International Journal of Mathematics and
Computer Science, **16**(2021), no. 1, 9–21

Quantum Cryptography: A way of Improving Security of Information

Muhammad Aamir Panhwar[1], Sijjad Ali Khuhro[2], Tehseen Mazhar[3], Deng ZhongLiang[1], Nabeel Qadir[3]

[1]School of Electronic Engineering
Beijing University of Posts and Telecommunications
Beijing, China

[2]School of Computer Science and Technology
University of Science and Technology of China
Hefei, Anhui, China

[3]School of computer science
Virtual University of Pakistan
Lahore Punjab, Pakistan

email: maamirpanhwar@gmail.com

(Received April 16, 2020, Accepted May 14, 2020)

Abstract

The main challenge in the current era is how to secure the communication networks on which the information is transmitted from source to destination. Different techniques and algorithms are used for securing the communication system and providing a more secure system that ensures confidentiality and the integrity of data. The secret in this system includes the shared key algorithm and the public key. By using the Quantum Cryptography technique, a more secure communication network is achieved. This technique of Quantum Cryptography is based on the following two elements, photon polarization and the principle of uncertainty. Photon polarization ensures that an eavesdropper cannot copy or even try to read the information which is being

Key words and phrases: Quantum Cryptography, secured network, photon polarization, Quantum key distribution, uncertainty principle.
AMS (MOS) Subject Classifications: 81P94, 68P25.
ISSN 1814-0432, 2021, http://ijmcs.future-in-tech.net

transmitted by using photons. The principle of uncertainty states that it is impossible to measure or observe the state of photons without disturbing their actual state. The main focus of this paper is on photon Cryptography and how this can be used to make the network more secured. Finally, we discuss the future of Quantum Cryptography.

1 Introduction

The main driving force behind the development of photon Cryptography is that traditional public-key Cryptography, private key Cryptography and one-time pad do not provide that level of security that is desired by some organizations. In these two systems, the sender and receiver need to exchange the secret sequence of bits that is called the key. The main idea is to ensure the privacy of this key. This key may be transmitted by using computer networks or by some physical means. This way of exchanging key creates security loopholes in communication system most of the algorithms that are used are based on some mathematical technique as RSA (Rivest-Shamir-Adleman) use factoring an extremely large prime number, some based on calculating the discrete logarithm. Nowadays, very fast computing devices have been invented that can compute this calculation within a few hours. Most of these cryptographic systems do not refresh their keys that result in key expansion rate and it is very harmful for information and network security. This key can also be compromised in various ways like a brute force attack in which iteratively test or check the key.

By applying different possible values of the key, a traditional algorithm like Advanced Encryption Standard (AES), RSA, among others, cannot detect eavesdropping while data is transmitted over the medium. As a result, it is urgent and necessary to develop a technique that can detect an eavesdropper while data or information is being transmitted over the medium. Many efforts were made to develop such a technique that led to the development of the Quantum Cryptography technique which has played a marvelous role in securing communication networks especially detecting eavesdropping while the message is transmitted on the communication medium.

Quantum Cryptography is based on the uncertainty principle and polarization of the photon. These principles described that it is impossible to measure the exact state of the photon which are carrying the information without disturbing the actual state of these photons. When eavesdroppers try to read information from photons, the state of these photons is changed and it is detected that somebody is trying to sniff or listen. Quantum Cryptography has

played a revolutionary role in securing a communication network especially in Quantum Key Distribution (QKD).

