International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 07 | July - 2021 ISSN: 2582-3930

A Study on Quantum Cryptography

Aayush Garg, Sanya Sharma
Manav Rachna Institute of Research & Studies, Faridabad, India

ABSTRACT- This article addresses the introduction to quantum cryptography and its main distribution protocols that make this technique even better to use and more secure. Quantum cryptography is art and science to use the effects of quantum mechanics for cryptographic tasks, although the most renowned illustration of this is the quantum key distribution (QKD). Quantum cryptography uses the Quantum Key Distribution (QKD) and enables the users to detect the presence of eavesdroppers. In this review article, we survey the area of theoretical quantum cryptography and some of its well-known protocols. This paper focuses on how quantum cryptography is better than modern cryptography and how the vision of fast and secured internet could be attained. We even focus on various applications such as securing the communication with space and ultra-secure voting we even have various key exchange methods such as BB84 protocol, B92 protocol, decoy-state protocol, etc.

Keywords- Quantum Cryptography, Quantum Key Distribution, Quantum Key Distribution Protocols

I. INTRODUCTION

Cryptography is an art of converting unblended or plain text into blended or cipher-text and vice-versa. It is specifically encryption and decryption of data. It was first used by Egyptians 4000 years ago, in the form of the hieroglyph for transmitting messages by the kings, later Romans used the Ceaser-cipher method. Modern cryptography is based on mathematics and is based on the difficulty of calculating the factorization of a large number. The security of modern cryptography is based on the great complexity of the mathematical problem, for example, the factorization of large numbers. There are two types of Cryptography: Asymmetric Key Cryptography and Symmetric Key Cryptography. A key is a collection of bits of information that controls the operations of encryption and decryption.

Asymmetric Key Cryptography makes use of a pair of keys among which one is kept private and the other is public which makes it public-key cryptography. Asymmetric Key algorithmic techniques include RSA, ECC, Diffie-Hellman, ElGamal. It does not require an exchange of the key between parties.

Symmetric Key Cryptography makes use of only a single key for encryption and decryption purpose, which is shared between the sender and receiver both which makes it secret-key cryptography. Symmetric Key Algorithmic Techniques include Blowfish, AES, RC4, DES, RC5, and RC6. It involves the exchange of the key between parties.

The primary functions of cryptography are privacy, authenticity, integrity, non-repudiation, and key exchange. Secure key exchange is one of the biggest problems faced and Cryptographers endeavors methods to secure the message but intruder keeps on working to crack the systems by gaining access to the key and to overcome this Quantum Cryptography was instigated. Quantum Cryptography makes it hard for the eavesdropper to decrypt the key transmitted and alerts the end-users of interruption if any. But, this technique cannot transmit the key for a long distance and is very expensive in use which makes it a limitation but studies are being carried on to resolve these limitations.

II. QUANTUM CRYPTOGRAPHY

Unlike conventional public-key cryptography, quantum cryptography is based on the fundamental principles of quantum mechanics, which is based on the difficulties of calculating certain mathematical functions and at no point in the communication process can it indicate listening or mathematical proof of the real complexity of the inversion of the one-way functions used.

It involves the use of quantum mechanical properties to implement cryptographic tasks. The idea of quantum cryptography was first devised in 1970 by Stephen Wiesner. It allows the user to install a secret key and perceive if an eavesdropper has transpired.

Quantum cryptography doesn't depend on mathematical problems; it frames on two backbones of 20th-century quantum mechanics:

a) Heisenberg Uncertainty Principle
b) Principle of Photon Polarization

Heisenberg Uncertainty Principle: Computing the quantum state of any system isn't feasible without interrupting that system. Photon's polarization can be known at a measured point. The main objective of this principle is to block the efforts of eavesdroppers in a cryptosystem based on quantum cryptography.

Principle of Photon Polarization: It describes how photons are polarized into specific directions. Though a photon filter with correct polarization can either identify a polarized photon or destroy the photon.

This unilateralism of photons along with Heisenberg Uncertainty Principle makes an appealing option to ensure

privacy and vanquish eavesdroppers. The best example of quantum cryptography is quantum key distribution.

