International Journal of Recent Research and Review, Vol. XIII, Issue 3, September 2020
ISSN 2277 – 8322

A Review on Quantum Cryptography

Laxman Poudel
Department of Computer Science, Kalika Manavgyan Secondary School, Butwal, Nepal
E-mail: coderlaxman@gmail.com

***Abstract* - Cryptography is associated with the process of transmission of a secret code over a network. It is a procedure of storing & transmitting data in a particular form so that intended user can read & process it.Most of the cryptographic method uses public key for the transmission of data which may be detected by eavesdroppers & access the information without the knowledge of sender & receiver. Quantum cryptography is a special technique that applies principles of quantum mechanics to encrypt messages in such a way that is never read by anyone outside of the intended recipient. Quantum Cryptography use QKD (Quantum Key Distribution) techniques for exchanging encryption keys only known between shared parties. This paper analyses weakness of the modern cryptosystem, the fundamental concept of quantum cryptography, application of quantum cryptography along its limitation.**

***Keywords*- Modern Cryptography, Photon polarization, Quantum Cryptography, Quantum entanglement, Quantum KeyDistribution, Cryptosystems**

I. INTRODUCTION

Cryptography is the study and practice of techniques for secure communication in the presence of third parties called adversaries. It deals with developing and analyzing protocols that prevent malicious third parties from retrieving information being shared between two entities thereby following the various aspects of information security [1]. Basically, cryptography consists of two main branches as: - Symmetric Key Cryptography & Asymmetric Key Cryptography. A Key is a piece of information that determines the functional output of a cryptographic algorithm. For encryption algorithms, a key specifies the transformation of plaintext into cipher text and vice versa for decryption algorithms. Keys also specify transformations in other cryptographic algorithms, such as digital signature schemes and message authentication codes. Modern cryptography algorithms are based on the fundamental process of factoring large integers into their primes and are vulnerable. Cryptographers add their persistent exertion to make framework vulnerable free yet the programmers, code breakers, busybodies work furiously to split the frameworks. So to actualize advance security during the transmission of information and data cryptographer bring quantum physics into cryptography, which lead to the assessment of quantum cryptography.

Quantum cryptography, by extension, simply uses the principles of quantum mechanics to encrypt data and transmit it in a way that cannot be hacked. Quantum cryptography, or quantum key distribution (QKD), uses a series of photons to transmit data from one location to another over a fiber optic cable. By comparing measurements of the properties of a fraction of these photons, the two endpoints can determine what the key is and if it is safe to use [2]. Each photon represents a single bit of data. The value of the bit, a 1 or a 0, is determined by states of the photon such as polarization or spin. Using, this method one party can send key encoded with photons to the other party. If the photon is read or copied in any way by an eavesdropper, the photon's state will change. The change will be detected by the endpoints. In other words, this means you cannot read the photon and forward it on or make a copy of it without being detected.

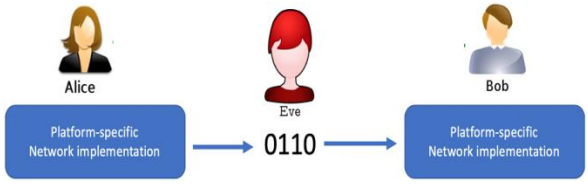

Fig. 1. Communication in presence of Eavesdropper

II.LIMITATIONS OF MODERN CRYPTOGRAPHY

An individual owns multiple electronic devices such as laptops, smartphones, tablets, etc. to use them in their workplace or remote location. The protection of individual information is pivotal as it can travel across the globe within a second. Cryptography provides protection and plays an integral part in against fraud in electronic transactions and anything that involves important financial information. Strength of modern cryptography algorithms are based over the fundamental process of factoring large integers into their primes which are so-called intractable. Modern cryptography uses a public key for the transmission of data which involves complex calculations that are relatively slow, they are employed to exchange keys rather than for the encryption of voluminous amounts of data. The security of the cryptographic technique is based on the computational difficulty of mathematical problems. Any breakthrough in solving such mathematical problems or increasing the computing power can render a cryptographic technique vulnerable.

RSA &Diffie Hellman algorithms used in modern cryptography is used to distribute symmetric keys resulting in slow performance & require more computer power supply compared to single-key encryption. Likewise, the DES algorithm (Asymmetric cryptography) has a 56-bit key which was considered to be secure before, it is no longer thought of as such since advancements in technology have made it trivial to defeat [3]. The fact that powerful computers may crack DES in a few hours served as a catalyst for the development of the replacement Advanced Encryption Standard. Hence public key cryptography may be vulnerable to future technology developments in computer processing.

