International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 5 | ISSN : 2456-3307

Quantum Cryptography : Latest Security Measure For Network Communication

Neha Yadav, Alka Agrawal

Department of information Technology, Baba Saheb Bhimrao Ambedkar University, Lucknow, India

ABSTRACT

This research paper focuses on the origin and concept of quantum cryptography, and how quantum cryptography will prove to be beneficial for security in network communication. Quantum key distribution (QKD) technique of quantum cryptography is described in detail. It also briefs the present state of quantum cryptography, and its practical applications, and at end the future aspects of quantum cryptography.

Keywords : Quantum cryptography, Quantum key distribution (QKD)

I. INTRODUCTION

Quantum cryptography is a technique to protect the data, transmitted from sender to receiver, from unauthorized access by using properties of physics [1]. It is different from classical cryptography as in classical cryptography we uses mathematical techniques to secure our data while in quantum cryptography phenomena of quantum physics are applied [2]. The two important principles of quantum physics used in quantum cryptography are Heisenberg Uncertainty principle and photon polarization principle [3]. The Uncertainty principle is the specific property of quantum physics, which makes it different from the classical physics. As per uncertainty principle we cannot determine both position and momentum of an atomic particle simultaneously [4]. On the other hand photon polarization is the description of quantum mechanical properties of electromagnetic wave. A photon can be left polarized or right polarized or it the superposition of both [5]. So, due to Heisenberg uncertainty principle, in quantum cryptography an eavesdropper cannot get complete information of a photon, which carries data bit. When he tries to get one part of data the other part will be destroyed and vice versa [3]. Quantum key distribution (QKD) is the important technique of quantum cryptography, which provides the data secure solution to the problem of key exchange [5].

II. Quantum Key Distribution (QKD)

The non-cloning theorem, the key principle used in quantum cryptography, states that we cannot make exact copy of the unknown quantum states. Only identical and orthogonal states can be copied [1]. This non-cloning theorem is the main component used in quantum key distribution. Quantum key distribution is an important technique of quantum cryptography in which sender and receiver communicate over a quantum channel where a sequence of qubits is transferred between them this sequence will serve as key when communication takes place over an insecure medium. The data and the key are aggregated in such a way that even if an eavesdropper knows the key he cannot find the message communicated. Only the receiver can decrypt the message by using the copy of the key, which was generated over the quantum channel. The main purpose of quantum key distribution is not the data encryption but to maintain the secrecy of the key. So in order to keep our data secure we have to focus on two parameters, which are key security and the algorithm needed to encrypt data. In quantum key distribution we can generate long keys as frequently as needed by sender and receiver, this makes quantum key

distribution as one of the unique and most used technique of quantum cryptography. Coming to the working of quantum key distribution, it requires a quantum channel to transmit the quantum particles these particles can be photon or trapped ions. The channel can be optical fiber. While transmitting key over the quantum channel the eavesdropper may listen to the communication and know about the key. But this will not compromise the security of the system in quantum key distribution as in quantum key distribution it is easy to detect the transmission error and overcoming these errors by using distillation of key.

After the transmission, the sender and receiver can share a fraction of the message to make sure that the data transferred is correct and not altered by the eavesdropper. For this the public channel as shown in figure 1 is used by the sender (Alice) and (Bob). Eavesdropper may detect the transmission over this channel but it is necessary to prove the authentication of the channel in order to confirm that Alice and Bob are communicating with each other only. BB84 practically used the quantum key distribution most successfully. In this the sender use the quantum states that are related to each other, unknown states are not used. According to uncertainty principle we cannot determine two related states. So unauthorized access become difficult for the eavesdropper [3].

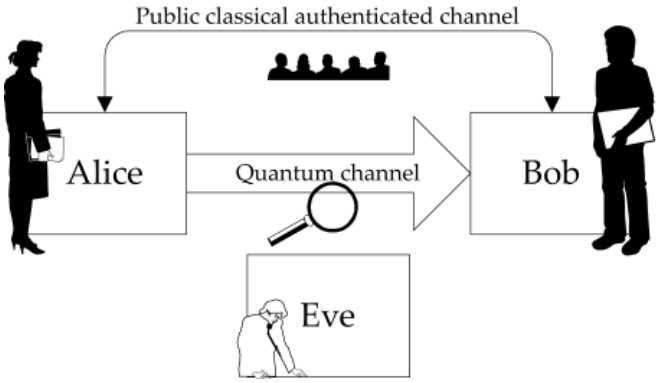

Figure 1 : Quantum key distribution comprises a quantum channel and a public classical authenticated channel. As a universal convention in quantum cryptography, Alice sends quantum states to Bob through a quantum channel. Eve is suspected of eavesdropping on the line. [3]