Table I - Modern Cryptography v/s Quantum Cryptography

Parameters	Modern Cryptography	Quantum Cryptography
Basis	Mathematical Fundamentals	Quantum Mechanics
Existing Usage	Widely used	Futuristic
Digital Signature	Present	Absent
Bit Rate	Depends on Computing Power	Average Rate is 1Mbits per sec
Range	Less than a few 100miles	Millions of miles
Bit Storage	2n n-bit string	One n-bit string
Expenses	Less Expensive	Highly Expensive

III. QUANTUM KEY DISTRIBUTION

It is a method that secures the exchange of keys by the laws of physics between at least two parties.
It involves the generation of a random key by the quantum engine and its transmission as a beam of photons through optical fibers to the intended recipient. If anyone tries to interrupt the transmission, the polarity of the photons changes, and the system gets alerted and the key gets disrupted. Quantum Key Distribution ensures security where classical cryptography doesn't.
Considering the example of Alice as a sender and Bob as a receiver: Usually, the data is ciphered on single photons. Alice classic cryptography doesn't consider having options of either opting to cipher these in a bit sequence using one state like horizontal or vertical polarization or opting to cipher in two different states +45° and -45°. Then Bob either assesses horizontal, vertical or he assesses -45°, +45°. If Bob assesses what Alice opted then they will have harmonized outcomes if not then it will be relinquished.
E.g.: Alice sends vertical and Bob assesses vertical then these are kept. This step lets Alice and Bob converse without babbling any information and becomes the secret key.
Once a secret key is induced then it's consolidated into cryptographic protocols assuring the security of the application where it's used. If an interloper tries to obstruct the key generation errors will instigate and they will divulge themselves.

IV. KEY PROTOCOLS OF QUANTUM KEY DISTRIBUTION

1.) *BB84 Protocol*- BB84 was the first protocol of quantum cryptography devised in 1984 by Charles Bennet and Gilles Brassard and was mainly dependent on the Heisenberg's Uncertainty Principle. It uses the polarization state of the individual photons to encode the key bits. The two-component bases of this protocol are Rectilinear (R) and Diagonal (D) as well as four states of polarized photons. 0° and 45° of the polarized photon in rectilinear and diagonal basis respectively represent as binary 0. Whereas, 90° and 135° represent binary 1.

Bases	Angle	Binary Bit	Photon
+	0°	0	↔
✖	45°	0	↗
+	90°	1	⇳
✖	135°	1	↖

Fig 1: BB84 Protocol

2.) *B92 Protocol*-The B92 Protocol was devised in 1992 by Charles H. Bennet. It stated the use of two non-orthogonal states instead of the four polarization states of photons used earlier in BB84 without affecting the security of transmission

against eavesdropping. It uses two bases, one rectilinear and the other diagonal. The polarization 0^0 in the rectilinear base denotes binary 0 and 45^0 in the diagonal base denotes binary 1.

Bases	Angle	Binary Bit	Photon
✖	0°	0	⇿
+	45°	1	↗

Fig 2: B92 Protocol

3.) Decoy State Protocol- The decoy-state scheme was proposed by Hwang. Practical QKD systems use multi-photon sources; in deco- state technique, this basic weakness of practical QKD systems is corrected by using multiple intensity levels at the source of the emitter, leading to varying statistics on the number of photons across the channel. For this reason, both legal parties can detect a PNS attack with significantly increased secure transmission rates or maximum channel lengths, making QKD systems suitable for practical applications.

4.) SARG04 Protocol- SARG04 protocol was devised in 2004 by Scaraniet.al The researchers produce SARG04 when they discovered that using the four BB84 states with different information encoding could develop a new protocol that would be more robust, especially against PNS attacks, when diminished laser pulses are used instead of single photons source.

5.) Six-State Protocol- The six-state protocol was instigated in 1999 by Pasquinucci and Nicolas Gisin. BB84 quantum utilizes a six-state polarization design on three orthogonal bases and six-state protocol is a variety of BB84. The six-state protocol is a distinct variable protocol for the allocation of quantum keys, allowing a stronger channel to be endured than the BB84 protocol. Without a quantum computer, the execution of the six-state protocol can only be by operating optical technologies.