2 Quantum Cryptography

Quantum Cryptography is based on the Heisenberg Principle of uncertainty and polarization of the photon. Heisenberg Principle defines that physical properties in a set of pairs are attached or related in such fashion that only one property can be measured at a single time. No one can measure these two related properties at the same time. It is simply stated that the polarization of photons that is light particle can be known in which it is measured. In Quantum Cryptography, both the sender and receiver must be agreed on a specific bit sequence or bit stream before the actual communication start. This agreed string must be secured and this must be shared between the communicating entities. A protocol BB84 enables the sender and receiver to make a secure key sequence or stream of bits using polarized photons.
Every photon must have the one of the following four possible forms or symbols: $0(\_), \pi$ /2(|), π /4(\ ), 3π /4(/). Now both sender and receiver must agree first the exact meaning of photon polarization. Now after this step sender generates the random bits stream and random sequence of photons bases and then the sender sends this photons sequence to the receiver one by one. Now the receiver applies the polarization filters to measure the polarization of the photons that are transmitted by the sender [1].
In the next step, the receiver will inform the sender about the bases that he measured against each photon that he received. Now the sender will check and tell the receiver which one combination or sequence is correct. Now the sender and receiver will extract the bits from the correct bases [2]. This is ensured that this sequence of bits in only known to the sender and receiver. This sequence of bits is shared as a secret bit stream or secret key for communication between the sender and receiver to carry out further communications. If an eavesdropper tries to sniff while the communication between the sender and receiver is done, the sender and receiver will estimate the error rate in a bit stream generated and received. If this error rate is more than 25 percent, then the sender and receiver will have to discard the sequence of bits. In case of error rate is less than 25 percent, both parties will accept this sequence as a secret key. The Uncertainty Principle ensures that the transmission process of a key is secured and any type of attacker will not be able to read the transmitted key over the medium. Quantum Cryptography

ensures the secrecy of the key by encoding bits at the photon level. An act of eavesdropping, trying to measure the state of the photon, will disturb the actual state of the photon and in this way eavesdropping will be detected.

3 Implementation of Quantum Cryptography

The first Quantum network was DARPA which was developed by BBN at Boston and Harvard Universities. This DARPA Quantum network was able to provide end to end security of information through a very high traveling photon QKD. This network only covered a small area, for example a metropolitan area, by using fiber optic cables. The model of DARPA network [13] was based on the cryptographic virtual private network and, usually, these VPNs use both types of symmetric key and public key algorithms to attain authentication, integrity and confidentially. These algorithms (public key) use key exchange or agreement and, in this way, source and destination are authenticated.
DARPA design was a private virtual network that used the cryptographic techniques to transmit the desired data or keys. Usually, private virtual networks used both types of public key and symmetric Cryptography to gain different types of services that included the integrity of data, authentication, and confidentiality. The public key was used as a key exchange algorithm. Different algorithms like 3DES and SHA1 provided traffic confidentiality and data integrity services. In the DARPA network model, this public-key Cryptography was replaced with the Quantum Cryptography and the remaining work of VPN is the same as the work of other different VPNs. The architecture of the DARPA network [13] is shown in figure 1. Another company that worked on the development of Cryptography solutions was MagiQ technologies which provided the financial services to its customers and also different Government and private lab services. The work of this company was based on the hybrid mechanism for providing a more secure information system. MagiQ is considered the first company that provided the first QKD [3, 4].

4 Quantum Key Distribution Protocols Implementation

QKD consists of a different specialized set of protocols that are called QKD protocols. The arrangement of these protocols is shown in figure 2.

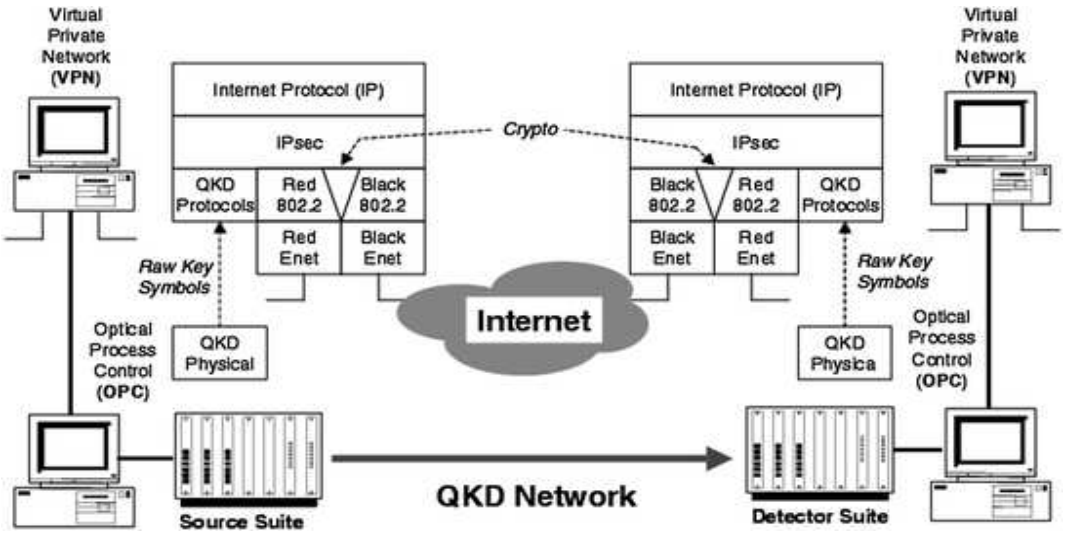

Figure 1: The architecture of DARPA Network [22]

