization such as horizontal or vertical [6].

- | - denotes a photon in vertically polarized state.
- . - denotes a photon in horizontally polarized state.
- / - photon in a 45 degree polarized state.
- \ - photon in a 135 degree polarized state.
- + - denotes the pair of states {|, .}, also called as the +- basis.
- X - denotes the pair of states {\, /}, also called as the x-basis.

3.1 Steps in quantum cryptography

Sending

i. Data is converted into bits and Alice determines the polarization way horizontal, vertical, left or right circular.

ii. Laser source produce the polarized photons. Ideally each pulse is composed of one photon. In actual, it is beam of light of low intensity. Intensity is needed to regulate carefully.

Receiving and converting

iii. Bob generates randomly a sequence of bases either rectangular or circular and measure polarization of each photon.

iv. Bob shared the sequence of base publicly to the Alice, and Alice respond back with chosen base.

v. Alice and Bob discard the non-required observations and chosen observations are converted into binary.

Correcting errors

vi. Alice and Bob agreed on random permutation of bits to make the position of errors randomized

vii. Strings are partitioned into block of size s, where s is so chosen to make the probability of multiple errors per block very less.

viii. Alice and Bob create and exchange parities of each block by dropping last bit of each for security aspects.

ix. Block which is different at both sides is broken down to locate the error.

x. Repeat above steps by increasing block size value k to discover undetected errors within original blocks

xi. To determine additional errors Alice and Bob do another randomized check. After r repetitions they infer that string disagree with probability of (1/2) r which can be decreased by increasing r. [6,7]

IV QUANTUM KEY DISTRIBUTION BB84 PROTOCOL:

Benett and Brassard proposed protocol in 1994 to exchange key before communication. This protocol is known as BB84 in Fig3. Each photon is carrying one qu-bit of information. Polarization represents 0 or 1. Alice suggests a key by sending a stream of randomly polarized photons converted to a binary key. To ensure consistency Alice and Bob agreed upon a random subset of the bits to compare. If the key is found to be intercepted then discarded and a new stream of randomly polarized photons sent. Any two pairs of conjugate states are used for the protocol. [3]

