IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 8 Issue 1, January 2021
ISSN (Online) 2348 – 7968 | Impact Factor (2020) – 6.72
www.ijiset.com

Quantum Cryptography

Pranav Mendiratta
Computer Science, Amity University, Noida, Uttar Pradesh, 201313, India

Abstract:

Quantum Cryptography is a transpiring technology in which two groups of people can conduct secure networks communication using theories of Quantum Mechanics. The security of this means of transmission of information is the inviolability of the rules of Quantum Mechanics. Quantum Cryptography gets its derivation from early 1970s when Stephen Wiesner, then at the Columbia University in New York gave the notion of "Conjugate Coding" that formed the basis of this technology. It is based on two important theories of Quantum Mechanics, namely the Heisenberg Uncertainty Principle and polarization of Photons. The Heisenberg Uncertainty principle states that physical properties of position and momentum are connected in such a way that quantification of one averts the observer from concurrently knowing the value of the other. The theory of Photon polarization averts the eavesdropper (person or group of people trying to intercept or leak the information) from copying the qubits following the no cloning theorem articulated by James Park in 1970 that was rediscovered by Wootters and Zurek and by Dieks in 1982. This research paper concentrates on the roots of this technology that is the different protocols it uses, breakthroughs in this technology and its requirements in various other fields. In the end we will also discuss about the scope of this technology in future and its market growth.

Keywords: *Quantum Cryptography, Quantum Mechanics, Qubits, Heisenberg Uncertainty Principle, Eavesdropper, Cloning theorem*

Introduction:

Quantum cryptography is a relatively recent technology and was advanced due to flaws in the prevailing classical cryptographic systems that make use of mathematical algorithms to provide security in communication, these are also referred to as "public-key systems", "private-key systems" and "one-time-pad systems". These classical cryptographic systems are exposed to security inconsistencies related to key refresh and key expansion rates. Most systems sporadically regenerate their keys which leads to large key expansion rates thus are wide-open to security loopholes. Classical/Mathematical cryptographic systems are based on the difficulty in the prime factorization of very large integers that forms the basis of this system for providing secure means of communication. Keys can easily be divulged in many ways by brute-force deciphering, by betrayal from within the company or by exercise of Trojan or sniffer software. In this the encrypted message can be send on public platforms (online chat or email) but the key (that are large prime factors) required to decrypt the message is only known to the communicating parties and the key should only be exchanged via secure platforms otherwise it could be compromised due to action of eavesdroppers. In many famous classical cryptographic systems such as RSA, AES and Diffie-Hellman, eavesdropping or hacking of the system cannot be diagnosed and are purely based on the computational power required for prime factorization of very large integers. For many personal computers finding prime factors of these integers can even take millions of years but advancements in the world of mathematics and that of computers (development of Quantum computers) has reduced the time for which these keys actually remain safe because of high computational powers and new algorithms that can factorize these keys very quickly. And moreover, longer keys can require larger computational power that limits the channel capacity bits-per-second of the information.

So, to summarize this, classical cryptographic systems are no longer that reliable due advancements in technology thus the need to develop better and sophisticated systems of cryptography has given rise to developments of Quantum Cryptographic systems that rely on inviolability of laws of Quantum Mechanics.

1. Quantum Cryptography (Also known as Quantum Key Distribution):

Quantum cryptography focuses on giving security in networks communication using the laws of Quantum Mechanics. The foremost key dispensation protocol was developed by Charles Bennett and Gills Brassard in 1984. It was called the BB84 protocol and is the first quantum key distribution (QKD) scheme. The BB84 protocol relies on sending and receiving of polarized particles or photons that act as traditional bits thus giving

values of 0 and 1. These polarized photons that are in a superposition of 0 and 1 are called qubits. These are passed from one party to another, traditionally from "Alice" to "Bob" which are the names of computers that were originally used in the experiment. The different protocols of Quantum Key Distribution are mainly based on the two important principles of Quantum Mechanics namely the Heisenberg Uncertainty principle and polarization of photons.

