A Review on Quantum Cryptography Technology

[1]Premjeet Kumar, [2]Yashpal Singh
[1,2]Department of Computer Science &Engineering,
Ganga Institute of Technology and Management,
Kablana, Jhajjar, Haryana, India

***Abstract* -Nowadays, the information is exchanged among the computer network. These data and information are involved in business, military, academic education, research and etc. which are shared around the world in both private and public network. Since, many categories of data are required restriction on authorization of access, modify, delete and insert, security in communication is increasingly important to the network communication. Currently, computer security applies mathematic theory to computer security for encrypting and decrypting on both sender and receiver. To use security attack with high performance computer (e.g. quantum computer), attacker can find a key and then obtains the data in feasible period. Quantum cryptography is one of the solutions that use property of polarization to ensure that transmitted data is not trapped by eavesdropper. Quantum cryptography is improved significantly in the last decades including the most two dominant protocol BB84 and BB92.**

Keywords: ***Quantum Cryptography, QKD(Quantum Key Distribution), BB84, BB92***

I. INTRODUCTION

In general cryptography can be categorized as symmetric and asymmetric cryptography. Symmetric cryptography uses one key in decrypting and encrypting data such as DES (Eli and Shamir, 1993), 3DES (Merkle and Hellman, 1981) and AES (Ferguson *et al.*, 2001). In contrast, asymmetric cryptography uses one key to encrypt and another key to decrypt. These two keys in asymmetric cryptography are related in mathematically method where one encryption key has only one decryption key that can reveal the encrypted data. An example of asymmetric cryptography is RSA (Rivest *et al.*, 1978) which contains public key and private key. In the security perspective, asymmetric cryptography is more secured than symmetric cryptography and reduces the chance that eavesdropper breaks the security because of increasing domain of available keys and complex computing. However, if computing power is increasing significantly such as quantum computer, the time to reveal the key can be reduced significantly from million years in today computer to seconds in quantum computer. As a result communication needs a new technique to transmit data securely other than depending on mathematically method and large set of keys. Quantum cryptography uses a property of laws of quantum mechanics to inform sender and receiver (Alice and Bob) if other person attempts to retrieve transmitting data. If this case is occurred, both sender and receiver will ignore this part of data or this key. Then, they will re-start transmitting a new key for encrypting data again. To compare with current cryptography, both symmetric cryptography and asymmetric cryptography have no information when eaves dropper intercepts the transmitting key.

II. QUANTUM CRYPTOGRAPHY

Quantum cryptography contains a key distribution system that uses the laws of quantum mechanics to guarantee secure communication. The crucial element of quantum mechanics such a Heisenberg's uncertainty principle (Heisenberg, 1927) prevents anyone directly measuring the bit value without introducing errors that can be detected. A single photon is indivisible which means that an eavesdropper cannot split the quantum signal to make measurements covertly. Quantum cryptography has a quantum no-cloning theory. This theory shows that it is not possible to receive a single photon and duplicate the photon without giving the notice to others. There are two dominant schemes for quantum key distribution protocols which are the BB84 protocol and the BB92 protocol.

2.1 BB84 Protocol

BB84 (Bennett and Brassard, 1984) protocol is the first quantum cryptography protocol which is proposed by Charles Bennett and Gilles Brassard in 1984. This protocol employs two polarization bases of single photon; rectilinear basis and diagonal basis. The single photon may be polarized with four states: horizontal |h>, vertical |v>, left circle polarized |lcp>, and right circle polarized |rcp>. Polarization state horizontal |h> and left circle polarized |lcp> represent a '0'. Polarization state vertical |v> and right circle polarized |rcp> represent a '1'. To exchange secret key between sender and receiver (Alice and Bob) needs two channels, quantum channel and public channel, process as follow: Alice sends a random sequence polarize photons to Bob via quantum channel. After transmission is completed, Bob randomly chooses his detector either rectilinear basis or diagonal basis and then reports his detector to Alice via public channel. After that Alice responds the correct basis to Bob. Finally, Alice and Bob share the correct bits which are used as the key for the secure encryption. The procedure of BB84 protocol