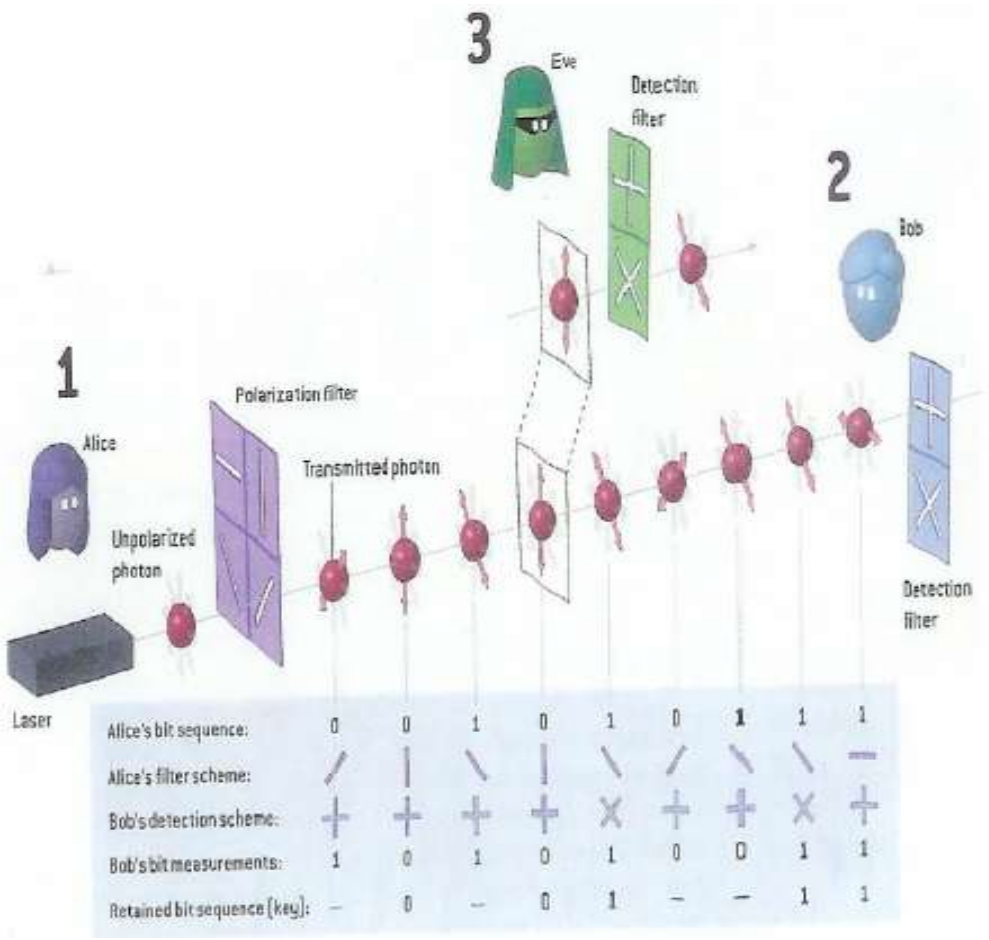

Fig3. Quantum Communication Using BB84 [10]

4.1 Steps of the algorithm

- Alice using laser, creates a photon and then send through the polarizer. Photon is given one out of four possible polarizations in Fig4. and bit designations — Vertical (One bit), Horizontal (Zero bit), 45 degree right (One bit), or 45 degree left (Zero bit) randomly
- Photon travels towards Bob. Bob is accustomed with two beam splitters: a diagonal and vertical/horizontal and two photon detectors.

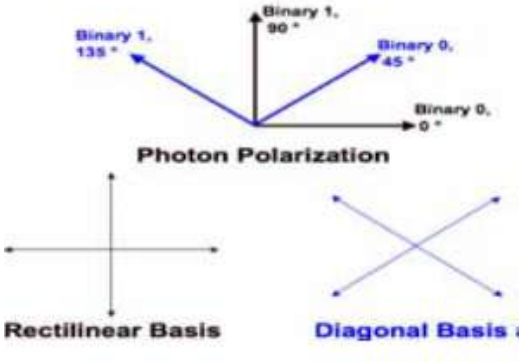

Fig4. BB84 bit encoding [5]

- Bob randomly chooses one beam splitters and checks the photon detectors.
- The process is repeated till the entire key has not been transmitted to Bob.
- Bob confirms Alice in sequence about the beam splitter he used.
- Alice compares this information with the sequence of polarizers used by her to send key
- Alice confirms Bob the position in the sequence of sent photons where he used the right beam splitter.

Now both have a sequence of bits they both know.

Basis	0	1
+	↑	→
×	↗	↘

Table1. basis format

Example: Consider Alice ‘A’ and Bob ‘B’ are generating secret key using above procedure. They agreed upon the table1 basis format. A sends bits in photons and B generates the random basis. During discussion if A and B’s basis match the bit is generated otherwise discarded. Shared key generated is of 4 bits, means at 4 positions the basis are same of both A and B.

The following table2 forms during the process:

A's random bit	1	0	1	1	0	0	0	1
A's random sending basis	+	x	x	+	+	x	+	x
Photon Polarization A sends	→	↗	↘	→	↑	↗	↑	↘
B's random measuring basis	+	+	x	x	x	+	+	x
Photon polarization B measure	→	↑	↘	↗	↗	→	↑	↘
Public Discussion of Basis								
Shared secret key	1		1				0	1

Table2. sharing of secret key using BB84 protocol

V B92 PROTOCOL

The B92 protocol is a simplified version of the BB84 protocol. This is also using polarized photons, but with non-orthogonal quantum states for encoding information [8]. In this, two quantum states Fig5. are used as compared to BB84 in which four states are used. Again, Alice randomly chooses one of these available quantum states and transmits towards Bob via a quantum channel. Bob has two methods to measure the arrived photons that will either register detection or no detection. During the Key Sifting stage, Bob confirms Alice about photons he detected without his actual measurement, while other photons are discarded. Error correction method is same as previous to verify the consistency of secret key.