The Heisenberg Uncertainty principle [$\Delta \times \Delta p \geq \frac{h}{4\pi}$] states that physical properties of position and momentum are connected in such a way that quantification of one averts the observer from concurrently knowing the value of the other. Also, the theory of Photon polarization averts the eavesdropper from copying the qubits following the no cloning theorem (quantum particles cannot be replicated). Quantum Cryptography allows the parties to share decryption keys with a guarantee that the keys will remain exclusive between them only.

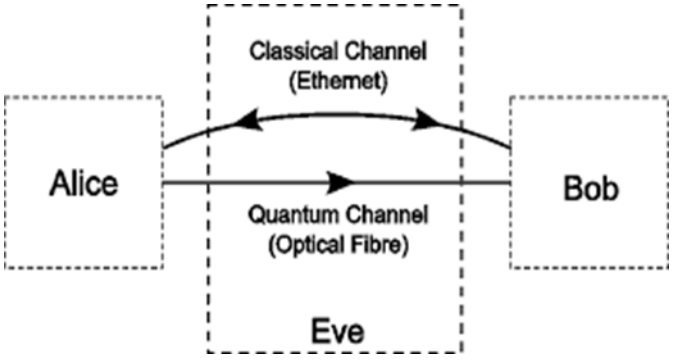

Figure 1: Foundation of Quantum Key Distribution

1.1 BB84 Protocol:

In the BB84 protocol the qubits or polarized photons are transmitted via an optical fibre line and they can be in 4 different polarized states depending the filter/scheme used by Alice for sending the photons to Bob. The polarization of photons can be indicated by these four symbols: -

| — / \

| (0°) and — (90°) represent the rectilinear scheme and can be produced and measured by the filter **+**.

\ (135°) and / (45°) represent the diagonal scheme and can be produced and measured by the filter **X**.

- Photons send by Rectilinear scheme representing 0 and 1:

+(0)= — and **+(1)=**|

- Photons send by Diagonal scheme representing 0 and 1:

X(1)=\ and **X(0)=/**

Alice sends the polarized photons to Bob in one of the four polarized states via the fibre line. Bob can then read/measure the polarization of photons randomly using one of the filters since Alice has not yet told him the sequence of filters that she used. Bob then gets a set of strings in form of 0 and 1s.

For example:

- If Alice sends a sequence of photons from following filters:
  | — \ \ — / | / \ / —

- Then Bob should ideally receive the following set of strings:

  10110010100

Then Alice and Bob will physically contact each other to counter check the filters that each of them used and listening to this conversation will be of no use to the eavesdropper since qubits cannot be replicated (no cloning) and can only be measured at the time they are sent (Heisenberg uncertainty). Thus, if they used the same filter for a particular photon, Bob will record the correct bit but if they used different filter then Bob records the wrong bit and that bit is then discarded. Thus, after discarding the 10% of photons for sifting and calculating the Quantum Bit Error, both get a set of strings of 0 and 1s that is only known to them that can be used for securing the line of networks communication. Quantum Cryptography is also resistant to eavesdropping (people trying to leak information) and even provides a way to check if there is an attempt of hacking of the system or tampering of information, some ways how it is resistant to eavesdropping are broadly explained as follows:

1. The sending of material on photon level secures it against eavesdropping as any attempts of eavesdropping can irrevocably change the material encrypted on the photon because it is backed by the principles of Quantum Mechanics. That is why the polarized photons are very sensitive and exposure to even a little bit of light can change their energy levels thus changing their spin (polarization).

