Quantum Cryptography: Future of Today

Vashnavi Tariyal, Gunjan Sharma** and Shikha Bhalla****

ABSTRACT

In today's world where everyone relies mostly on the internet for information exchange, security has become a major area of concern. Traditional cryptography makes use of powerful encryption methods to obscure the message from the intruders. Most of the encryption techniques that we use today are based on large numbers that are difficult to factor. A typical computer may take millions of years to intercept the code, but with the advent of Quantum Computers, there is a possibility, that time taken to break the code may be reduced by a significant amount and current encryption techniques may become fragile. Therefore need has arisen to address the security aspect with respect to these powerful Quantum Computers. Quantum computer as for now is a theoretical concept, but the researchers are striving hard to come up with a working model of these powerful computers that is proposed to be much faster than the binary computers and it is possible that quantum computers may replace binary computers in the near future. Quantum Cryptography is one of the promising cryptographic techniques in this context that will primarily address the security aspect of Quantum Computers. The main objective of this paper is to find and analyze the difficulties faced during QKD due to various factors and why still Quantum cryptography is not fully adopted, also the traditional cryptography is also compared with the powerful Quantum Cryptography along with a brief overview of Quantum Cryptography, QKD and its working.

Keywords: *Quantum, QKD, Photons; Qubits; Cryptography; Eavesdropper; Polarizers.*

1.0 Introduction

The term cryptography word "crypt" means "hidden" and "graphy" stands for "writing". Cryptography is the process of converting plain text into unintelligible text and vice-versa so that it could be transmitted securely to its intended recipient. It is part of the broader field of cryptology, which also includes cryptanalysis, known as the art of code breaking. [1] The information that we need to encode is called plaintext or the original text. It could be in any form of like characters, numbers, pictures or images, or any other kind of information. The plaintext that will be encrypted is called cipher text, it refers to the series or string of "meaningless'' data or "unclear text'' that nobody must understand, except the receiver (after decoding back).It is the data that will be transmitted through the network or a communication channel. Many different algorithms are now used to transform plaintext into cipher text. [1][2]Cryptography techniques can be divided according to their standard principles or protocols they follow. But here, we are only concentrating on the two types of cryptography technique- Classical Cryptography and Quantum Cryptography.

A. Classical Cryptography

Classical cryptography is based purely on mathematics.

**Corresponding author; Student, Department of CS&IT, Trinity Institute of Professioanl Studies, New Delhi, Delhi, India. (Email: vashnavi9128@gmail.com)*

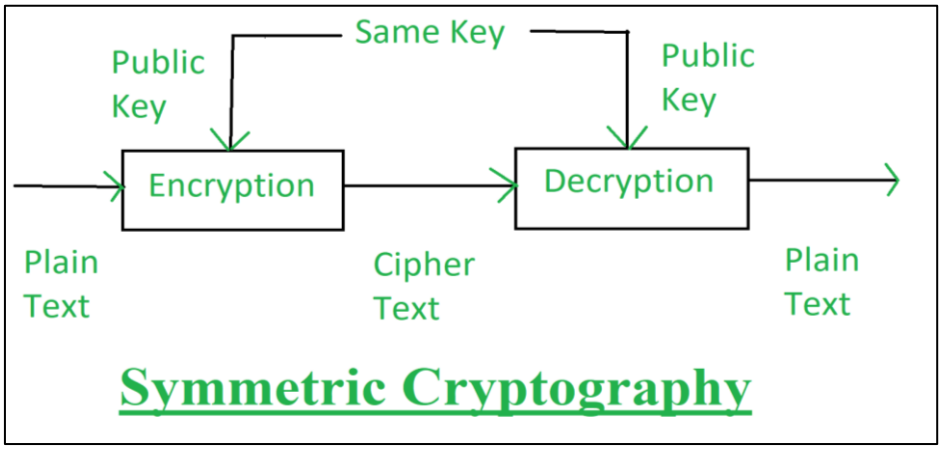
***Student, Department of CS&IT, Trinity Institute of Professioanl Studies, New Delhi, Delhi, India. (Email: gunjan.sharma1601@gmail.com)*

