Journal of Management and Service Science, 2021,
Vol. 01, Iss. 01, S. No. 004, pp. 1-12

Quantum Cryptography: The Future of Internet and Security Management

Faisal Abbasi[1], Pawan Singh[2]

Amity School of Engineering and technology, Amity University, Lucknow, India[1,2]
faisalabbas2599@hotmail.com[1], pawansingh51279@gmail.com[2]

How to cite this paper: F. Abbasi and P. Singh (2021) Quantum Cryptography: The Future of Internet and Security Management. *Journal of Management and Service Science,* **1(1)**, 4, pp. 1-12.

https://doi.org/10.54060/JMSS/001.01.004

Received: 24/02/2021
Accepted: 08/03/2021
Published: 10/03/2021

Abstract

In today's world, cryptography techniques are used and implemented on the elementary method of finding the prime factor of large integer, which is said to be "Inevitable to Track". But living in an era where nothing is impossible to achieve, so cryptographic techniques are exposed to both technologies' advancement in computational power of machines and advancement in the fields of mathematics to break the notion that factoring of large integers into their prime is impossible. To cope up with the threat that cryptography will face is handled by fusion of physics into cryptography, leading to the evolution of Quantum Cryptography. It is one of the fast-growing fields in computer technology. In this paper, I am going to brief the concepts of Quantum Cryptography and how this technology has led to the development of the strategy of complete secure key distribution. The paper covers the loophole present in the modern cryptography techniques, the fundamental principle of quantum cryptography, its implementation in the real world along with the limitation faced in this field, and the possible future of quantum cryptography.

Keywords

Quantum, Cryptography, Intractable, Confidentiality

1. Introduction

Quantum Cryptography is the newly emerging field, still there is a lot of work to be done in this field. It is growing pace to achieve more secure transmission of data. The quantum cryptography came into the light when recently a European Union member announced to invest huge amount of $15 million in development of a communication system that will not face threats due to development of computational power of machines and advancements of mathematics. The only option available for now is quantum cryptography.

Quantum cryptography is still in its initial phase. But still its importance cannot be ignored or underestimated [1-2]. In 1994, there was a famous mathematician Shor who has given the quantum cryptography algorithms by which integer factorization problem can be solved in polynomial time. One should keep in mind that till now no researchers has not found any

classical algorithm that can efficiently decompose the large integer into its factor under Turing machine model [5]. Therefore, the challenges of the emergence of quantum computers to the traditional cryptosystems cannot be ignored even if it is still in its infancy.

The technology in which they were investing is based on Quantum Cryptography known as SECOQC (Secure Communication based on quantum cryptography) [6]. It was developed to use as a defense against the Echelon intelligence (a surveillance program) system used by United States, Australia, Britain, and many other countries. Some of the giant company in quantum information process technologies like MagiQ Technology and ID Qu antique, are using quantum cryptography to fulfill the requirements of businesses-based communication, keeping governments communication secure from other organization, and other institutions where secrecy and unauthorized access of information plays the crucial factor. It has gained success in managing secrecy of institution over any adversaries. So, there must be a question in a mind if the modern cryptography is called "INTRACTABLE" then what is the need of spending lots of money on quantum cryptography. In next section it is elaborated why it is important…Stay focused.

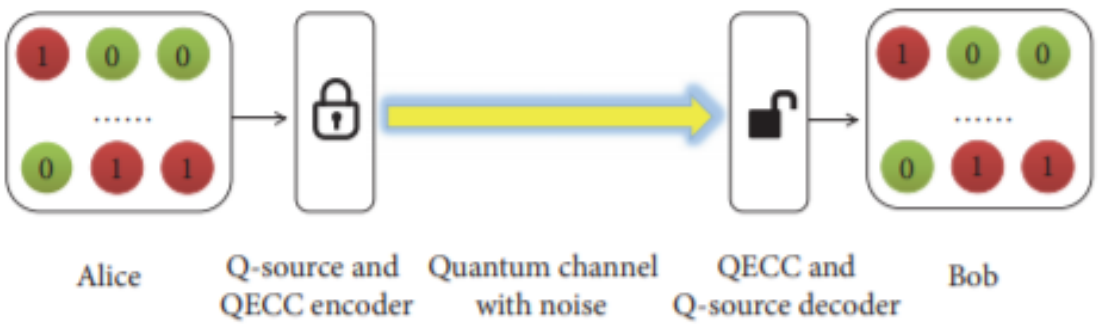

Figure 1. Cryptography

2. Limitation of Modern Cryptography

In cryptography techniques the concept used is public key which mainly deals with the complex calculations which are slow in performance and they are developed on public key exchange, not focused on the encryption of huge amount of data [1]. The cryptography techniques which are used now a days are based on distributed symmetric key among communicators. But symmetric encryption is quite faster than asymmetric encryption, therefore fusion of both these key encryptions (combining the concept of symmetric and asymmetric encryption) give us the advantage of speed of a shared key system and the secrecy of a public key [7].