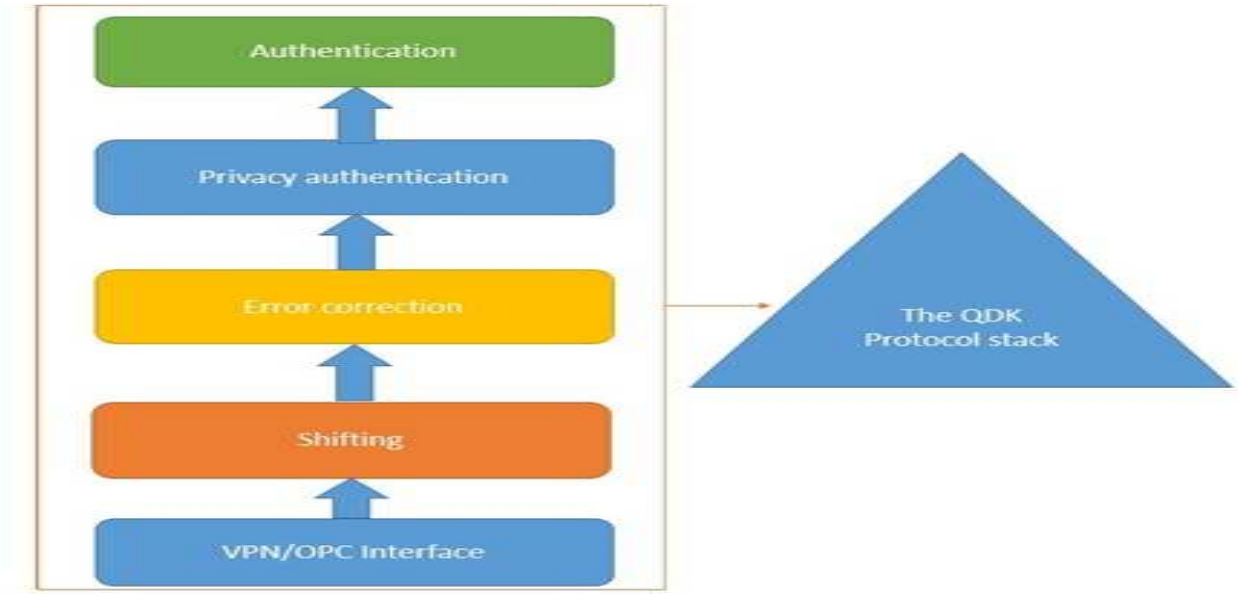

Figure 2: Arrangement Protocols of QKD

Figure 2 describes the arrangement of protocols that are running on a different level of the layers of protocol suit. These different protocols and sub-layers do not correspond to the QKD protocols as the OSI layer in the network communication model.

Authentication: the basic purpose of the sender and receiver authentication in key distribution is to avoid "the man in the middle" attack especially in the case of Diffie-Hellman public key cryptosystem. By doing authentication, Aamir (sender) and Tehseen (receiver) both are sure that they are exactly communicating with one another and there is no third person involved in the middle. Before starting actual communication, authentication must be performed. The actual BB84 paper explained the authentication problem and gave a solution to this problem by using the hashing functions. In this method, the sender and receiver choose a hash function randomly from the list of hash functions to form an authentication hash for both of them. As these hash functions are easy to perform in one direction and not in opposite direction due to the extreme nature of these hash function, there are rare occasions that anyone that did not know the secret key is able to grab or steal the information which is transmitted over the medium. The disadvantage of this technique is that the secret can be used only once for a particular transmission. Luckily we have an approach in which a whole authentication can be validated over a large number of secret bits from QKD. It is not enough to only authenticate the QKD protocols; we also need to authenticate the virtual private networks [5, 6, 7].