****Assistant professor, Department of CS&IT, Trinity Institute of Professioanl Studies, New Delhi, Delhi, India. (Email: Shikhabhardwaj87@gmail.com)*

The high security of classical cryptography is based on the mathematical problem for the instance factorization of large numbers. A string of data which is known as key is used to control the change of the data from plain text to cipher text. This technique helps to keep data safe as it requires the key for decrypting the original information from the cipher text. Classical Cryptography has two types of techniques: - [2]

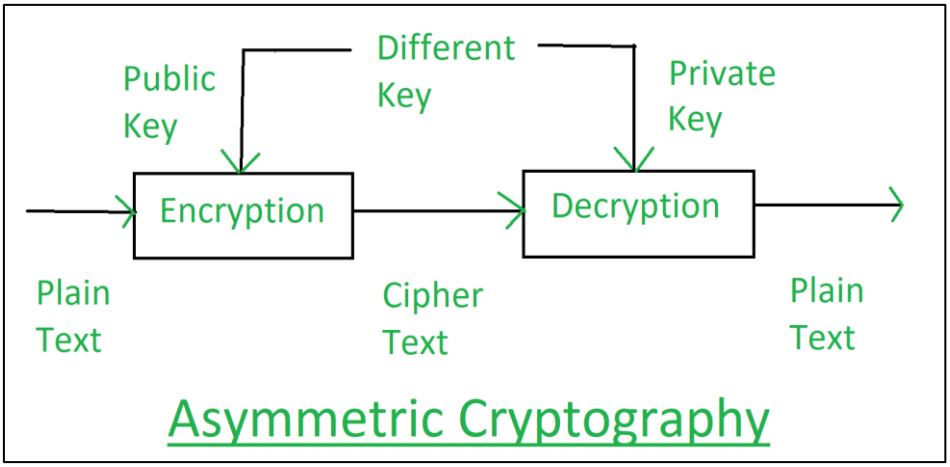
1) **Symmetric Cryptography:** Symmetric key cryptography is also known as private-key cryptography or single key cryptography. In this a single key is used for both encryption and decryption. Key must be kept secret between the sender and the receiver. Both the sender and receiver must have a copy of the secret key and they both share same copy of key.[3]

Fig 1: diagram showing the private key cryptographic technique[3]



2) **Asymmetric Key Cryptography:** This two-key system is also known as the public key system. It uses two separate keys that is receiver's public key for encryption and receiver's private key for decryption instead of single shared key. Using this public-key cryptographic method, the sender and receiver are able to authenticate one another as well as protect the secrecy of the message.[1][3]

Fig 2: block diagram depicting the public key cryptographic technique[3]