Thus, this approach maximizes the speed, performance, and scalability of private key infrastructure. The cryptography techniques which are used now a days are not based on any mathematical proof rather it is considered secure because of years of inspection of process of factoring the large integer into its prime is found to be "intractable". It means that if anyone get successful in breaking the integer into its prime by that time data which have been protected would loss its value. The basic reason for its trustworthiness is that even if anyone is given computational power then also there is no mathematical operation for quick factoring of these integers [8].

Though todays cryptosystem is secured now but, in the future, there is the possibility of cracking it and there are other risk factors also some of them are:

- Quantum computing may defeat the modern cryptography techniques.
- Advancement in technology has made breaking of 56-bit DES algorithm which was secure.

- The main problem with the existing cryptosystems is uncertainty of proof of factoring the integer.

This uncertainty can cause havoc in future if certain mathematical proof come out. It may cause risk in national security and privacy of the individuals. To conclude, the modern cryptography is exposed to numerous threats which are advancement of technology in the fields of computational power of computers and the evolutions of mathematics which if made public can collapse the whole the infrastructure on which the cryptography is build. It will cost billions of resources to repair the damage caused.

3. Quantum Cryptography in Theory

As seen above, the threat which are faced while using the concept of modern cryptography and its basis of factoring large integer. This led to the development of new technology called quantum cryptography. The quantum cryptography uses the fundamental and unchanging concepts of quantum physics. There are two fundamentals on which it works:

- The famous Heisenberg Uncertainty principal
- Principal of Polarization of photon

The Heisenberg uncertainty principal describes that one cannot measure the states of any system without disturbing the system. The polarization of photon can be known only when it is measured at a point. These two principal play's important role in prevents the attempts of eavesdroppers to stole the data. Most importantly the principal of polarization states how photons can be polarized in specific direction. To identify that polarized photon, only a photon filters which has correct polarization can detect a polarize photons otherwise it will be destroyed.

This unique features of photons in addition with the Heisenberg principal make the quantum cryptography remarkable way of providing the protection of data and hoax eavesdroppers. Charles Bennet and Gillies Brassard were the first people to come up with the concept of quantum cryptography as part of their studies between physics and information. They give the theory that the encryption key used can be developed on depending on number of photons reaching the destination how they were received. They developed this concept on DUAL CHARACTERISTICS OF LIGHT (light can behave as particle nature and wave nature). one can polarize the light in different direction and these orientations can be represented in bits representing zero and ones. This bit's representation forms the foundation of quantum cryptography.

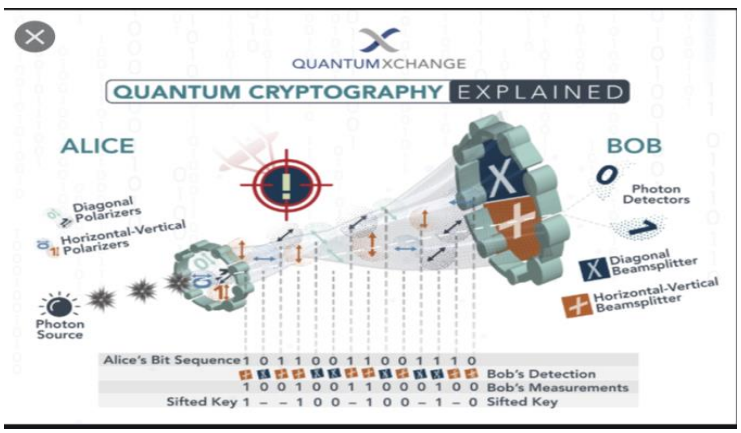

Figure 2. Quantum Cryptography

The strength of modern cryptography lies within the computational difficulty of factoring the large integer while the strength of quantum cryptography lies within the laws governing the physics thus this makes it independent of computational power of machines. The uncertainty which is faced in modern cryptography was resolved in quantum one as its bases on physics and this law are always true so no one can ever be able to hack the system for ages to come. This makes it a reliable cryptography technique.

4. Quantum Key Distribution Example

So, let us see with an example how quantum cryptography works. Cryptography is all about the distribution of keys. Suppose there is a sender named "MARK"; a receiver named "BOB" an imposter eavesdropper named "ANON". Mark has started a communication with Bob by sending the message by using a photon guns to send a stream of photon chosen in an arbitrary manner in one of the defined photon polarizations (HORIZONTAL, VERTICAL, DIAGONAL, OPPOSTIE DIRECTION). Every photon received, Bob will choose a filter in an arbitrary fashion and use a photon receiver to count and compute the polarization of light which can be any value as mentioned and maintain the record of this result based on which measurements correct depending on the polarization selected by Mark. When photon is transmitted, a small part of stream of photons will be deteriorated over the distance of communication and only the set of it is needed to build a key sequence for onetime pad. Once the key is built, Bob will communicate with Mark using some different band order to tell Mark about the type of measurements taken and how many calculations were correct by keeping the actual result hidden [9-11]. The photons with wrong measurements were removed and the correct measurements were used to form the bit pattern depending on the value of polarization.