V. ULTIMATUMS for QUANTUM KEY DISTRIBUTION PRACTICAL SUCCESS

1.) *Key Rate*: To increase the practical future applications of quantum cryptography, we need a higher secure key rate. But practically, applications require less bandwidth, whereas to provide services to a larger number of people we need large bandwidth and the key rate needs several updates to be high and secure. The final key rate depends on the type of protocols used for the transmission, as the slowest layer of the protocols decides the key rate.

For high secure key rates we need:

a) Optical fiber channels with less loss
b) Sifting electronics which has can handle greater raw counts
c) A powerful stabilized hardware
d) Error Correction implementations with little information loss.
e) Both, privacy amplification and error correction should have greater data throughput.

2.) *Communicable Distance*: Increasing the range of communication of Quantum Key Distribution is one of the major challenges with the growing world. The single-photon detection system of Quantum key distribution enables point to point communication over a comparatively small distance, where low noise of the single-photon plays the enabling role. But when the distance of a point to point communication is to be increased, the channel loss will diminish the key rate to very low practical bearing level.

Table II - Comparison between different QKD protocols

Features	BB84	B92	Decoy-State	SARG04	Six-State(SSP)
Founder	Charles Bennet and Gilles Brassard	Charles H. Bennet.	Hwang	Scaraniet.al	Pasquinucci and Nicolas Gisin
Year	1984	1992	2003	2004	1999
Number of States	4	2	2	4	6
Polarization	Orthogonal	Non-Orthogonal	Novel high speed	Orthogonal	Orthogonal
Efficiency	Low	Best	Very Good	Average	Good

VI. APPLICATIONS OF QUANTUM CRYPTOGRAPHY

1) *Secure Communications with Space:* Objective of securing communication with astronauts and satellites regardless of the intelligence to which a contender has approached. Quantum cryptography never performed over many prolonged intervals. Chinese Satellite the micius changed that. The first intercontinental Quantum cryptography amenity was structured by this satellite. A secured video conference was set up between China and Europe where the laws of physics guaranteed security. A One-time pad is what Quantum cryptography leans on. Assurance of the key that it's not copied by an eavesdropper while the transmission between sender and receiver is the problem with one-time pads. This is where the quantum particles resolve the problem by transmitting the key using quantum particles. The receiver receives the same one time pad from micius that was sent from Chinese ground station encrypted photons using established protocols.

2) *Quantum Internet*: The Internet today is comparatively speedy but insufficient when it comes to security. Switching to quantum encrypted internet will attain the vision of speedy as well as secured internet.

3) *Ultra Secure Voting:* Ciphering votes and channeling the results over optical fiber to a data storage facility. Quantum cryptography assures the vote results. Geneva Switzerland was the first to use quantum cryptography to encrypt ballots. Quantum cryptography was emerged at the University of Geneva by Id Quantique and Professor Nicolas Gisin. The cryptographic structure secures the link between ballot counting stations and government data centers.
Public election totals are imparted using quantum cryptographic structures. Exchange of secret keys for perceiving any eavesdropping on the communication surge.

4) *Smarter Power Grid*: The American power grid is the most endangered target for a cyber assault. A smart electricity grid is controlled by a small encryption device that helps to channel secured signals using public data networks. With appropriate provision, it's remarkably more secure than traditional grids.

VII. LIMITATIONS OF QUANTUM CRYPTOGRAPHY

a) Practical devices are not ideal, introducing noise disturbances in communication, results in contradiction of the data.
b) It is difficult to produce a perfect single-photon pulse.
c) Due to the non-uniform selection of bases, the efficiency of the string bit sequence to be used as the key decreases.
d) It lacks vital features such as digital signatures.
e) While computing through the channel polarization of a photon may change.

VIII. CONCLUSION

For transmission of any important data between two parties, there is a need for some resistant technique that can transmit the key safely from the eavesdroppers. Quantum cryptography and its ciphering techniques help us secure important information persuasively. Quantum cryptography is a move that makes us feel more firm about the data we share. Quantum cryptography isn't based on mathematical problems, it is based on principles of quantum mechanics. Quantum cryptography is being used in various ways such as securing communication with space, quantum internet, ultra-secure voting, and the smart power grid. There are various ways for the execution of quantum key exchanges such as B92 protocol, BB84 protocol, decoy-state protocol, SARG04 protocol, etc. that make it even more secure. Thus, we conclude that Quantum Cryptography is one of the best techniques and it is something that the future can rely on.

