Survey of Most Prominent Quantum Key Distribution Protocols

Ajay L[1]

[1]*M.Tech Student, Dept. of Computer Science and Engineering, Siddaganga Institute of Technology, Karnataka, India*

---***---

Abstract - *Security is the most important area of interest. To ensure the security in communication networks, Symmetric key cryptography and asymmetric key cryptography is proposed. These cryptosystems uses the secret key, if the key is weak then the whole system will be collapsed. To overcome this a new key distribution technique based on quantum physics is proposed called Quantum Key Distribution(QKD).We survey the different protocols which implements the quantum key distribution.*

***Key Words*: Quantum key distribution, BB84 protocol, BB92 protocol, SARG04 protocol, E91 protocol, COW protocol, DPS protocol, KMB09 Protocol, S09 protocol, S13 protocol.**

1.INTRODUCTION

The security is a big concern in wired networks and wireless networks. The characteristics of networks pose challenges in achieving the security goals, such as confidentiality, authentication, integrity, availability, access control, and no repudiation. Cryptographic techniques are widely used for secure communications. To ensure the security the symmetric cryptography and asymmetric cryptography is proposed.

Classical cryptography can be divided into two major methods; secret or symmetric key cryptography and public key cryptography, which is also known as asymmetric cryptography. Secret key cryptography is the most traditional form of cryptography in which two parties perform both encryption and decryption of their messages using the same shared secret key. While some secret key schemes, such as one-time pads, are perfectly secure against an attacker with arbitrary computational power they have the major practical disadvantage that before two parties can communicate securely they must some how establish a secret key. In order to establish a secret key over an insecure channel, key distribution schemes based on public key cryptography, such as Diffie-Hellman, are typically employed.

In contrast to the secret key cryptography, a shared secret key does not need to be established prior to communication in public key cryptography. Instead each party has a private key, which remains secret, and a public key, which they may distribute freely. If Alice, wants to send a message to another party, Bob, she would encrypt her message with Bob's public key after which only Bob could decrypt the message using his private key. While there is no need for key exchange, the security of public key cryptography algorithms are currently all based on the unproven assumption of the difficulty of certain problems such as integer factorization or the discrete logarithm problem. This means that public key cryptography algorithms are potentially vulnerable to improvements in computational power or the discovery of efficient algorithms to solve their underlying problems. Indeed algorithms have already been proposed to perform both integer factorization and solve the discrete logarithm problem in polynomial time on a quantum computer.

While the advent of a feasible quantum computer would make current public key cryptosystems obsolete and threaten key distribution protocols such as Diffie-Hellman, some of the same principles that empower quantum computers also offer an unconditionally secure solution to the key distribution problem. Moreover, quantum mechanics also provides the ability to detect the presence of an eavesdropper who is attempting to learn the key, which is a new feature in the field of cryptography. Because the research community has been focused primarily on using quantum mechanics to enable secure key distribution, quantum cryptography and quantum key distribution (QKD)[1][2] are generally synonymous in the literature.

The focus of this paper is to survey the most prominent quantum key distribution protocols and their security. In this paper we briefly describe the principles of quantum mechanics(Heisenberg Uncertainty Principle and Quantum Entanglement).

2. QUANTUM CRYPTOGRAPHY

Quantum Cryptography is a recent arrival in the world of information security. It uses the laws of quantum mechanics to create new primitives of cryptography. One quantum cryptographic primitive can be Quantum Key Distribution. By using the quantum properties such as light, fiber-optics, lasers and free space transmission technology we can perform the Quantum Key Distribution. Quantum key distribution is a key establishment protocol which creates symmetric key by using the laws of quantum physics(Heisenberg Uncertainty Principle and Quantum Entanglement).

2.1 HEISENBERG UNCERTAINTY PRINCIPLE

According the this principle, it is not possible to measure the quantum state of any system without disturbing that system. Thus the polarization of photon or light particle can only be known at the point when it is measured. This principle play a critical role in thwarting the attempts of eavesdroppers in a cryptosystem based on quantum cryptography.

According to this principle we cannot partition the photon into two halves measuring the state of photon will affect the value. If someone tries to tries to detect the state of photons being send to the receiver, error can be detected.

2.2 QUANTUM ENTANGLEMENT

Another important principle is quantum entanglement. It is possible for two particles to become entangled such that when a particular property is measured in one particle, the opposite state will be observed on the entangled particle instantaneously. It is impossible, however to predict prior to measurement what state will be observed thus it is not possible to communicate via entangled particles without discussing the observation over classical channel.