One of key feature is that both the Bob and Mark will not be able to determine in advance what will be the key because it is purely randomly selected depending on the product of their choices. Thus, this makes this technology secured.

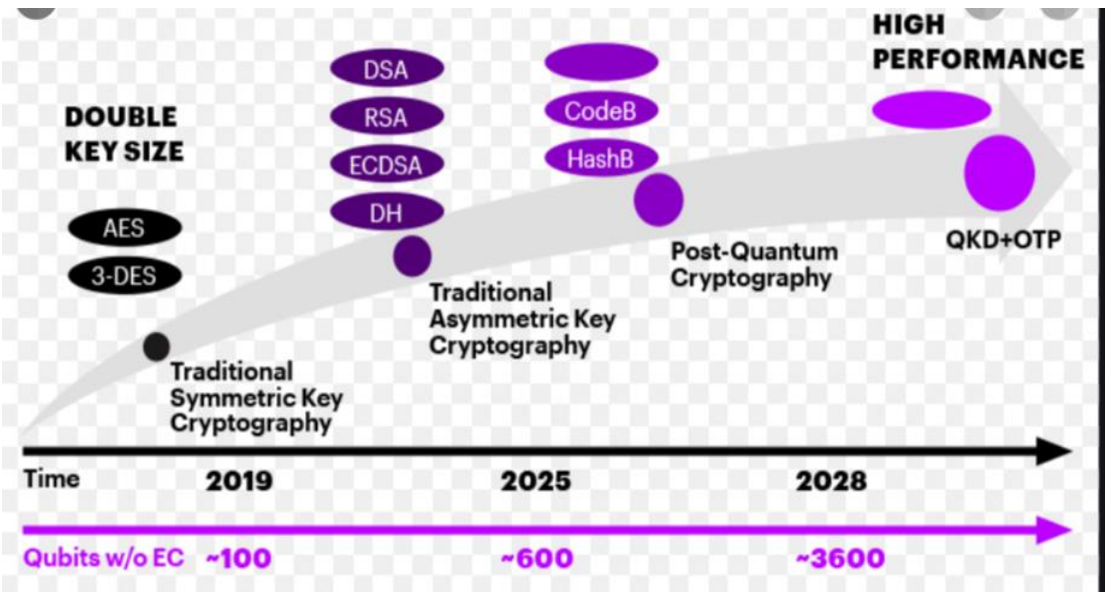

Figure 3. Quantum Processing.

Now assume that any imposter named EVE wants to eavesdrop on our cryptosystem and wants to get access to our quantum key distribution. To eavesdrop on our system, the attacker should also choose an arbitrary orientation of photon beam and after it should confirm it with the Mark's photons.

This provides the equal probability of selecting the correct and wrong filters, but the twist is that it will not be able to confirm with Mark about the type of filter used. This is an advantage that Bob carries over Eve that is even if Eve is having right photons, he must made it confirm with the Mark photons and without confirming it with Mark photon, the photons received by Eve will be of no use. They will serve no purpose to Eve As a consequence, the Eve will not be able to correctly interpret the messages thus will be defeated.

To conclude, the quantum cryptography has three advantages:

- First, the Heisenberg uncertainty principal means that one cannot duplicate the photons data and once the photon has hidden the detector it will be destroyed. Any tempering also will lead to the photon destruction.
- Secondly, Mark and Bob should decide before only the amount of photon they will be needed to form the encryption key. If Bob receives the smaller number of photons, he will get the clue that anyone is trafficking the route as the photon received by attacker will no longer exist to be received by Bob due to quantum nature.