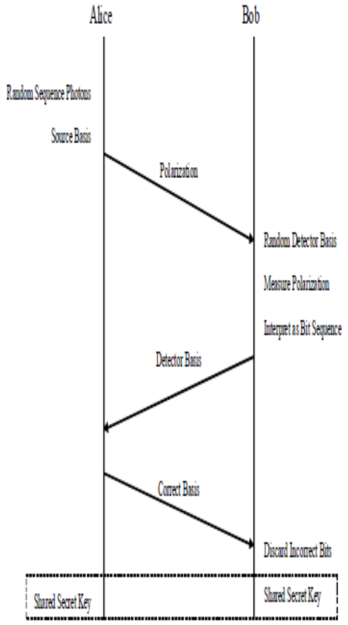

Fig 1: Procedure of BB84 Protocol

2.2 BB92 Protocol

BB92 (Bennett and Brassard, 1982) protocol is proposed by Charles Bennett and Gilles Brassard in 1992, similar to BB84 protocol but uses only two non-orthogonal quantum state |h> represent a '0' and |rcp> represent a '1', half of the BB84 protocol to transmit the key. The process of secret key transmission: Alice sends a random sequence of photons, |h> and |rcp>.Bob randomly chooses his detector basis from |lcp> or |v> and interprets as a quantum bit sequence, '0' and '1'. Alice and Bob share the same quantum bits, discarding all other bits. The BB92 protocol is shown in figure 2.

III. CRYPTOGRAPHY ATTACK

In general cryptography, key or password is the target of an intruder which attempts to reveal the encrypted data. There are several methods to attack by using the opportunity in transmitting data in network as shown below.

3.1 Brute Force Attack (BFA)

This method defeats cryptography by trying every possible key. It expects to find a correct key approximately at half of key domain (e.g. if there is 2n possible keys, BFA will average be founded correct key at 2n-1). However, this theory has a limitation in real world that array processors require a large amount of energy and continuous operation for a long period (Blaze, 1993).

3.2 Known Plain Text Attack (KPA)

KPA is attacking model where adversary has samples of plaintext (e.g. sensing data in network) and uses them to reveal secret key. As a result, an adversary could translate all the encrypted messages and also transmit fraudulent messages to the network (Meyer and Wetzel ,2004).

3.3 Replay Attack (RPA)

RPA is an attack against the message which is repeated or delayed. It could be using as duplicated authentication or malicious data. In network communication, RPA can use for creating a new session or to bypass authentication (Kwon and Song , 1999).

3.4 Maninthemiddle Attack (MITM)

MITM has the intent to read, add and modify messages between two parties. It requires intercepting messages between two parties (Meyer and Wetzel , 2004).

3.5 Denial of Service Attack (DoS)

DoS is an attack to disrupt computer resource or obstruct communication between user and service. DoS in network can be in the form of flooding network which disturbs communication between nodes, or continuous communication burns out the equipment's battery (Deng *et al.*, 2005).

IV. DISCUSSION

Since Brute Force Attack (BFA) is focused on the key, quantum cryptography is increasing the computation time that BFA required to decrypt an entire set of information because the frequency of key changing in quantum cryptography is increasing more than general cryptography. Known Plain Text Attack (KPA) is more difficult in quantum cryptography because rapidly key change during the session increasing more varieties of encrypted pattern, so attack in quantum cryptography is required more processing time significantly than general cryptography. However, Man-in-the-middle Attack (MITM) and Denial of Service Attack (DoS) still able be occurred in this quantum cryptography because these two attacks are not focused in cryptography method but rely on trust and network protocol mechanisms.

V. CONCLUSION

Quantum cryptography is alternative security solution for computer network. Instead of using general encryption and decryption technique, quantum cryptography can verify that key is transmitted without interception from eavesdropper. In the case that key is intercepted, both sender and receiver are simple drop the key and re-send the new key.

BB84 is the protocol that introduces the method to transmit the key with quantum technique. However, BB84 requires four polarization states: horizontal |h>, vertical |v>, left circle polarized |lcp>, and right circle polarized |rcp> comparing to two non-orthogonal quantum state |h> represent a '0' and |rcp> represent a '1' in BB92. Also, the procedure during setting up the shared key for both sender and receiver, BB92 is simplified with more effective of transmission. This quantum cryptography can be applied to application and superior secure channel. In the future, this protocol is also prepared for the upcoming high performance computer (e.g. quantum computer).

ACKNOWLEDGEMENTS

For this paper, we would like to thank Optical and Quantum Communication Research Lab, National Research Council of Thailand, Faculty of Engineering Thammasat University and Thammasat University for the support and cooperation.

REFERENCES

[1]. Bennet, C.H., and G. Brassard. Quantum cryptography using any two non-orthogonal states, *Physical Review Letters*, Vol. 68, 1992; 3121-3124.

[2]. Bennet, C.H., and G. Brassard. Quantum Cryptography: public key distribution and coin tossing, *Proceeding of IEE International Conference on Computers, Systems and Signal Processing*, India 1984; 175-179.

[3]. Blaze, M. A cryptographic file system for UNIX ,in *Proceedings of the 1st ACM conference on Computer and communications security Fairfax*, Virginia, United States ACM Press,1993; 9-16.

[4].` Deng, J., R. Han, and S. Mishra, Defending against pathbased DoS attacks in wireless sensor networks, in *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks Alexandria*, VA, USA ACM Press, 2005; 89-96.