III.QUANTUM CRYPTOGRAPHY

Quantum cryptography uses our current knowledge of physics to develop a cryptosystem that is not able to be defeated - that is, one that is completely secure against being compromised without the knowledge of the sender or the receiver of the messages.The word quantum itself refers to the most fundamental behavior of the smallest particles of matter and energy: quantum theory explains everything that exists and nothing can be in violation. It is different from traditional cryptographic systems in that it relies more on physics, rather than mathematics, as a key aspect of its security model [4].

A bit is a base of classical information either read as 0 or 1.A quantum bit or qubit is a unit of quantum data. Conversion and Polarization are the two different process carried out in quantum cryptography in which data is converted to bits of 0s and 1s and is transferred using polarized photons. Quantum cryptography accomplishes these remarkable feats by exploiting the properties of microscopic objects such as photons. The photons have three chosen bases of polarization and the probable results of measurement according to the bases are:

- Rectilinear (horizontal or vertical)
- Circular (left-circular or right-circular)
- Diagonal (45° or 135°).

In spite of the fact that there are three bases, however, two of them are generally utilized. Photons are utilized to decide their direction comparative with each of these bases of polarization in turn. Traditionally, one would anticipate that the photon should have a specific polarization, which can be measured but isn't changed by the measurement. Photons, in any case, are quantum objects, which are considered to have a property simply after it is measured. The sort of measurement impacts the property of the object. This suggests a photon must be considered to have a specific polarization after it is measured, and that the premise picked for the estimation will affect the polarization.

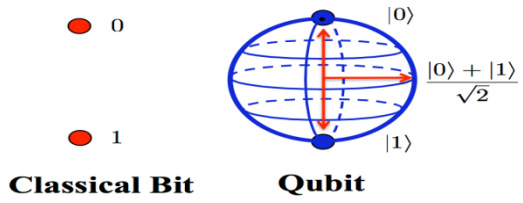

Fig 2. Classical bit vs Quantum bit

IV. QUANTUM KEY DISTRIBUTION (QKD)

Charles Bennet and Gilles Brassard forwarded the concept of first quantum key distribution protocol in 1984 and now is known as "BB84"[5]. Further development in hypothetical quantum cryptography occurred in 1991 when ArturEkert proposed that Einstein-Podolsky-Rosen (EPR) [6] "entangled" two-molecule states could be utilized to actualize a quantum cryptography convention whose security depended on Bell's inequalities. In 1989 Bennet and Brassard along with his collaborator performed the first experiment on QKD by working on a prototype system for BB84 protocol. The propagation distance is about 30cm showing a practical demonstration of quantum cryptography [7].

Hackers steal data constantly, so protecting it is an ongoing challenge. Today's information encryption technology has been compromised and will be obsolete in just a few years. Quantum Key Distribution (QKD) technology can be proven by the laws of physics to help secure the sensitive data we deliver—today and into the future. Quantum key distribution (QKD) is a secure communication method that implements a cryptographic protocol involving components of quantum mechanics. It enables two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages [8]. QKD is the one technology that can actually address this issue of long-term security.

Here is a simple demonstration of how quantum cryptography can be used to securely distribute keys. Here “Alice”, a sender, “Bob” as a receiver and “Eve” represented as an eavesdropper. Typically, information is encoded on a single photon. Alice begins to send message to Bob in four different polarization states like vertical, horizontal, or diagonal in opposing direction(0°,45°,90°,135°). Bob then measure the polarization state which is either rectilinear (0° or 90°) or diagonal (45° or 135°). If he measures a base that is different from that of Alice used to prepare, then his answer will be random & discarded but if they choose the same one, they will have perfectly correlated result .The photon that is incorrectly measured will be discarded and correctly measured photons are translated into bits based on their polarization. Now, these photos are used to form the basis of a one-time pad for sending encrypted information. The practice of this cryptography is too secured as Bob and Alice are also unable to determine the key because the key will be the product of both random choices.

Let us consider eavesdroppers are on the network to crack the system where attacker named Eve tries to eavesdrop and randomly select either a rectilinear or diagonal filter to measure each of Alice’s photons. During the process of cracking the framework, Eves will have an equal probability of selecting the correct and wrong filters and won’t be able to determine the filter used by Alice during the transmission. Indeed, even Eve is able to gather the correct information while Bob confirms with Alice the photons he received; information will be of little use to Eve unless she unknowns the correct polarization state of each and every photon. Eve is not capable to form the final key if she is unable to identify the polarization state of the photon.