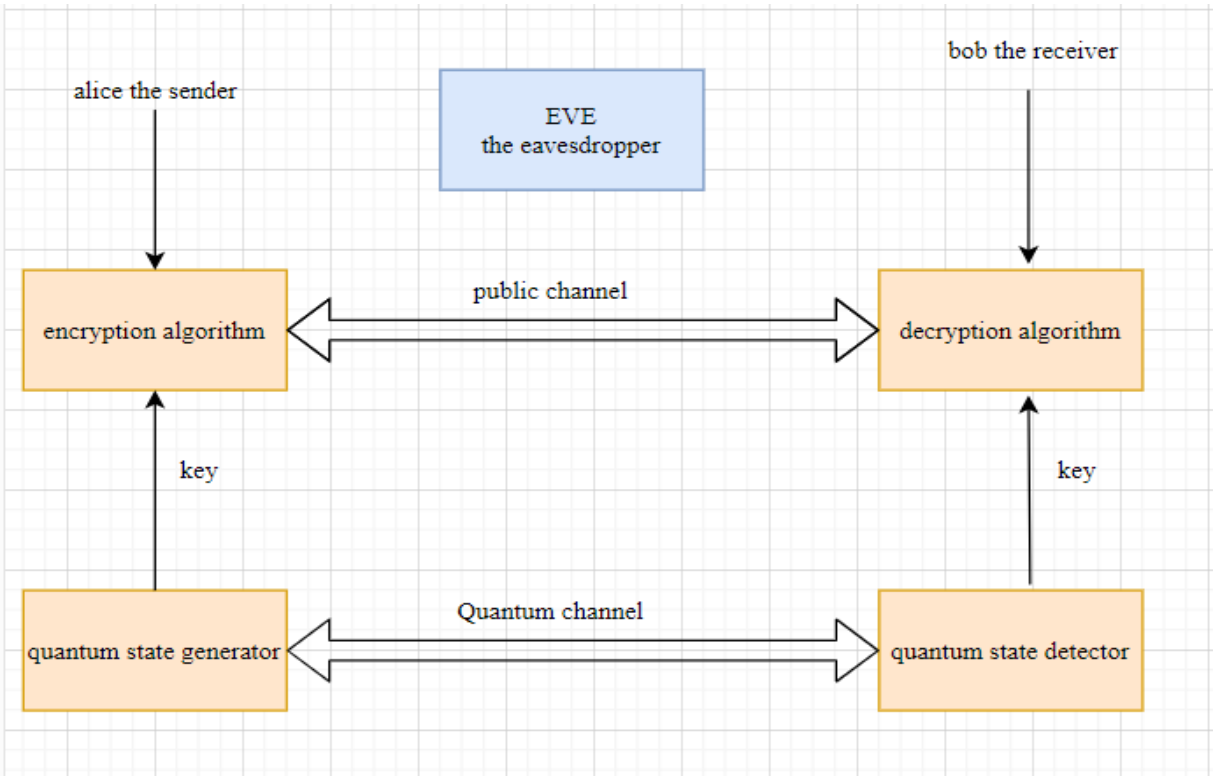

Figure 4. Quantum key Distribution.

5. Desirable Quantum Key Distribution Attributes

Quantum key distribution provides us the tool for reaching to an agreement upon shared arbitrary pattern of bits between two different devices, with a negligible probability that other devices can interfere with that bits. This bit forms the back-bone of quantum cryptography as it serves as secret key used for encrypting and decrypting of messages between the two devices. Let us throw some lights on the strength of quantum key distribution [12-14].

5.1. Confidentiality of keys

Being a key to remain confidential is one of the most important reason for researchers' interest in quantum key. Public key has the drawback of being uncertain principal governing it is working. It is based on the un-certainty that factoring of large integers is impossible due to absence of any concrete proof and that it is in-tractable. Many of the encryption meth-odology can be broken in future leading to havoc on earth. But quantum key distribution can solve this problem if it is properly implemented in the secure system as it pro-vides the automatic distribution of keys which have better security than the existing methodology.

5.2. Authentication

The authentication is not provided by quantum key distribution alone. Some of techniques used to provide the authentication are based on hash-based authentication schemes or hybrid approach (quantum key distribution -public key). Neither of the approach is completely resolving the issue. The advance knowledge of secret key needs a method to distribution of keys before the quantum key distribution start which not possible to achieve and the approach has the of hybrid inherits the loophole of public key distribution.

5.3. Sufficiently rapid key delivery

The distribution of key should be fast sufficiently for the devices(encryption) so that they do not lose their or exhaust their supply of key bits. It is defined as the rate at which key material put into place and the rate it used by the encryption/decryption devices (also known as throughput). The maximum rate reached by the quantum key distribution is 1000 bits/second in the real world, but it usually works at less rate than that. This is usually very low for many of the encryption technologies but fair enough for less secure systems.

5.4. Robustness

While developing the quantum key technology the researcher does not take in the account of robustness of system. It is one of the most important features of the system to provide secure and uninterrupted services. For the quantum key distribution, it important that the flow of keying material is not disturbed. Today the quantum key distribution work on point-to-point link. So, if that link is disturbed than or tampered by the eavesdropper the flowing material would to cease. In our view the mesh network will provide the more robustness [15-18.

5.5. Distance and location dependence

In present situation distance and location independence feature is missing in quantum key distribution so that is secure and robust path between the photons to few tens of kilometer through fiber unlike internet IPsec protocol.