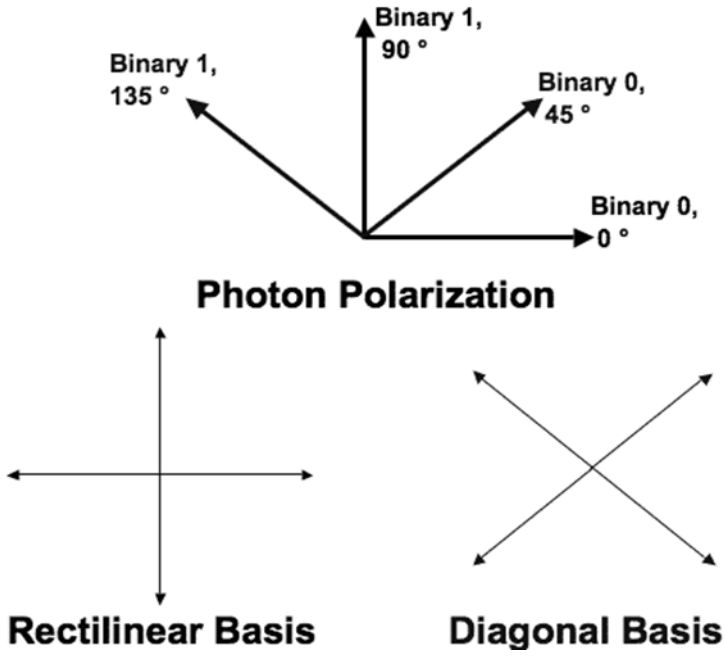

Figure 2: Transmission schemes of the BB84 Protocol

2. Concluding from the Heisenberg's uncertainty principle, the polarization of photons can only be read/measured at the time they are sent and reading/measuring it through the wrong filter can change the spin(polarization) of the photons thus protecting the key from the eavesdropper. This also acts as a means to check if the system has been compromised, if the spin has been changed then during counter check of the filters between Alice and Bob, they would come to know if any photon spin has been tampered with.

3. No cloning theorem also helps to protect the key against eavesdropper because it prevents the eavesdropper from fabricating/making replicas of the quantum cryptographic keys. No cloning also harbours the Uncertainty principle, if one could clone or create replicas of a concealed state and quantify each dynamic mutable with extreme precision then it would contradict the uncertainty principle. Thus, no cloning also harbours the uncertainty principle.

1.2 B92 Protocol:

B92 protocol for transfer of bits is very similar to the BB84 protocol but it makes use of only 2 out of 4 BB84 quantum states for transfer of the qubits.

1. In this protocol Alice sends Bob qubits or polarized photons either in 0° (horizontal) or in +45° polarized state. Let's assign 0° polarized state a bit value of 0 and +45° polarized state a bit value of 1.

2. Now Bob has filters (polarization analysers) and will measure the polarization of each photon randomly by keeping his filter in one of the directions **orthogonal** to that of Alice's. This way he will be able diagnose the photons and will eventually get a string of 0 and 1s.
   For example: If Bob measures and detects the photon along -45° filter then he certainly knows that Alice send a photon using the 0° filter thus he receives a bit value of 0 and similarly a bit value of 1 is obtained if he measures the photon through the +90° filter. Thus, he will now obtain more bit values which are combinations of 0 and 1s.

3. Then Alice and Bob can physically contact each other and confirm which filters they used, listening to this conversation would be of no use to the eavesdropper since the qubits cannot be cloned (no cloning theorem) and can only be measured at the time they are sent (Heisenberg uncertainty).

4. Hence after checking the filters used and calculating the quantum bit error, they will discard some qubits and will now get a set of string that remains exclusive between them. This will be now used to secure the line of networks communication.

1.3 Ekert 91 protocol:

E91 or Ekert 91 protocol was given by Artur Ekert in 1991 and relies on properties of Quantum Entanglement and Superposition of particles.

- Unlike the BB84 and B92 protocol, in this protocol, the polarized photons that are in superpositions of 0 and 1 (also called qubits) exist as an entangled pair in the middle of both Alice and Bob. Thus, Alice is not the one sending the photons to Bob, but both Alice and Bob will receive one photon each, from the source in the middle. This protocol could be the key to implement long distance quantum communication using the source in middle, Satellites can be considered an example of a source in the middle communication. This forms the basis for this protocol to actually work. The particles are given out of the source in the form:

  $\varphi = 1/\sqrt{2}\ (|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle)$

- This represents the superposition of both states of 0 and 1. We already know that the pair of photons in superposition have opposite spins but still we cannot determine which particle is spinning in which direction until spin of one of them is measured, this is due the property of Quantum Entanglement. Quantum Entanglement states that, two particles are co-related in such a way that we cannot know the quantum state of one particle without knowing the quantum state of the other particle far away from it. Thus, when we measure spin of one particle, the other will automatically adjust to spin in opposite direction. For example, if Alice measures particles spin upwards then Bob's particle will automatically acquire a downward spin.