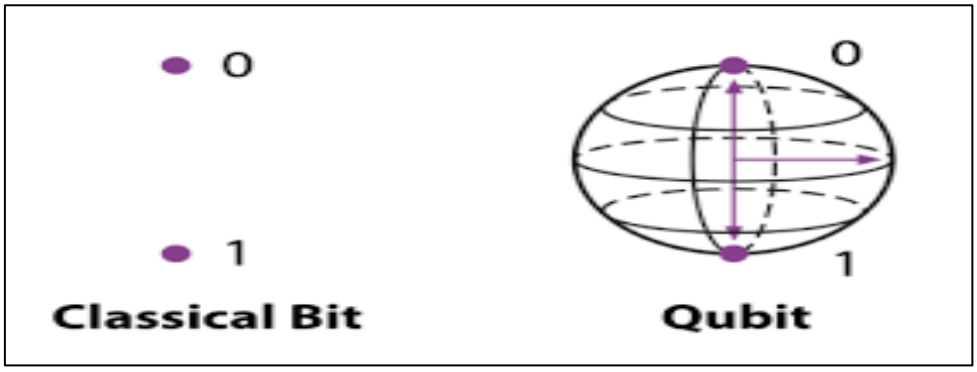
B. Quantum Cryptography

As computers have grown more powerful and with the emergence of quantum computers, factorization of large numbers have become easy – no secret would be safe, hence there is an alternative and more safer option to traditional cryptography- that is Quantum Cryptography, one that's just not hard to break but impossible to break .The word quantum refers to the most fundamental behavior of the smallest particles of energy and cryptography means secret writing what makes it so powerful is that instead of math it relies on the laws of physics. Quantum Cryptography is also called as Quantum encryption as it applies the principles of quantum mechanics.[4] A technology that hides information in photons or the particles of light. The most important thing is that quantum cryptography is the only known secure method for transmitting a key at least in theory. The Quantum cryptography uses the two important principles of quantum mechanics - first is of the principle of photon polarization and the other is the Heisenberg Uncertainty principle. The idea of Quantum cryptography was proposed first by Stephen Wiesner, who in the early 1970s introduced the concept of Quantum conjugate coding[5]. For Quantum cryptography these three basic things are needed with some other components of telecommunication - a quantum channel, a photon source, a photon detector. If anyone is eavesdropping then, according to the principles of quantum physics, the polarization of the photons is affected, and the recipient can tell that the message isn't safe anymore. [11]

C. Bits and Qubit

So before proceeding further the difference between bit and qubit should be well known. Well, in case of classical cryptography, all information is in the form of 0's and 1's (bits) for both sending and receiving, while qubits or quantum bits have a different behavior while sending and receiving and are used in quantum computers. In classical cryptography, the value of the key is always the same, it does not matter how you read it, but this is different in the case of quantum cryptography. In quantum cryptography the value of the bit depends on how one measures it (measure the value of qubit). Qubit is the basic unit of quantum information. Qubits can have up to 2 bits (due to entanglement). In order to get the right value, you also need to measure the qubit in the right way.[6] The qubits are connected through entanglement. Entanglement refers to a connection that makes each of the qubits react to a change in the state of other qubits instantaneously; no matter how near or far they are from each other. If the qubit is measured incorrectly then a random bit value is received (or incorrect data). [10] In order to transmit the qubits, polarizers are used.

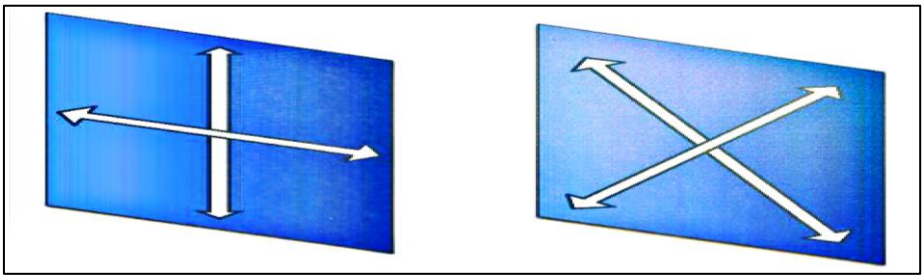
Fig 3: figure depicting classical bit and qubit[12]



D. Photons

Photons are the smallest measure of light, and they can exist in all of their possible states at once- diagonally, vertically and horizontally. One photon represents a qubit. They are also referred to as some zero-mass particles and are never in a stationary position. These light quanta can be used to carry information. [6]

Fig 4: diagram depicting two basis- rectilinear basis and diagonal basis



1) Photons and Polarizers

- A single photon is discharged from a light source and moves through a linear polarizer. If a horizontal polarizer is used, a horizontal polarized photon is transmitted. In this situation (horizontal). This process creates a qubit with horizontal polarization.
- When the horizontally polarized photon moves through a horizontally/vertically-intended polarizing beam disjoin, it always remains its horizontal polarization.
- If that horizontally polarized photon moves through a diagonally-oriented polarizing beam disconnect.[11]

Fig 5: diagrams representing the above three mentioned statements respectively[12]