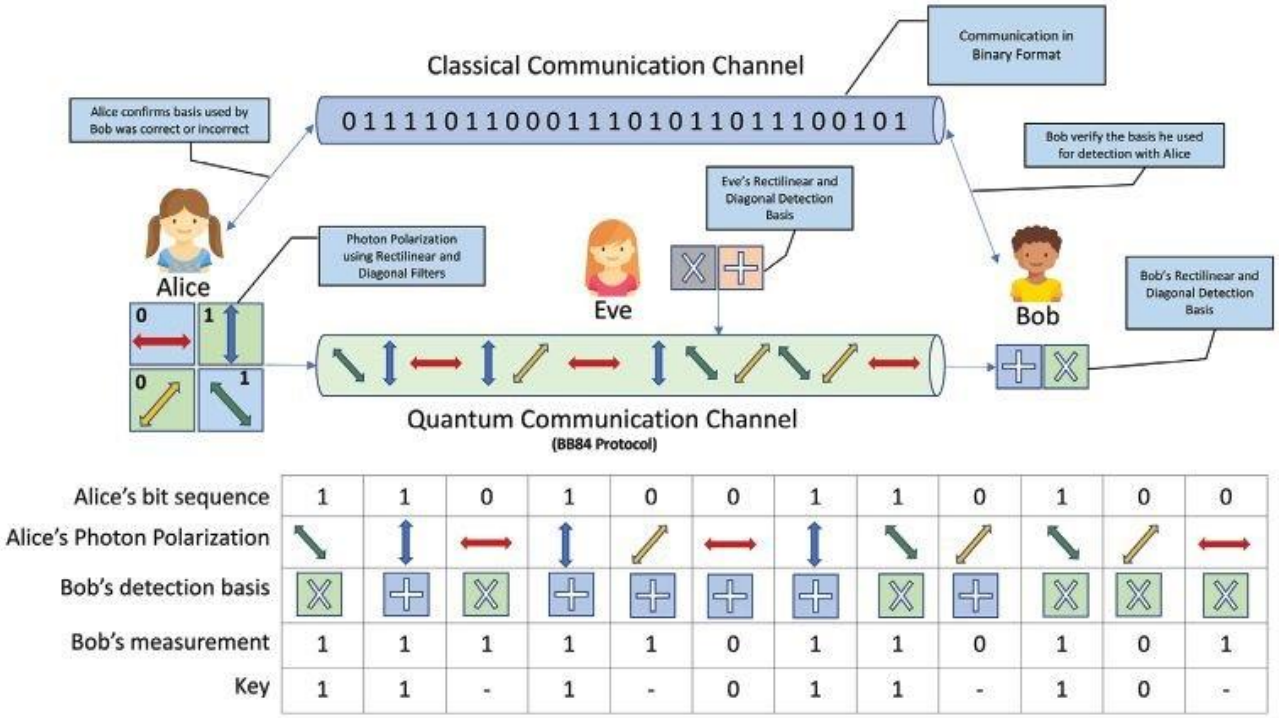

Figure 5. Quantum Cryptography Implementation

6. Implementation of Quantum Network

There is existing two technologies that have successfully implemented the quantum cryptography technologies.

6.1. The DARPA Quantum Network

DARPA stands for Defense Advanced Research Projects Agency. They are the first agency to develop the world first quantum cryptography network and providing their services in metropolitan cities. The model developed by DARPA is based on cryptographic virtual private network. The virtual private network implements public key as well as symmetric cryptography to provide the confidentiality and integrity. The public key helps to provide the exchange mechanism of data and to provide the authentication between the endpoints where symmetric cryptography provides the confidentiality and integrity. There is loophole in this type of VPN network as it can provide the integrity and confidentiality without trusting the public network interconnecting the VPN sites. Thus, this loophole can overcome by replacing the public key by the key provided by the quantum cryptography. Therefore, this technology is 100 percent compatible with models that are used now a days.

6.2. MagiQ Technologies

There is another technology that is developed by companies is called MagiQ Technology, which is a start up with its headquarters in New York city. This technology is developed for customers including financial ser-vices with academic and government areas. This technology does not provide the replacement for the existing model, but it provides the additional feature along with the current cryptography techniques algorithm providing the hybrid model to provide the more efficient and secure system.

7. Quantum Key Distribution Protocols Implementation

Quantum cryptography has specialized protocols which are called as “quantum key distribution protocols”. Almost every protocol is abnormal in implementation but interest’s specialist working in the fields of communication protocols. Here I am going to discuss the various protocols that the used in the quantum key distribution protocols implementation. All these protocols are written in c language. Specialist are devoting their time for developing the new quantum key distribution protocols and trying them in practice.