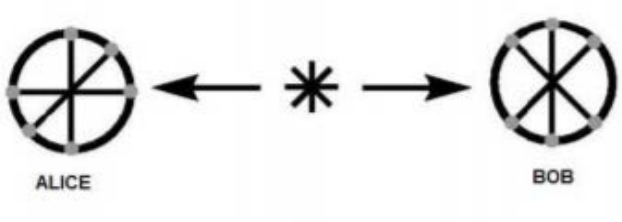

Figure 3: Transmission basis of Ekert 91 protocol.

- Now, one particle is sent to Alice and the other to Bob, they use analysers in one of the three coplanar axis to measure the spin. For Alice A_i represents her particle where i= 1,2,3 and for Bob B_j represents his particle where j=1,2,3. If particles travel along z direction then A_i and B_j can be found in x-y plane.

Taking measuring direction to be along vertical x axis, Alice will measure the particles along angles **φ=** 0°, 45° and 90° whereas Bob will measure along angles **φ=** 45°, 90° and 135° (their measuring basis will differ by 45°). Thus if Alice and Bob both use compatible measuring basis, they will surely get the correct spin otherwise using the analyser in non-compatible basis could give them very random spin results because of entanglement.

For example: If Alice measures along 45° then Bob could get a particle in either spin up or spin down along 90° basis.

- Also, this protocol is resistant to eavesdropping even if the source is in control of the eavesdropper due the very simple property of Quantum Entanglement. The eavesdropper cannot determine the quantum state of one particle until he knows the quantum state of the other which is far away from it because the particles are co-related.

1.4 K05 Protocol:

K05 protocol is a more generalised form of the BB84 protocol for Quantum Key Distribution and unlike the BB84 that uses only 4 polarization states, K05 uses a number of polarization states for the binary digits {0,1}. KO5 has two general subsets of polarization states and each subset is having a number of polarization states for each qubit/logic symbol thus making it difficult for the eavesdropper to measure the polarization states because Alice might randomly select two polarization subsets or polarization states within them. Various steps of the K05 protocols are:

1. Alice sends Bob set of strings of 0s and 1s, for example 1101001110. This binary combination is send to Bob by Alice by randomly choosing two subsets for 0 and 1 from the Poincare sphere. These two subsets and logic for translating the binary states ‘0’ and ‘1’ is only known to Alice and unknown to Bob.

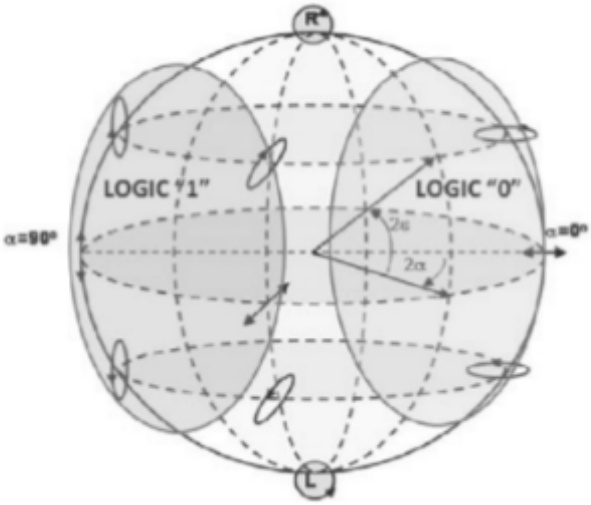

Figure 4: Areas on the Poincare Sphere that contain large polarization sequences that correspond to logic 0 and 1

2. Bob receives the polarized photons and passes them through filters of different orientation which he has chosen randomly since he does not know the subset or logic value used for binary states 0 and 1.

3. The polarization filters used by Bob will either measure the photon or let the photon pass through it, thus giving Bob a string of binary digits.

4. Suppose Bob receives 010110101001 string by randomly measuring the photons, although this is not what Alice had transmitted but the incorrect bits will be discarded later.

5. Bob then contacts Alice over the phone and tells the polarization sequence received by him by measuring the photons but will not reveal the logical sequence he generated.

6. Alice then carries out an experiment, she passes the logic sequence she sent to Bob through the polarization sequence that Bob reported to receive. Then she compares the initial bit string with the one produced in the experiment and notes the common bits.