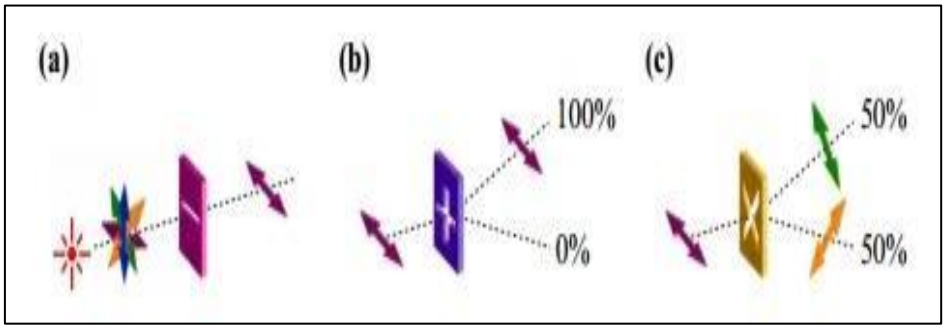
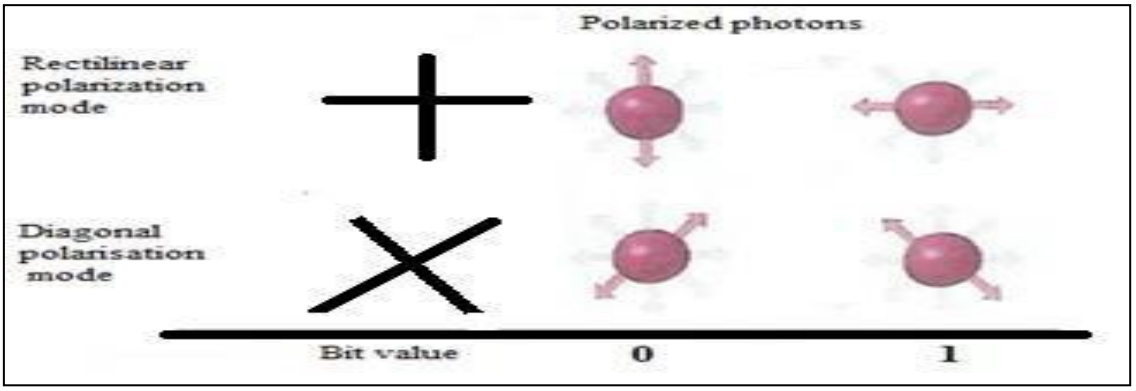


Fig 5: Polarized photons and corresponding bit values[12]



2) How does a photon become a key: Each type of a photon move represents a single piece of information usually 1 or 0, for binary code. This code uses strings of ones and zeros to create a coherent message. For example, 11100100110 could correspond with "h-e-l-l-o". A low level language (binary code) can be allocate to each photon, like a photon that has a vertical spin (|) can assigned a 0. It uses the properties of quantum physics to scramble information at the physical network layer. Post-quantum and quantum-resistant cryptography efforts, however, remain focused on developing encryption methods that are based on hard math problems the kind that quantum computing is not easy to solve.

2.0 Principles of Quantum Mechanics used in Quantum Cryptography

It is easy to understand Quantum cryptography but the complexity behind it totally lies in the principles of quantum mechanics, all these principles plays an important role in Quantum Cryptography.

- The particles that make up the universe are uncertain and can simultaneously exist in more than one place or more than one state of being.
- The Photons are generated randomly in one of the two quantum states.
- One can't measure the quantum property without changing or disturbing it.
- Some of the quantum properties of a particle can be cloned, but not the whole particle.[7]

3.0 A Brief about Qkd

The most well known application of Quantum cryptography is Quantum key Distribution (QDK). QKD ensures a secure communication based on the law of physics rather than math, but QKD should not be confused with Quantum cryptography. It is used to generate and distribute the key, not for transmission of information. With quantum cryptography a key is a stream of photons or light particles. They have a property known as spin which can be changed when it passes through a filter. The key produced can be used with any selected standard encryption algorithm to encrypt the information that can be transmitted over a communication medium. It actually enables two parties (sender and the recipient) to produce a shared random key which is a secret key which is only known only to them, that can then be used to both encrypt the message and decrypt message. Unlike mathematical encryption that is generally used in classical cryptography, quantum cryptography uses the principles of quantum mechanics (physics) to encrypt data and make it near to unhackable. Mainly, quantum cryptography based on the photons and quantum properties to develop systems that are not easy to decrypt. Quantum cryptography uses photons to transfer key from sender to receiver. Once the key is transmitted, coding and encoding using the secret-key method can take place. [1][4] [5]