7.1. Shifting

Shifting may be defined as the process where Mark and Bob remove all failed bits from the series of pho-tons beam. These failed bits comprise of all that Mark laser gun did not transmitted, that bob detectors did not received and the number of photons that were lost. It also includes the bits that Mark chooses for transmission, but bob chose the other for receiving. All these bits are discarded by both from their storage and kept only those which matched on both chosen requirements.

7.2. Error Correction

Error correction is the process that helps the Mark and bob to keep the correct chosen sequence of bits and to determine all the failed or error bits. error bits are defined as the bit that is transmitted as 0 by the Mark but interpreted by bob as 1 or vice versa. The error are consequences of eavesdropper trafficking the line or noise caused from another source. Error correction is designed by keeping in mind that even if any third party gets the information of this missing bits then also, he will not be able to track the real message. It thus re-duces the hidden entropy present for key material.

7.3. Authentication

Authentication act as a bodyguard to guard the Mark and bob against any attackers. It makes sure that Mark is communicating with bob only and vice versa. Authentication should perform on daily basis to manage the traffic and keep an eye over the network to check whether any attacker is trying to eavesdrop the communication. In quantum key distribution it is insufficient to authenticate only QKD protocols, it should also apply these techniques to authenticate the VPN data traffic.

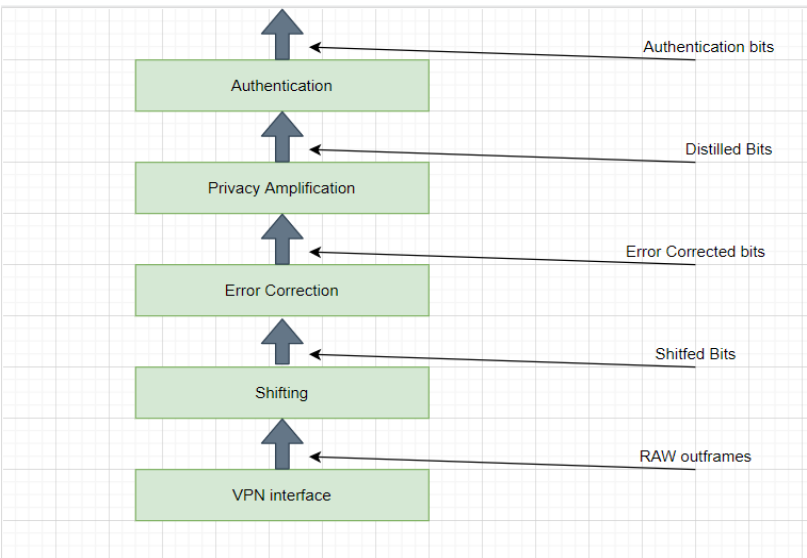

Figure 6. Authentication Implementation

8. Difference Between Cryptography and Quantum Cryptography

Classical Cryptography	Quantum Cryptography
It is based on mathematical computation.	It is based on quantum mechanics.
It is widely used.	It is sophisticated.
Digital signature is present.	Digital signature is absent.
Bit rate depends on computational power.	Average bit rate is 1 MBPS.
Communication range is millions of miles.	Communication range is maximum 10 miles.

9. Analysis of Quantum Cryptography Implementation

Security for internet communication network in the future should be guaranteed as everything done is online and all the information are stored there. There should be a way to provide guaranteed security as failing in so will cost the human survival. So, to overcome it the quantum cryptography model was taken into consideration.

9.1. Unconditional Security

In today's world cables are used transmission for data. But there is always a threat of an attacker in these medium. To achieve high level of security, the encrypted message should be trans-mitted in public channel. The classical cryptography that are using is basically divided into category one is public key cryptography and other is symmetric key cryptography. The security of these two models is basically depends on the complexity of computing power of machines. But there is rapid development of hardware and software equipment and there are many advanced algorithms that have challenged the security of the following two models. It also possesses the thread of quantum computing which has made possible things that were impossible then.

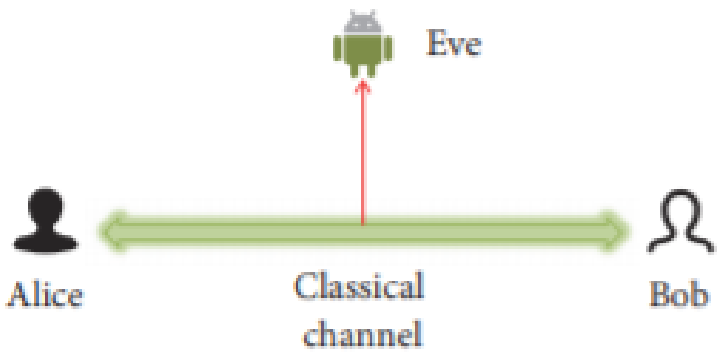

Figure 7. Classical Communication Model

9.2. Sniffing Detection

Whenever Alice and Bob Wants to exchange information between them, they should do through public channel. But the confidentiality of data must be encrypted but they cannot prevent an attacker from eavesdropping. The characteristics of channel are such that eavesdropper cannot be detected weather he is in the cable channel or optical fiber medium. In cable transmission the attacker uses the multimeter or the oscilloscope to eavesdrop and in optical medium it gains information from light signal. In optical loss of data is caused by environmental factor which makes it more difficult to detect whether who has caused the error.