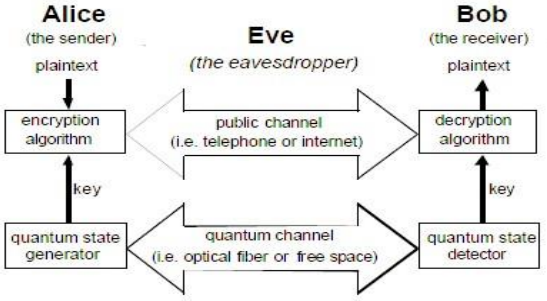

Fig 3. Quantum Key Distribution Model

Based on Heisenberg Uncertainty principle information regarding photons cannot be duplicated because photons will be destroyed once they are measured or interfere. Since photons are indivisibleonce it hits an eavesdropper, the photon no longer exists. Likewise, in order to form the encryption key Bob & Alice must calculate the amount of photon. Mathematically Bob should receive about 25 percent of transmitted photons but if there is a deviation in the number of the transmitted photon he can be certain that something is wrong in the system. In order to grasp the information Eve needs to determine the state of the photon. If Eve attempts to create and pass on to Bob a photon, she will have to

randomly choose its orientation, and on average be incorrect about 50 percent of the time –enough of an error rate to reveal her presence [9].

V.ONE TIME PAD METHOD

Information can be exchanged over the channel in various ways.One time pad method is one of the various method used for exchanging the information.Here is a simple demonstration of how this method works.

- Alice generates two random bits,B1 and B2 where B1 is used to select the basis,and B2 is used to select the polarization of the photon. Likewise, Bob generates a random bit B3 and sets his detector to that basis. Using the basis Bob reads Alice's signal and records B4.

- Alice and Bob compares the basis B1 and B3 used over the public channel.These bases will be the same half of the time, since Alice'sbase can be one of two things, and so can be of Bob's. The fours possibilities are (B1, B3) = (0, 0), (0, 1), (1, 0), (1, 1). Here two bases may match half of the time.

- Until the bits , B1 and B3 get matched bits need to be sent. Each time the bases should be chosen randomly to ensure security.

- When B1 and B3 match, Alice and Bob record B2 and B4, realizing that they are the equivalent except if Eve is tuning in, in which case she would be changing the state of the photons.Comparing string using the binary search allow Alice and Bob to detect any such interventions.

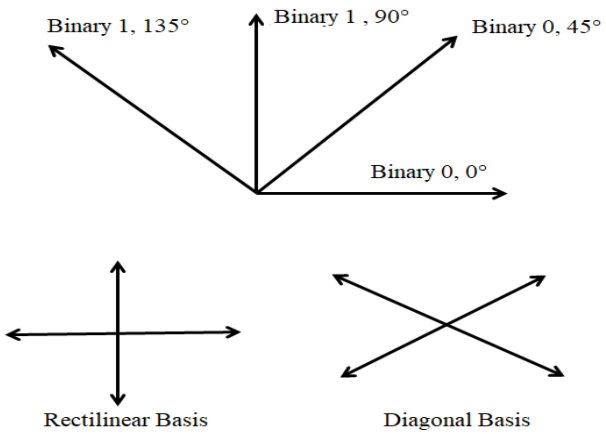

Fig.4. Photon Polarization

VI. QUANTUM ENTANGLEMENT

Based on quantum entanglement theory of Albert Einstein quantum particles (atoms, photons or ions) become correlated with each other, meaning that if one particle changes its state, the entangled particle will undergo the same change. Therefore, by measuring one particle, one can also determine the state of the other. If an eavesdropper tries to measure the state of a photon, the laws of quantum mechanics cause the entangled particles to lose their magic connection. This property makes the communication secure since any attempt to eavesdrop would change the state of the particle and thus be exposed. Thus, disturbing the state of one will instantly disturb the other, no matter how far apart they are which is extremely useful in detecting eavesdroppers.

Alice's random byte	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		1			0		1

Fig.5. QKD Example

VII.ERROR CORRECTION

Error bits are ones that Alice transmitted as a 0 but Bob received as a 1, or vice versa. These bit errors can be caused by an eavesdropper. Error correction helps Alice and Bob determine all the “error bits” among their shared bits and correct them so that they share the same sequence of corrected bits. It is very important to design error detection and correction codes that reveal as little as possible in their public control traffic between Alice and Bob.

VIII. EAVESDROPPER DETECTION

Measuring the polarization of the photons helps to determine the presence of the eavesdropper in the network. But without destroying photon it is impossible to measure the polarization. So if Eve catches the signals, she should send new photons to the collector with the goal that she may not be identified about her activity. However, she will definitely present blunders, since she doesn't have the idea about the state and polarization. During this procedure, Bob and Alice strictly check errors by revealing a random subset of their generated sequence and compare them publicly. If they find a dispute and are not satisfied with it they will setup different channels for the transmission. This guarantees Eve cannot listen the conversation between Bob and Alice.