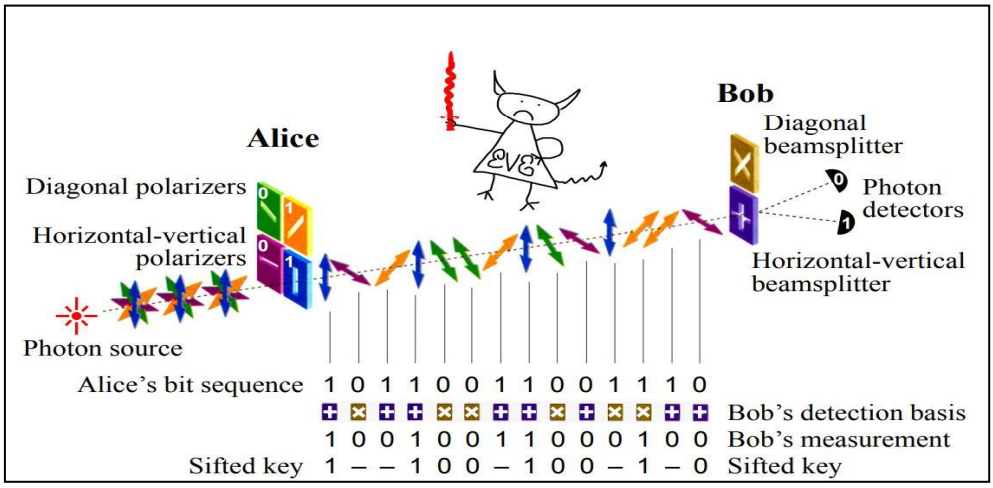
1) Unique feature of Quantum key distribution

In quantum key distribution the two communicating parties (sender and receiver) can detect the presence of any third party i.e. the intruder trying to gain some information about the key. This is basically possible because of the aspect of quantum mechanics - the process of measuring a quantum system in general disturbs the system. The intruder trying to eavesdrop on the secret key must measure it in some or the other way thus introducing some inconsistency. This can be done by using quantum superpositions or quantum entanglement and by transmitting information in quantum states; in such a way communication system can be implemented that detects eavesdropping. [11]

4.0 A Brief Working of Quantum Key Distribution, Bb84 Protocol

QKD protocol, BB84, was named after Charles Bennett and Gilles Brassard. Photons are used to transmit data from one location to another using a fiber optic cable(or free space); this cable may or may not be secure. Let's say Ron and Lisa wants to communicate with each other. They both are connected using a quantum communication channel which allows quantum states to be transmitted. Using Quantum Key Distribution(QKD), the photons are transmitted(one at a time)by the sender Ron through a polarizer(filter) which randomly gives one out of the four possible polarizations and bit designations - Vertical(One bit), Horizontal (Zero bit), 45 degree right(One bit), or 45 degree left(Zero bit). The photons can be sent in superposition state, they transform into a fixed state only when they are read, measured or observed. The photons then travels to Lisa(receiver), which uses two beam splitters – horizontal/vertical and diagonal) to read the polarization of each photon. The receiver does not know which beam splitter to use in advance so; he has to guess which beam splitter to use for each photon. Once the series of photons has been sent, the receiver informs the sender which beams splitter was used for each of the photons in the exact sequence they were sent, and then the sender compares that information with the sequence of polarizers used to send the key. The photons that were read using the wrong beam splitter are discarded, and the resulting sequence of bits becomes the key. If an intruder named Tom tries to eavesdrop on the ongoing conversation and he reads or copies the photon in any way, the state of the photon's will change which will in turn bring errors in the quantum key. By this way the sender Ron and receiver Lisa will come to know that the key has been compromised and hence they will discard the key. Lisa now has to send a new key to Ron so that they could use that key to encrypt and decrypt the information.[8][11]

Fig 5: A diagram that depicts the basic working of Quantum cryptography



5.0 Major Problems in The Quantum Cryptography and Qkd

The security of QKD protocol can be a solid proof of security, but its implementation in real scenario often have imperfections that may be overlooked in the theory[3]. By exploiting such flaws, various attacks, targeting the source(the detectors), have been proposed. With regards to entangled photons, which is proven to be absolutely secure, there are some serious practical problem such as- the cost, another problem is that QKD depends on authenticated classical channel, distance is another factor- the fiber based Quantum Cryptography works only for short distances though the limit can be extended with the help of repeaters but it will definitely create weak points, the error rate is also typically high ,and also keeping the photons entangled long enough to meet the needs of the real

world. Though this kind of system is perfect in theory, but very hard to implement in practice also keeping in mind the real world scenarios.[6]