But quantum cryptography changes the whole concept as attacker is sure to be detected due to quantum no cloning theory. If an eavesdropper monitors the quantum channel, for a bit of quantum information, he will choose the same measuring base with the sender with a 50% probability. Therefore, the eavesdropper will be detected at a 50% probability for a bit of quantum information.

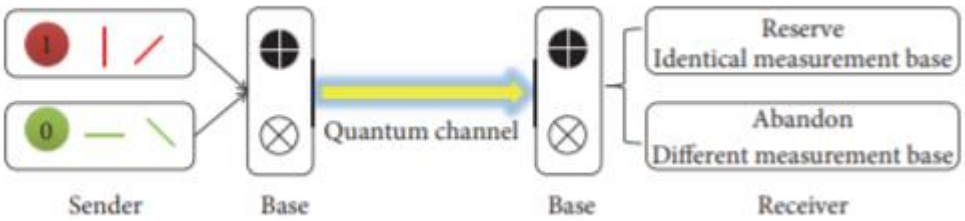

Figure 8. Model of QKD protocol

9.3. Security of the QKD

To analysis security of QKD protocol, list the encoding of quantum information and the measurement results under different measurement. The two parties agree in advance that the horizontal and oblique downwards polarization represents "1" while the vertical and oblique upward polarization represents "0." The probability that the eavesdropper is found for 1-bit quantum information is calculated as 1/2 × 1/2 × 1/2 = 1/8.

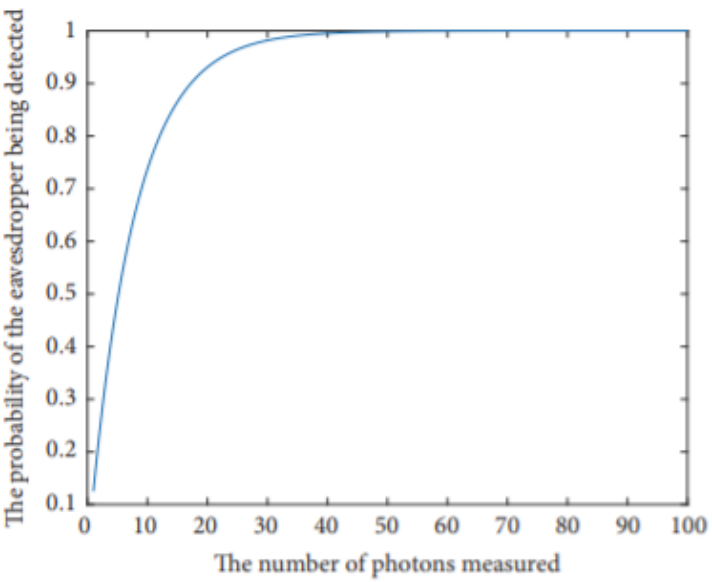

Figure 9. QKD noise free channel

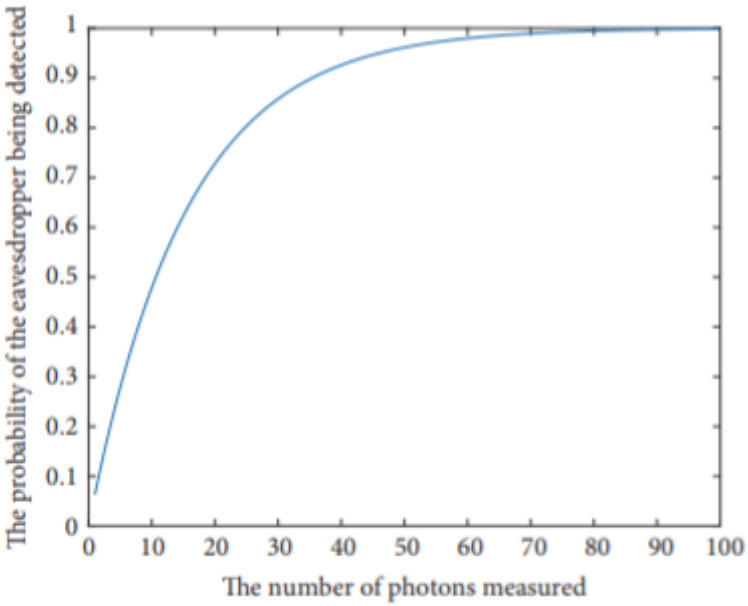

Figure 10. QKD protocol in 30% noise

Conclusion

The quantum cryptography works on the point-to-point quantum key distribution link but now the DARPA has to start focusing on building the multiple QKD links in the form of mesh so that if any of the link fails due to problem in fiber or noise then it could use another path. This design is called key transport network. The main problem that quantum cryptography faces is that weakness of untrusted QKD networks and limited geographical reach.