REFERENCES

[1] Anne Broadbent and Christian Schaffner, *Quantum Cryptography beyond Quantum Key Distribution*, December 2015

[2] J. Aditya, P. Shankar Rao, *Quantum Cryptography*, Dept of cse, Andhra University

[3] N.Sasirekha, M.Hemalatha, *Quantum Cryptography using Quantum Key Distribution and its Applications* in International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-3, Issue-4, April 2014

[4] D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan, and M. Schauer, *Quantum Cryptography* University of California, Physics Division, Los Alamos National Laboratory Los Alamos, NM 87545

[5] Priyanka M., Dr. Urbasi Sinha, *Study of BB84 QKD protocol: Modifications and attacks,* Kerala

[6] Eleni Diamanti, Hoi-Kwong Lo, Bing Qi, and Zhiliang Yuan, *Practical challenges in quantum key distribution,* Quantum Information (2016) 2, 16025; published online 8 November 2016

[7] Aakash Goyal, Sapna Aggarwal and Aanchal Jain, *Quantum Cryptography & its Comparison with Classical Cryptography: A Review Paper,*

[8] Gabriela Mogos, *Quantum Key Distribution Protocol with Four-State Systems – Software Implementation*, Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015)

[9] Tianqi Zhou, Jian Shen, Xiong Li, Chen Wang and Jun Shen, *Quantum Cryptography for the Future Internet and the Security Analysis,* Hindawi Security and Communication, Networks Volume 2018, Article ID 8214619, 7 pages https://doi.org/10.1155/2018/8214619

[10] Igor Tselniker, *Eavesdropping in Quantum Cryptography - BB84 vs. Six States,* 236823 - Seminar in Quantum Information processing.

[11] Dagmar Bruß, *Optimal eavesdropping in quantum cryptography with six states,* ISI, Villa Gualino, VialeSettimioSevero 65, 10133 Torino, Italy

[12] Xiangjun Xin, Xiaolin Hua, Chaoyang Li and Dongsheng Chen, *Quantum Authentication of Classical Messages Using Non-orthogonal Qubits and Hash Function,* International Journal of u- and e-Service, Science and Technology Vol.9, No. 10 (2016), pp.181-186 http://dx.doi.org/10.14257/ijunesst.2016.9.10.17

[13] Xiangjun, Chaoyang Li , Dongsheng Chen and Fagen Li, *Quantum Authentication Protocol of Classical Messages Based on Different Sets of Orthogonal Quantum States,* International Journal of Future Generation Communication and Networking Vol. 9, No. 5 (2016), pp. 123-130 http://dx.doi.org/10.14257/ijfgcn.2016.9.5.12

[14] Maithili S. Jha, Samrit Kumar Maity, Manish Kumar Nirmal, Jaya Krishna, *A survey on quantum cryptography and quantum key distribution protocols* at International Journal of Advance Research, Ideas and Innovations in Technology ISSN: 2454-132X Impact factor: 4.295 (Volume 5, Issue 1)

[15] Saha, Kaushik, Ghosh, Sirshendu Sekhar, Shaw, Dilip Kumar, *QUANTUM KEY DISTRIBUTION SCHEME: AN IMPROVEMENT BASED ON BB84 PROTOCOL,* International Journal Of Advanced Research in Computer Science, Volume 9, No.2, March 2018, DOI:10.26483/ijarcs.v9i2.5

[16] Z. L. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. W. Sharpe, A. R. Dixon, E. Lavelle, J. F. Dynes, A. Murakami, M. Kujiraoka, M. Lucamarini, Y. Tanizawa, H. Sato, and A. J. Shields,*10 Mb/s quantum key distribution,*https://arxiv.org/pdf/1807.04484.pdf

[17] A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, S. Tam, Z. L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki, and A. J. Shields, *High-speed prototype quantum key distribution system and long term field trial,*23 Mar 2015 | Vol. 23, No. 6 | DOI:10.1364/OE.23.007583 | OPTICS EXPRESS 7583