Privacy Amplification: This is a process by which Aamir and Tehseen can reduce the eavesdropper chance to grab the information to a certain acceptable level which is called an advantage distillation. The sender side that starts this privacy amplification selects a random linear hash function to the Galois Field (GF). Now, this initiating entity will send four things to the other entity. The number of reducing bits m, primitive polynomial, a multiplier and m bit polynomial for addition. Now both entities will perform the relative hash and append the result to m bits.

Error Correction: Aamir and Tehseen will know about the error bits that are introduced in their shared sequence of bits by using the error correction mechanism. They can also do corrections so that both the communicating entities can share the same bits as a key between them. For example, Aamir sends 0s bits to Tehseen but Tehseen receives these bits as 1s which

are called the error bits. These errors may be caused by an act of eavesdropper or by any kind of noise. QKD has a very usual error correction constraint that can do error detection and error correction. There is an essential need to make error detection and correction codes that can reduce or control error occurrence between Aamir and Tehseen as they communicate.

Sifting: This is a technique through which Aamir and Tehseen buffering window will drop all the failed m bits from the different number of bits. These failures may be caused by different reasons as those bits that Aamir has never sent or Tehseen detector could not detect the photons or these photons were lost during transmission. These failures may also be due to Aamir selecting a different base symbol to send the bits but Tehseen applying different symbols for receiving. In this case, both Aamir and Tehseen will reject these bits from their internal storage.

5 Desirable Quantum Key Distribution

Generally, Quantum key Cryptography is a technique in which two different devices, one is the sender and the other is the receiver, can randomly select the sequence of bits in such a way that there are minimum chances to grab this random sequence of bits that are transmitted over the medium. This secret sequence of bits serves as the key for encoding and decoding the data between the communicating devices over the medium. QKD is simply a key distribution mechanism that provides a secure way for the distribution of the key. This distribution is very secure as no one even sniffs the key or transmitted data. The following are the desirable attributes of QKD [8-9].

Confidentially of Keys: The major concern or interest in QKD is confidentiality of the key that is used for encryption and decryption purposes. Before the QKD, Diffie-Hellman public key cryptosystem was used to exchange the key between the communicating devices. Later, there was a discovery of a man in the middle attack in this Diffie-Hellman key exchange mechanism [10]. So the key can be compromised and secret information can be grabbed as it transmitted on the medium. QKD is a secured process in which the sender and receiver both randomly select the sequence of bits and send them using the polarized photons. This QKD system is a superior method of key exchange between the remote devices than the other classical cryptosystems [11].

Authentication: The QKD technique does not provide any authentication. The authenticity of the devices that are involved in communication is done by using the prepositioning of the key on remote devices and then this key is verified by using a hash-based authentication scheme. Placing the copy of keys on both sender and receiver devices using the human courier may be unsecured, costly and time-consuming. A DOS attack may be launched against the devices that are authenticating the devices and in this way devices will not be able to do authentication [12].

Rapid Key Delivery: The system must provide a fast key delivery mechanism so that the devices that are doing encryption and decryption do not exhaust their supply of key bits. This is the ratio between the rate at which the key bits are placed and the rate at which the key bits are used for the encryption and decryption process. Nowadays, the QKD systems attain the rate of 1000 bits/sec for keying material but, in reality, they run at a very slow rate. This becomes unacceptable if someone uses the keys in different ways. Thus QKD provides more and improves rates for keying material.

Robustness: The key element in QKD is providing the keying material and it must be ensured that keying material must not be disrupted either by the act which in intentional or accidental. As QKD is exclusively employed on point to point link and if this link is disturbed either by eavesdroppers act or by accidental event, then the flow of keying material will be stopped and no further keying material will be available for encryption or decryption process. That is why a meshed network is more robust as the single link failure will not bring down the whole QKD network. Multiple links are available in the meshed network.

Distance and Location-Independence: It is possible that any entity can agree upon the keying material of any other entity in the world. Internet infrastructure does not support this kind of feature. By using IPsec terminology, any computer on the network can make a security association with any other computer on the internet. This type of service or feature is not present in QKD which is required to direct interaction between the devices. This can operate only within a few kilometers by using the fiber optic cable.