The solution to this problem is to form a chain quantum cryptography links and secure the intermediary stations. Another possible solution is the transmission through low orbit satellite. The satellite act as interne-diary stations and there is less loss of photons in atmosphere. Researchers are giving their best to find and efficient transmission solution. There is very little development in the fields of quantum cryptography in the previous decade, there are bright future of quantum cryptography and will led to the development of more secure way transmitting the data which will redefine the meaning of cryptography.

Quantum cryptography is still infancy and looks very promising so far. It could bring revolution by contribute to e commerce and business security, personal security, and security among government organization. If implemented successfully in future, then it will have profound and revolutionary impact on our lives.

Acknowledgements

I would like to thank my university for giving me this golden opportunity to research on such an interesting topic. I would also like to thank Dr. Anil Kumar, Assistant Pro Vice Chancellor & Director, ASET and Dr. Deepak Arora, Professor & Head, Dept of CSE & IT, ASET for encouraging students to indulge in valuable research activities to enhance their technical skills. Next, I want to thank my faculty guide Dr. Pawan Singh for guiding me throughout the course of this project. I would also like to thank the internet, books, and the institute for the knowledge I acquired with their help.

References

[1] C. H. Bennett and G. Brassard, “Quantum public key distribution reinvented,” ACM SIGACT News, vol. 18, no. 4, pp. 51–53, 1987.

[2] C. H. Bennett, G. Brassard, and A. K. Ekert, “Quantum Cryptography,” Sci. Am., vol. 267, no. 4, pp. 50–57, 1992.

[3] C. H. Bennett and D. P. DiVincenzo, “Quantum information and computation,” Nature, vol. 404, no. 6775, pp. 247–255, 2000.

[4] C. H. Bennett and P. W. Shor, “Quantum information theory,” IEEE Trans. Inf. Theory, vol. 44, no. 6, pp. 2724–2742, 1998.

[5] G. Brassard and C. Crépeau, “25 years of quantum cryptography,” ACM SIGACT News, vol. 27, no. 3, pp. 13–24, 1996.

[6] D. Gottesman and H.-K. Lo, “From quantum cheating to quantum security,” Phys. Today, vol. 53, no. 11, pp. 22–27, 2000.

[7] H.-K. Lo, “QUANTUM CRYPTOLOGY,” in Introduction to Quantum Computation and Information, WORLD SCIENTIFIC, 1998, pp. 76–119.

[8] M. Khan and T. Shah, “A construction of novel chaos base nonlinear component of block cipher,” Nonlinear Dyn., vol. 76, no. 1, pp. 377–382, 2014.

[9] W. Stallings, “Secure hash algorithm,” *Cryptography and Network Security: Principles and Practice*, 1999, pp. 193–197.

[10] Wiesner, S. (1983). Conjugate coding. *ACM Sigact News*, *15*(1), 78-88.

[11] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, “Experimental quantum cryptography,” J. Cryptology, vol. 5, no. 1, pp. 3–28, 1992.

[12] “Quantum Key Distribution as a Next-generation cryptographic protocol. Andrew Campbell,” Docplayer.net. [Online]. Available: https://docplayer.net/12798486-Quantum-key-distribution-as-a-next-generation-cryptographic-protocol-andrew-campbell.html. [Accessed: 11-Jan-2021].

[13] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned,” Nature, vol. 299, no. 5886, pp. 802–803, 1982.

[14] D. G. Enzer, P. G. Hadley, R. J. Hughes, C. G. Peterson, and P. G. Kwiat, “Entangled-photon six-state quantum cryptography,” New J. Phys., vol. 4, no. 345, pp. 45–45, 2002.

[15] N. Gisin, “Quantum cryptography,” Rev. Mod. Phys, vol. 74, no. 1, 2002.

[16] G. Brassard and L. Salvail, “Secret key reconciliation by public discussion,” Lect. Notes in Computer Science, vol. 765, p. 410, 1994.

[17] M. N. Wegman and J. L. Carter, “New hash functions and their use in authentication and set equality,” J. Comput. Syst. Sci., vol. 22, no. 3, pp. 265–279, 1981.

[18] B. Slutsky, R. Rao, P. C. Sun, L. Tancevski, and S. Fainman, “Defense frontier analysis of quantum cryptographic systems,” Appl. Opt., vol. 37, no. 14, pp. 2869–2878, 1998.