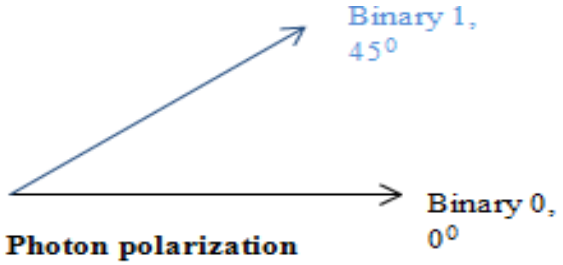

Fig.5: B92 2-state encoding [5]

VI ADVANTAGES AND LIMITATION OF QUANTUM CRYPTOGRAPHY

6.1 Advantages

The purpose of quantum cryptography is to provide the different foundation for cryptography with the use of quantum mechanics. Quantum cryptography achieves the most of the benefits of public-key cryptography and

has the advantage of being secure even against an adversary with superior computing power system and technology.

In cryptography, digital communications are sustainable to track and copy even by someone who is unaware of their meaning. Such copies can be used in future to decrypt the messages and secret key. However, in quantum cryptography the information is unachievable with traditional media.

6.2 Disadvantages

There are some problems while using quantum states to transmit information. Some problems are with quantum theory itself and some regarding equipment efficiency which affects the security of protocols.[10]

i. Point to Point links and Denial of Service-The quantum channel is point to point connection that is 1:1 connection. To link N number of nodes, N(N-1)/2 links will be required which increase cost and maintenance overhead. If attacker cuts the physical link Dos attack takes place.

ii. High Bit Errors Rate-The bit error rate of a quantum key distribution is higher than an optical communication system. The Error control protocol called CASCADE is used to correct bit errors, but it further makes system vulnerable to new attacks. The CASCADE leads to the problem of leakage of bits of secret key which is nullified by the process Privacy Amplification. Privacy amplification performs a compression function on the bit error corrected key. This will guarantee that the bits leaked to attacker will become useless and both communicating parties will have the same key.

iii. Losses in the Quantum Channel-Free space quantum channels suffer from the atmospheric and equipment dependent geometric losses. Quantum signals cannot be amplified therefore; the losses on the channel will be too high to distinguish the readings from dark count rates.

iv. Key Distribution Rate- The length of the quantum channel also affects the rate of key distribution. The rate at which key material is sent, decreases exponentially with respect to distance.

v. Classical Authentication-Quantum cryptography does not provide the digital signature as in classical cryptography and related features, such as certified mail.

The limitations can be overcome by Post Quantum Cryptography and other concepts.

VII CONCLUSION

Quantum cryptography is a new technology relies on quantum physics phenomenon and it is amazingly easy to integrate. The past few years have seen vast advances in experimental quantum cryptography systems and several companies have developed quantum cryptography prototypes because it is very secure key distribution, truly random key generation, faster key refresh rate, proactive intrusion. Thus Quantum cryptography provides the security in key distribution much better than classical cryptography that make use of mathematical concepts. The large number of quantum cryptography algorithms exists. BB86 and B92 are two protocols discussed in this paper provide the clear idea of generating secret key. Despite of having great advantages it suffers from some limitations too as high bit error rate, losses in quantum channel.

It can be concluded that Quantum Cryptography is really a robust technology. To take the advantage, limitations are needed to be overcome.

REFERENCES

[1] Forouzan, B.A 2010.Cryptography&Network Security.Tata McGraw-Hill Education.

[2] Vivek, R., & Roopchand, J. (2012). Emerging Trends in Quantum Cryptography- A Survey. *International Journal of Computer Technology and Applications*, *3*(4).

[3] Elboukhari, M., Azizi, M., & Azizi, A. (2010). Quantum Key Distribution Protocols: A Survey. *International Journal of Universal Computer Science*, *1*(2).

[4] Aditya, J., & Rao, P. S. Quantum Cryptography.

[5] Haitjema, M. (2007). A survey of the prominent quantum key distribution protocols.

[6] Bennett, C. H., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.*, *560*(P1), 7-11.

[7] Lopes, M., & Sarwade, N. (2014). Cryptography from quantum mechanical viewpoint. *arXiv preprint arXiv:1407.2357*.

[8] Singh, H., Gupta, D., & Singh, A. (2014). Quantum key distribution protocols: a review. *IOSR Journal of Computer Engineering (IOSR-JCE)*, *16*.

[9] Bruss, D., Erdélyi, G., Meyer, T., Riege, T., & Rothe, J. (2007). Quantum cryptography: A survey. *ACM Computing Surveys (CSUR)*, *39*(2), 6.

[10] Rubya, T., Latha, N. P., & Sangeetha, B. (2010). A survey on recent security trends using quantum cryptography. *IJCSE*, *2*(9), 3038-3042.