International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Quantum Cryptography and Its Application

Er. Rishabh Sharma, Er. Purva Paroch*

Government College of Engineering and Technology,Jammu
*Email: Rishabhsharmasr74359@gmail.com

ABSTRACT

Cryptography is the process of hiding information. It is used for secure communication between sender and the receiver. Cryptography provides the confidentiality and integrity of messages and sensitive data. Now a days only cryptography is not sufficient. So the new technique is introduced called Quantum cryptography. It is assured that quantum encryption methods and quantum key distribution makes our data more secure and safe.

INTRODUCTION

Cryptography is the process of hiding information. It is used for secure communication between sender and the receiver. Cryptography provides the confidentiality and integrity of messages and sensitive data. The secret messages are made by transforming the plain text into cipher text and the process is called encryption. The process of changing the unreadable cipher text back into plain text is called decryption.

By using a secret ‘key’, the cryptographers can hide and un-hide the information. Key is the information used in the cipher only known to sender and receiver. Cryptography is of two types “symmetric key” and “asymmetric key” cryptography:

1. The symmetric key cryptography in which the same key is used for both encryption and decryption and that key is only known to sender and receiver. Symmetric key cryptography also name as shared key cryptography.

2. The asymmetric key cryptography is more complex in which two keys are used, one for encryption and another for decryption. Asymmetric key cryptography also name as Public key cryptography.

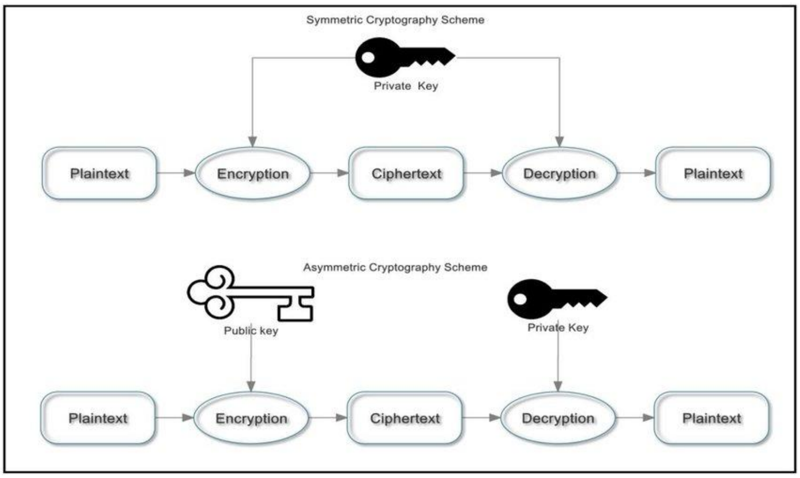


Fig1.

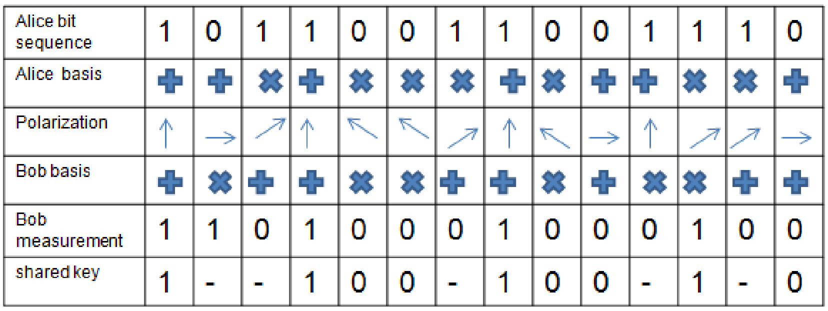
2. QUANTUM CRYPTOGRAPHY

Quantum cryptography is the technology that uses quantum mechanical properties to perform cryptologic tasks. Quantum cryptography was first proposed by Stephen Weisner in the early 1970s. In 1984, the two scientists Bennet and Brassard, who were familiar with Weisner's ideas, produced the first quantum cryptographic protocol called BB84. Cryptography is necessary but not sufficient for secure communication. By using quantum cryptography techniques, we can achieve more secure communication and transmission between the two parties. Quantum cryptography works on the principle of quantum mechanics for secure transmission. In simple computing the information is simply stored in bits, and in quantum computing bits called qubits store both binary values 0 and 1 at the same time. For secure communication the important part is the key which is used for both encryption and decryption. By quantum cryptography we can easily distribute the key between two parties with high security therefore it is also called

Quantum key distribution. Quantum cryptography can be done by exploiting the properties of light particles such as photons. The photons have chosen bases of polarization and result can be measured according to the bases like:

- Horizontal or Vertical (Rectilinear)
- Diagonal (45° or 135°)