III. Current Status of Quantum Cryptography

The researchers still doing the research that how we can use the quantum computer that make cryptographic system unbreakable. Based upon the difficulty of computing a specific mathematical problem, the current public key system like RSA and ECC are depended in security. Basically, quantum cryptography is based on the fact that how it can evaluate those mathematical problems which are difficult to compute. The mathematical problem, which is difficult to evaluate are called trapdoor functions. It is so, because it is not difficult from working in one set of values but when we worked in at the other end by deriving the solution from the set of values, it becomes a nearly impossible task. However, at the same time finding the same set of values from which trapdoor solution was derived is practically impossible as it requires very large assumption of big numbers. This would reduce the speed of computation and testing which is mainly oriented whether the guess is correct. The one solution to this problem is a quantum computation called Grover's algorithm, which ensures the safety and security of breaking of computational setup. In the present scenario, it is possible to speed up the trapdoor function at the other end like RSA and ECC are used for classical systems. However, it would surely lead to the attack on the quantum cryptographic system. Further, it may also break down the whole communication system, which involved the same quantum cryptographic methods. This problem can be resolved using an advanced system based on the laws of Physics. In order to break such a system, the laws of Physics will have to be compromised or broken, which is nearly impossible in terms of the Heisenberg uncertainty principle. It states that the more precisely the position of the particle is determined, the less precisely its momentum can be ascertained. One such system based on the above law of Physics is use of QKD in quantum cryptography. QKD uses Heisenberg principles to transmit symmetric encryption keys.

Research is being done today to increase the data rate to the larger distances using QKD system. Many researchers also believe that QKD system can also be integrated with the present information security systems. The basic roadblock to this system is the use of quantum repeaters, which enhances the signal to noise ratio for transmission of data and information to large distance. However, the use of quantum repeaters is constrained by the existing technologies and research. Researchers believe that the use of satellite system can facilitate the larger distance transmission using QKD [10].

IV. Challenges of Quantum Cryptography

At present quantum computing is at very initial stage so the quantum cryptography, for the full fledge development in the field of quantum computing we need to have a stable sequence of qubits array, universal gates for quantum computing and a single quantum measurement. At present it is not possible to achieve all these measures [7]. It is difficult to maintain superposition and entangled states continuously for long time. It is very difficult to isolate the system from environment noise on the other hand decoherence is needed for long time in quantum systems, for this the system should not interact with anything for long time [8]. Error correction and detection is very difficult as of now. The main purpose of quantum computing is to store large data on a single bit but at the same time a small change in a single bit is capable of causing a huge damage. So until and unless there is a robust system for quantum computing we don't get a full proof system for quantum cryptography.

V. Future Aspects

At present the quantum key distribution is in its development phase, a large number of researches are going on. These researches will take this system at international level and provide universal security. At present QKD systems are the secure systems, it is very difficult to attack a QKD system and also it is too expensive. So QKD will protect our data for long time and provide mental peace. In order to protect the data efficiently both classical cryptography as well as quantum cryptography is needed [9].

VI.CONCLUSION

Quantum cryptography provides data security using the quantum physics techniques. It is very difficult and costly to break the system which uses quantum cryptographic techniques to secure its data, a large number of researches showed that techniques of quantum cryptography provide much more secure systems than the classical cryptographic systems. Use of non cloning theorem in BB84 protocol of quantum cryptography proves its robust security system.

VII. REFERENCES

[1]. Dagmar, Bruss, Gabor Erdelyi, Tim meyer, Tobias Riege and Jorge Rothe,"Quantum cryptography: a survey", Vol. 39, No. 2, Article 6, Publication date: June 2007.

[2]. Ritesh Kumar Jain, Kamal Hiran, Gaurav Paliwal," Quantum cryptography: a new generation of information security system", Vol. 2, international Journal of Computers and Distributed Systems: December 1, 2012.

[3]. Gilles Van Assche," Quantum Cryptography and Secret-Key Distillation", Available from June 29, 2006.

[4]. Stanford encyclopedia of philosophy, first published Mon Oct 8, 2001

[5]. https://en.wikipedia.org/wiki/Photon_p olarization

[6]. https://en.wikipedia.org/wiki/Quantum _cryptography

[7]. Abhilash Ponnath,"Difficulties in the implementation of quantum computing"

[8]. https://www.quora.com/What-arethe- biggest-challenges-in-quantumcomputing

[9]. http://bigthink.com/in-their-ownwords/ the-grand-challenge-ofquantum- computing

[10]. https://labs.mwrinfosecurity.com/p ublications