Resistance to Traffic Analysis: An attacker or eavesdropper may try to perform some operations and can grab or try to sniff the information which

is transmitted over the medium. A large amount of data or keying material that can be traveled over the network reveals that huge secret information is traveling over the network. QKD has a weak approach for this kind of implementation because it has point to point link between the communicating devices that depict that underlying relationship is key distribution.

6 Quantum Key Distribution

We explain how the QKD works with the help of an example: We have sender Aamir and receiver Tehseen and an eavesdropper Sijjad. When Aamir starts sending the message to Tehseen using the photons that are fired by the photon gun to send a stream of photons in the agreed sequence between the sender and receiver, these photons use one of the four polarizations that may be horizontal, vertical or diagonal. Now, for every photon, Tehseen applies a filter and measures the polarization of the received photons and retains the record of these logs for that the measurements are correct as the polarization selected by Aamir.
A portion of the stream may be changed during the transmission of the sequence of photons but we need only a small portion of the stream to build the key sequence for the one-time pad. Now Tehseen will send the confirmation to Aamir and inform him what measurements he received without informing him of the right or correct sequence of photon stream. The number of photons that are wrongly received will be rejected and the accurately measured photons are computed into the bits based on the polarization of photons.
These are the actual photons that are used to make a one-time pad for sending the encrypted data or information. Now both the sender and receiver will not be able to determine in advance the key that will be used as the key for communication. In this way, this Quantum technology makes it possible to securely exchange the key. The whole process is described below with the help of figure 3. Now Sijjad tries to sniff the channel and measure the state to retrieve the information that is transmitted over the channel. To sniff or measure the state of the polarized photons, he has to apply a randomly selected filter. No eavesdropper can accidentally or by chance select the right sequence of photons selected by the sender and receiver for communication between them. He may select the wrong sequence for measuring the state of the photons. When the attacker tries to filter the information with a wrongly selected filter, this attack will change the polarization of these transmitted photons and, in this way, both the sender and receiver will detect the eaves-

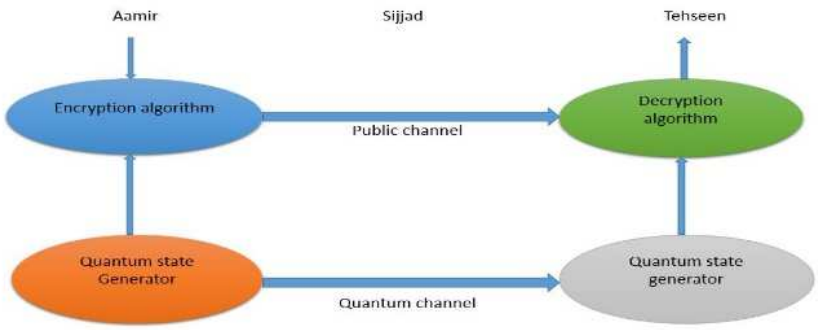

Figure 3: Quantum Key Distribution

dropper attack.

7 Challenges and the Future of Quantum Key Distribution

The most important challenge is the limited distance over which the QKD mechanism can be used. The reason is that when we try to send the key over a long distance, the polarization of photons may change due to various factors like when we try to amplify the qubits then this amplifier will destroy the state of polarization of these photons. We can only use QKD over a distance of 10 kilometers.

Another challenge of QKD is a lack of security or the standardization of the process or equipment. No doubt QKD has theoretically very strong security but there is a need for secure implementation of this technology.

As the computation is done by Quantum Cryptography is very slow, we cannot use this technology for a bulk amount of data for transmission from sender to receiver. We can use this technology only for the communication of the key. Algorithms, like those of RSA and Diffie-Hellman, are used for key exchange between the communicating remote parties. Asymmetric encryption is very slow compared to symmetric encryption. That is why a hybrid approach is adopted by many organizations to improve the speed of the key exchange. Public key encryption, like those of RSA and Diffie-Hellman, are not mathematically sound but these algorithms are considered more secure.