6.0 Comparative Study of Traditional Cryptography and Quantum Cryptography

Unlike Traditionally cryptography Quantum Cryptography is based on laws of physics rather than mathematical computation. Quantum cryptography does not have some important features such as digital signature, certified mail etc as compared to Classical cryptography which includes all such features. Quantum Cryptography is sophisticated and hence not widely used while traditional cryptography on the other hand is currently being used widely used all over the world. Quantum cryptography or quantum key distribution(QKD) solves the problem of key distribution by allowing the parties to exchange the key with complete security, as assured by the laws of quantum physics. The distance of communication of Quantum cryptography is limited to a few miles whereas communication range of traditional cryptography is millions of miles. As Quantum cryptography is a future technology hence it is not tested fully and it is in its initial stage but classical cryptography is deployed and tested. As it is an emerging technology therefore the cost is high as compared to traditional cryptography. [6]

7.0 Conclusion

Modern computers are likely to be replaced by the Quantum Computers in the near future; hence security aspect must be dealt in accordance with Quantum Computers. Soon the Quantum Computers will likely to break many current encryption protocols hence Quantum Cryptography is the solution that will be almost full-proof in this context. In this paper, attempt has been made to discuss the security aspect with respect to Quantum Computers. Also we have tried to cover and discuss few major areas of it including the working of Quantum cryptography. It is one such technique that may combat against many attacks during the transmission. Quantum cryptography is also compared with the traditional cryptography. Quantum Cryptography through QKD offers the ability and solution that is desired to keep the information safe and secure in all possible manner. Despite all the security provided by this type of cryptography, it definitely has few flaws one of the major flaws is - the length or distance under which the system will work, which is limited. Quantum cryptography and its applications is the future of cryptography and hence is a great area of study today. Quantum cryptography is still a wide area of research which is not fully covered yet such as how a proper quantum key distribution can be done, what are the types of attacks possible and how to prevent them, photon stabilization is another area of research which is under covered and many other such questions. Quantum cryptography is an arising technology and has been experimentally proven feasible so far. This may not be a need for today but with no doubt, it will be a need for tomorrow.

8.0 Acknowledgement

We would like to thank Assistant professor Shikha Bhalla for her helpful discussions and guidance throughout.

References

Kumari, S. (2017). A research Paper on Cryptography Encryption and Compression Techniques. International Journal of Engineering and Computer Science, 6. https://www.google.com/amp/s/searchsecurity.techtarget.com/definition/cryptography%3famp=1

https://searchsecurity.techtarget.com/definition/cryptography

https://www.geeksforgeeks.org/classical-cryptography-and-quantum-cryptography/

https://www.google.com/amp/s/www.csoonline.com/article/3235970/what-is-quantum-cryptography-it-s-no-silver-bullet-but-could-improve-security.amp.html

Sharbaf, M. (2009). Quantum Cryptography: A New Generation of Information Technology Security System. 2009 Sixth International Conference on Information Technology: New Generations,1644-1648. [6]https://www.google.com/amp/s/www.geeksforgeeks.org/differences-between-classical-and-quantum-cryptography/amp/

https://www.google.com/amp/s/www.zmescience.com/science/what-is-photon-definition-04322/amp/

https://www.google.com/amp/s/www.techrepublic.com/google-amp/blog/it-security/how-quantum-cryptography-works-and-by-the-way-its-breakable/

https://www.plixer.com/blog/quantum-cryptography-explained/

https://www.geeksforgeeks.org/classical-cryptography-and-quantum-cryptography/

https://www.norwegiancreations.com/2018/11/introduction-to-quantum-cryptography/

https://www.norwegiancreations.com/2018/11/introduction-to-quantum-cryptography/

https://en.m.wikipedia.org/wiki/Quantum_key_distribution

https://www.researchgate.net