3. QKD PROTOCOLS

3.1 BB84 PROTOCOL

This protocol is proposed by Charles Bennett and Gilles Brassard in 1984.It is based upon conventional cryptographic methods and extends these through the use of quantum effects. Quantum key Distribution (QKD) is used in quantum cryptography for generating a secret key shared between two parties using a quantum channel and an authenticated classical channel as show in figure 1. The private key obtained then used to encrypt message that are sent over an insecure channel (such as a conventional internet connection).

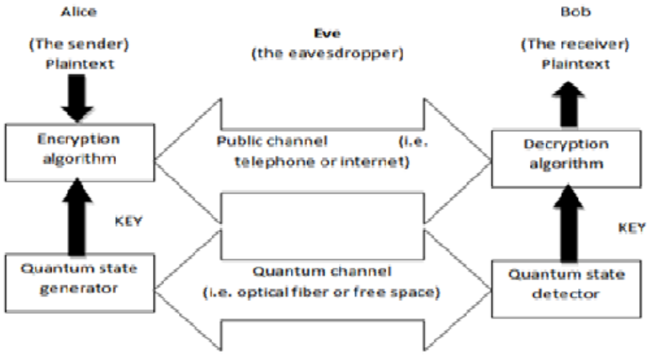

Figure 1: Quantum cryptographic communication System using two channels to generate random key.

This Protocol is described using the photon polarization as shown in the figure 2.

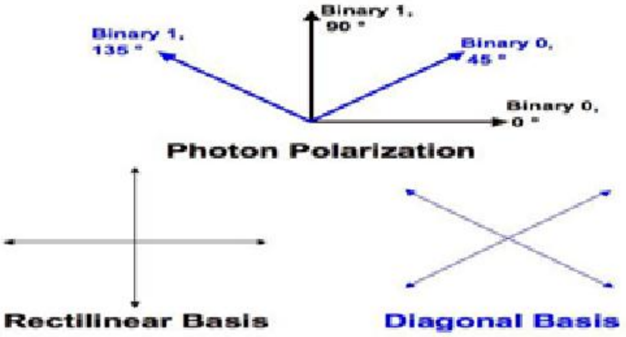

Figure 2: BB84 Bit Encoding.

This protocol communication takes place in two separate channels. Alice and Bob communicate each other using the two channels. Let us see how the protocol works.

Communication in Quantum Channel

Alice transmits photons in the four polarization states (0,45,90,135 degree) as shown in figure 2. Bob prepare the photon by randomly choosing the either rectilinear (+) or diagonal(x) polarization Basis. Alice records the polarization of each photon and sends it to the Bob. Bob receives the photon from the Alice and randomly records the polarization using the rectilinear or diagonal basis. Bob does not know that the measured in the same basis as the one used by the

Alice. Alice and Bob will proceed to communicate over the public channel.

Communication in Public Channel

Over the public channel, Bob communicates to Alice which quantum alphabet he used for each of his measurements. In response to the Bob, Alice will respond with the respective alphabet. There after both Alice and Bob delete all the bits which they used are incompatible alphabet to produce the resulting the raw keys. To estimate the error rate R, If through their public disclosures find no errors(i.e. R=0) then they will come to know the t the no eve dropping taken place and the tentative key will be the final key. If at least one error (i.e., R>0) then they will discard their tentative keys and start the whole process once again.

3.2 BB92 PROTOCOL

After the BB84 protocol is published, Charles Bennett realized that it is not necessary to have the two separate orthogonal basis for encoding and decoding. Instead of using the two orthogonal basis, we can go for the single non orthogonal basis. Without affecting the security of the protocol including the security over eve dropping. Key difference between the BB84 and BB92 protocol is, BB92 protocol uses two states rather than possible 4 polarization states in BB84 protocol.

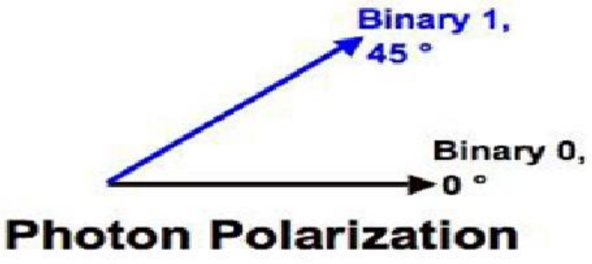

Figure 3: BB92 2-State Encoding

As shown in the Figure 3, 0 can encoded as 0 degrees in rectangular basis and 1 can be encoded by 45 degrees in diagonal basis. Alice transmits to Bob a string of photons encoded with randomly chosen bits but this time the bits Alice chooses dictates which bases Bob must use. Bob still randomly chooses a basis by which to measure but if he chooses the wrong basis, he will not measure anything; a condition in quantum mechanics which is known as an erasure. Bob can simply tell Alice after each bit Bob sends whether or not he measured it correctly.