8 Conclusion

QKD technology cannot show more progress or gain its objectives without the participation of the research community of the network. There is a constant threat or challenge of increasing the processing capabilities of the modern or upcoming technology for current work on cryptographic algorithms like AES, SHA, and other types of cryptographic systems. This technology advancement also provides a means of securing communication networks.
DARPA is planning to develop the number of QKD links that will merge into the main QKD network and these different ends of QKD networks connected via a mesh of QKD relays or routers. There is continuous effort of the DARPA QKD network to make it more resistant against eavesdropping or DOS attack. This type of network is also referred to as a "key transport network" .
The shorter distance on which QKD networks can be implemented is the main limitation of the QKD network. To extend the distance we have to apply repeaters that change the orientation and polarization of the photons but that is challenging.
For now, to overcome the limitation of the shorter distance, one can use "chain Quantum Cryptography " connections with other secured networks. Satellite Technology may offer a solution to overcome the shorter distance problem. In this case, the satellite can act as a station and the photon has to face low attenuation in free space. This area of search is still open in the United States and Europe.
Many advances had occurred in the field of QKD and research in this area is continuing as it is expected to play a vital role in business, government institutions, and personal lives.

Acknowledgment. The research work is financially supported by the national high technology 863 programs of china (no.2015AA124103) and national key R & D program (no. 2016YFB05502001) and carried out in state key laboratory intelligent communication, Navigation, and micro-Nano system, Beijing University of Posts and Communications, Beijing.

References

[1] Carlo Ottaviani, Stefano Pirandola, General immunity and super additivity of two-way Gaussian Quantum Cryptography, *Scientific reports,* **6,** (2016), 22225.

[2] Paul Jouguet, Kunz-Jacques Sébastien, Anthony Leverrier, Philippe Grangier, Eleni Diamanti, Experimental demonstration of long-distance continuous-variable Quantum key distribution, *Nature Photonics,* **7,** no. 5, (2013), 378-381.

[3] Daniel J. Bernstein, Tanja Lange, Post-Quantum Cryptography, *Nature,* **549,** no. 7671, (2017), 188–194.

[4] Priyanka Bhatia, Sumbaly Ronak, Framework for wireless network security using Quantum Cryptography, *arXiv preprint arXiv: 1412.2495*, (2014).

[5] Carlo Ottaviani, Stefano Mancini, Stefano Pirandola, Two-way Gaussian Quantum Cryptography against coherent attacks in direct reconciliation, *Physical Review,* **92,** no. 6, (2015), 062323.

[6] Stefano Pirandola, Carlo Ottaviani, Gaetana Spedalieri, Christian Weedbrook, Samuel L. Braunstein, Seth Lloyd, Tobias Gehring, Christian S. Jacobsen, Ulrik L. Andersen, High-rate measurement-device-independent Quantum Cryptography, *Nature Photonics,* **9,** no. 6, (2015), 397–402.

[7] Sebastian Etcheverry, Gustavo Cañas, E. S. Gómez, W. A. T. Nogueira, C. Saavedra, G. B. Xavier, Gustavo Lima, Quantum key distribution session with 16-dimensional photonic states, *Scientific reports,* **3,** (2013), 2316.

[8] Hoi-Kwong Lo, Marcos Curty, Kiyoshi Tamaki, Secure Quantum key distribution, *Nature Photonics,* **8,** no. 8, (2014), 595.

[9] Alicia Sit, Robert Fickler, Fatimah Alsaiari, Frédéric Bouchard, Hugo Larocque, Patrick Gregg, Lu Yan, Robert W. Boyd, Siddharth Ramachandran, Ebrahim Karimi, Quantum Cryptography with structured photons through a vortex fiber, *Optics letters,* **43,** no. 17, (2018), 4108–4111.

[10] Sergiy Gnatyuk, Tetyana Zhmurko, Pawel Falat, Efficiency increasing method for Quantum secure direct communication protocols, In *2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications,* **1,** 2015, 468–472.

[11] Anne Broadbent, Christian Schaffner, Quantum Cryptography beyond Quantum key distribution, *Designs, Codes and Cryptography,* **78,** no. 1, (2016), 351–382.

[12] Wei-Wei Zhang, Ke-Jia Zhang, Cryptanalysis and improvement of the Quantum private comparison protocol with semi-honest third party, *Quantum information processing,* **12,** no. 5, (2013), 1981–1990

[13] Chip Elliott, Henry Yeh, DARPA Quantum network testbed, BBN Technologies, Cambridge, MA, 2007.