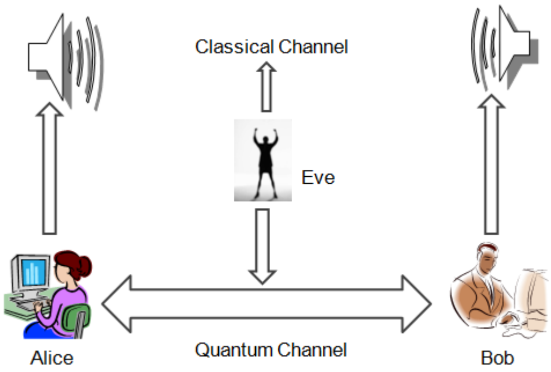
A photon is a light particle or packet of light. A photon has a property of polarisation. Quantum cryptography is based on two quantum mechanisms - photon polarisation property and Heisenberg uncertainty principle. According to Heisenberg Uncertainty principle, it is not possible to measure the quantum state of any system without disturbing that particular system. The polarization of photon can be known only at the time when it is measured. This plays a vital role in preventing the eavesdropping in quantum cryptography. The photon filter can only detect correct polarization and other photons will be destroyed. Conversion and polarisation take place in quantum cryptography. Conversion means converting the 0s and 1s and these bits are transferred by using polarized photons. Photons or light particles are sent by the sender and these photons are placed at particular quantum state which will be received by the receiver. A photon polarization can be in one of these four 0, 45, 90,135. A photon will be measured by using different filters or bases i.e. vertical or horizontal (rectilinear) and diagonal. The receiver can differentiate the polarized photon between 0° and 90° polarization or 135° and 45°.



Alice bit sequence	1	0	1	1	0	0	1	1	0	0	1	1	1	0
Alice basis	+	+	×	+	×	×	×	+	×	+	+	×	×	+
Polarization	↑	→	↗	↑	↖	↖	↗	↑	↖	→	↑	↗	↗	→
Bob basis	+	×	+	+	×	×	+	+	×	+	×	×	+	+
Bob measurement	1	1	0	1	0	0	0	1	0	0	0	1	0	0
shared key	1	-	-	1	0	0	-	1	0	0	-	1	-	0

Fig 2.1

Quantum key distribution model, sender is Alice, receiver is Bob and the eavesdropper is Eve shown in figure.Alice starts a communication by sending a message to Bob using a stream of photons choosing one of the polarizations out of 40,90,0 and 135. Bob chooses the bases (rectilinear or diagonal) and measures polarised state of each photon. Bob tells Alice about the sequence of bases by using some classical method. Alice also responds about the sequence of bases to be correct. Alice and Bob both only select the correct observation and all others are discarded. The correctly chosen observations are set to binary 0, 135 is set to 0 and 45 and 90 are set to 1.



If the eavesdropping is taking place, both sender (Alice) and receiver (Bob) detect the eavesdropper in between the communication. As we know the polarization measurement is not taking place by destroying the photon. So if Eve is eavesdropping the message, he/she will have to send a new photon to Bob so that Bob cannot detect the presence of Eve. But Eve does not know the state and polarization so there is a possibility of error. Alice and Bob share the sequence in between by using classical channel due to which error occurs in the bit sequence and they detect that there is eavesdropper in between them which is intercepting the communication.

3.APPLICATIONS

3.1. Secure Voting System

Voting is a very important part of elections and important for political stability in a country. Developed countries use quantum cryptography for secure online voting. In 2007, Switzerland used quantum cryptography for online voting in its regional elections. In Geneva, votes are encrypted at a central vote-counting station and the results are transferred through a dedicated optical fiber channel to a remote data storage facility. The v results are safe through quantum cryptography.

3.2. Communication in Space

In order to communicate with satellites and astronauts securely, many developed countries use quantum cryptography in space research program. China launched a quantum communication satellite name Micius in 2016. After one year China used Micius for QKD between Beijing and Vienna. In India, DRDO and IIT Delhi successfully tested QKD mechanism between 2 cities that were a distance of more than 100km from each other.

3.3. Health Sector

In medicine and health sector it plays an important role. The industrialized countries which prepare medicines can transmit various techniques and secret documents related to medicine and health. By using QKD, countries can communicate or transmit data securely.

4. CONCLUSION

It is concluded that to transmit sensitive information between two or more points, some stronger technique is needed. It is assured that quantum encryption methods and quantum key distribution will allow us to secure information more effectively in the future. Based on quantum mechanics and classical cryptography, quantum cryptography is a novel approach in the field of cryptography. In particular, quantum cryptography provides security for various applications (e.g., Internet of things and smart cities), in cyberspace for the future Internet. In future this technology is safest in cyber field.

REFERENCES

- https://www.ijeat.org/wp content/uploads/papers/v3i4/D2988043414.pdf Dr. N.Sasirekha, Dr. M. Hemaltha
- https://cs.stanford.edu/people/adityaj/QuantumCryptography.pdf J. Aditya, P. Shankar Rao {Dept of CSE, Andhra University}
- Security and Communication Networks Volume
- Understanding Quantum Cryptography
- Quantum Safe Cryptography and Security
- https://www.imperial.ac.uk/media/imperial-college/research-centres-and-groups/theoretical-physics/msc/dissertations/2020/Yoann-Pietri-Dissertation.pdf