3.3 SARG04 PROTOCOL

This protocol was proposed in 2004 by Scarani et.al. This protocol shares the exact same first phase as BB84.In the second Phase when Alice and Bob determine for which bits their bases matched, Alice does not directly announce his bases rather than Alice announces a pair of non-orthogonal states one of which she used to encode her bit. If Bob used the correct basis, she will measure the correct state. If she chose incorrectly he will not measure Alice states and will not be able to determine the bit. If there are no errors, then the length of the key remaining after the sifting stage is ¼ of the raw key.

The SARG04 protocol provides almost identical security to BB84 in perfect single-photon implementations: If the quantum channel is of a given visibility (i.e. with losses) then the QBER of SARG04 is twice that of BB84 protocol, and is more sensitive to losses.

However SARG04 protocol provides more security than BB84 in the presence of PNS attack, in both the secret key rate and distance the signal can be carried (limiting distance).

3.4 COW PROTOCOL

Coherent One-Way protocol (COW protocol) is a new protocol for Quantum cryptography elaborated by Nicolas Gisin et al in 2004. A new protocol for QKD tailored to work with weak coherent pulses at high bit rates [36]. The advantage of this system are that the setup is experimentally simple and it is tolerant to reduced interference visibility and to photon numbers splitting attacks, thus resulting in a high efficiency in terms of distilled secret bits per qubit.

3.5 DPS PROTOCOL

Differential Phase shift QKD(DPS-QKD) is a quantum key distribution scheme proposed by K. Inoue et al. Alice randomly phase-modulates a pulse train of weak coherent states by $(0,\pi)$ for each pulse with an average photon number of less than one per pulse. Bob measure the Phase difference between two sequential pulses using a 1-bit delay. After transmission of the optical pulse train, Bob tells Alice the time instances at which a photon was counted. From this time information and her modulation data. Alice knows which detector clicked at Bob's site. Under an agreement that a click by detector 1 denotes "0" and click by detector 2 denotes "1", for example Alice and Bob obtain an identical bit string.

The DPS-QKD scheme has certain advantageous features including a simple configuration, efficient time domain use, and robustness against photon number splitting attack.

3.6 KMB09 PROTOCOL

KMB09 protocol is an alternative quantum key distribution protocol. Where Alice and Bob use two mutually unbiased bases with one of them encoding as 0 and the other one encoding as 1. The security of the scheme is due to a minimum index transmission error rate (ITER) and quantum bit error rate (QBER) introduced by an eavesdropper.
The ITER increase significantly for higher dimensional photon states. This allows for more Noise in the transmission line, thereby increasing the possible distance between Alice and Bob Without the need for intermediate nodes.

3.6 S09 PROTOCOL

S09 protocol is quantum protocol based on public private key cryptography for secure transmission of data over a public channel [41]. The security of the protocol derives from the fact that Alice and Bob each use secret keys in multiple exchange of the qubit. Unlike the BB84 protocol [1] and its many variants. Bob Know the key to transmit, the qubits are transmitted in only one direction and classical information exchanged thereafter, the communication in the proposed protocol remains quantum in each stage. In the BB84 protocol, each transmitted qubit is in one of four different states in this protocol transmitted qubit can be in any arbitrary states.

3.6 S13 PROTOCOL

S13 protocol is a new quantum protocol that is identical to the BB84 protocol for all the quantum manipulation, but differs from it by using Private Reconciliation from a Random Seed and Asymmetric Cryptography. Thus allowing the generation of larger secure keys.

3. CONCLUSIONS

QKD Protocols are based on principles from quantum physics and information theory. Quantum key distribution is clearly an unconditionally secure means of establishing secret keys. Combined with unconditionally secure authentication, and an unconditionally secure cryptosystem. The current commercial systems are aimed mainly at governments and corporations with high security requirements. The major difference of quantum key distribution is the ability to detect any interception of the key, whereas with courier the key security cannot be proven or tested. QKD system has the advantage of being automatic, with greater reliability and lower operating costs than a secure human courier network.

REFERENCES

[1]. C. H. Bennett and G. Brassard, "*Quantum cryptography: public key distribution and coin tossing*," Proc. of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175-179, 1984.

[2]. E. Artur "Quantum cryptography based on Bell‟s theorem.", Physical review Letters, Vol. 67, No, 6,5 august 1991, pp 661-663.