According to the theory forwarded by Einstein, change in the polarization of one photon in a pair will affect the other one, no matter how far apart they are. In order to break the code, Eves have to detect one of the photons and measure it, thus destroying half of the pair. So to achieve actual content Eves applies an intercept and resend technique on both the conventional and the quantum channel by listening to the signals send by Alice. Now Eves try to perform a copy or read operations before she resends the signal to Bob. However, all these actions by Eve result in permanent quantum effects on the transmitted signals. This will end the quantum relationship of the two members of the pair, which is very easy to detect by Alice and Bob, and impossible to reverse for Eve.

IX.APPLICATIONS

Quantum cryptography is ultra secure as it relies on algorithms that can't be cracked in less than the lifetime of the universe by all the currently existing computers.Some applications are listed below.

1. Secure Communication With Satellite

In August 2016 China launched itsfirst quantum satellite named “Micius”whose goal was to facilitate quantum optics experiments over long distances to allow the development of quantum encryption and quantum teleportation technology. Secure communication between satellites and astronauts is very important. So utilizing the concept of quantum mechanics, one can guarantee the security of communications regardless of the technology or intelligence to which an adversary has access. Implementing the QKD technique in space satellites will ultimately increase the safety of the astronauts. This improved mechanism could revolutionize how we share sensitive data, protecting people’s information during a time of increasing cybersecurity threats.

2.Ultra-Secure Voting

It is important to protect the integrity of our elections.Millions of people vote illegally to various political parties during the time of the election. So to revolutionize and make fraud-free election quantum cryptography techniques should be implemented. Since 2007, Switzerland has been using quantum cryptography to protect voting ballots cast during parliamentary elections. Quantum cryptography is unconditional secure communication by using the phenomena of Heisenberg’s uncertainty principle, the non-cloning theorem of a photon of quantum mechanics. Thus utilizing the concept of quantum cryptography in voting would add extra security resulting in the fraud-free election as vote moved from counting station to central repository will be uninterruptible.

3. Finance & Banking

These days banks and financial institutions use either symmetric cryptography or asymmetric cryptography which are vulnerable and transactions could be corrupted and altered without the awareness of the bank. This may result in serious issues and profit of the breach to steal and highjack. Securing financial transactions is mandatory to prevent ourselves from economical crime. So utilization of quantum technology in banking would add an extra layer of security as it is unbreakable by hackers & geeks.

X. LIMITATAION OF QUANTUM CRYPTOGRAPHY

Despite the various advantages of quantum cryptography, it has some limitations too.The major downside of quantum cryptography is the fact that it is impossible to send information beyond 50km as the noise becomes so great and error rates also increase drastically resulting in channel vulnerable. Likewise while traveling through the channel (i.e. optical fiber or air), there is a possibility of change in polarization of photon due to various factors like temperature, pressure, etc. There is a need for a dedicated channel between source and destinations which implies a high cost. It is impossible to send keys to two or more different locations using a quantum channel as multiplexing is against quantum's principles. This demands separate channels between source and many destinations. This is a major disadvantage of quantum communication through optical channels. Real-world implementation of Quantum Cryptography could take up lots of jobs and hence unemployment will increase. Furthermore, quantum cryptography lacks many vital features such as digital signature, certified mail, etc. The biggest problem of quantum cryptography is that technology is not figured out yet and will be prohibitively expensive.

XI. CONCLUSION

The protection of individual information is pivotal so to transmit information stronger framework is required. Utilizing the concept of quantum cryptography and quantum key distribution technique one can securely transmit information. Quantum cryptography can be a favored choice for applications that require long-term information security and can be the future of the internet and security. Unlike other existing security solutions, it is secure from all future advances in mathematics and computing. Quantum cryptography promises to revolutionize secure communication by providing security based on laws of physic, instead of the current state of mathematical computing. So considering the security of an individual and company information quantum cryptography has enormous scope in thefuture.

XII. REFRENCES

[1] https://www.geeksforgeeks.org/cryptography-introduction

[2] https://quantumxc.com/quantum-cryptography-explained/

[3] Quantum CryptographyJ. Aditya, P. Shankar Rao {Dept of CSE, Andhra University} [https://cs.stanford.edu/people/adityaj/QuantumCryptography.pdf]

[4]https://searchsecurity.techtarget.com/definition/quantum-cryptography

[5] https://en.wikipedia.org/wiki/BB84

[6] https://en.wikipedia.org/wiki/EPR_paradox

[7] Richard J. Hughes*, William T. Buttler, Paul G. Kwiat, Steve K. Lamoreaux,,George L. Mokgari; Jane E. Nordholt, and Charles G. Peterson,"Quantum Cryptography For Secure Satellite Communications"

[8] https://en.wikipedia.org/wiki/Quantum_key_distribution

[9]https://www.sans.org/readingroom/whitepapers/vpns/securing-key-distribution-quantum-cryptography-1448