7. Finally, Alice will tell Bob which polarization filters were used correctly for measuring the states without telling him the logic used for ‘0’ and ‘1’.

8. After discarding the incorrect bits, Alice and Bob will get a secure key that is used to encrypt messages using a modulo-2 operation as shown in the Fig5.

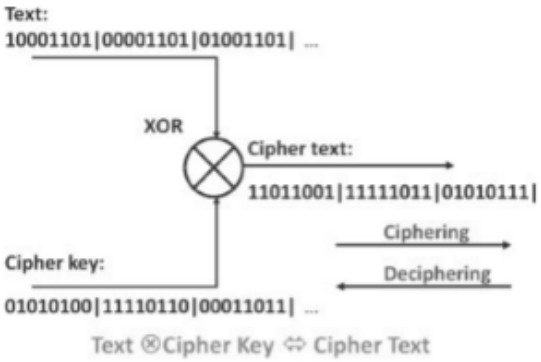

Figure 5: Ciphering of text message using modulo-2 operation.

1.5 KMB09 Protocol:

KMB09 is a 'prepare and measure' type of QKD protocol. Steps to conduct this protocol:

1. Alice first choses two or more sets of basis to send the binary bits. But right now we will assume that Alice has chosen two basis 'e' and 'f' on the Poincare sphere to send the binary bits. Where 'e' represents 0 and 'f' represents 1.

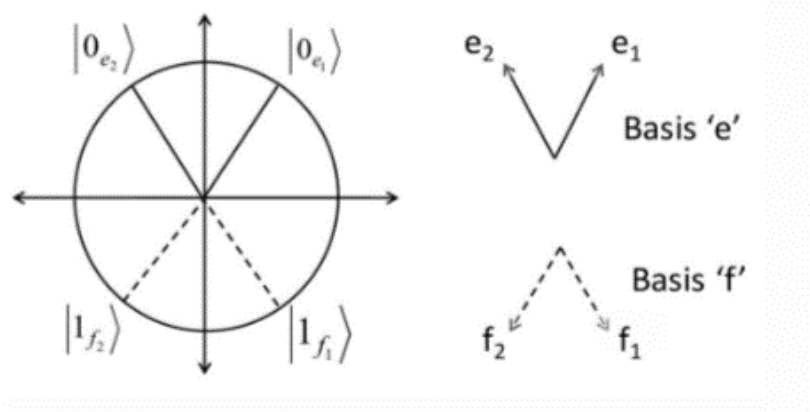

Figure 6: Basis of polarization for transmission.

2. These basis can be differentiated by the index 'i' (for example e_i and f_i) where i=1,….N. For simplicity, we are assuming N=2 for our example, otherwise the protocol can be easily extended to more than N=2 basis for transmission and measurement of photons.

3. Alice now sends the photons to Bob and Bob then measures the polarization states of the photons randomly using filters.

4. Alice and Bob will then physically communicate and Alice will only reveal the index 'i' (i=2 in this example) that is used to encode the bits. Alice will not reveal any information about the key or the sequence of filters used.

5. Thus using only the index values to decode the bits from e_i and f_i will help to improve the security of the system.

1.6 Decoy State Protocol:

Decoy state protocol is a widely used Quantum Key Distribution protocol because it is resistant to Photon Number Splitting (PNS) attack. In practical QKD systems (except the BB84 protocol), multi photon sources are

used for transmission of bits. But multi photon sources do not guarantee secure transmission rates and also limit the maximum channel length. This problem is solved by the Decoy State Protocol because it uses multiple intensity levels at the transmitter's end. This protocol can be implemented using the following procedure:

1. At the Transmitter's end (that is Alice's), the qubits are send using randomly chosen intensity levels.
2. The transmitted signal includes one main signal and several other decoy signals that leads to varying photon number statistics.
3. After the transmission has been done, Alice will publicly announce the intensity levels used for the transmission of qubits.
4. This information will be used by Bob for sifting his qubits and attain a secure key.

1.6.1 Ways how Decoy State Protocol is resistant to a PNS attack:

1. As we know that a successful PNS attack requires maintenance of Bit Error Rate (BER) at the receiver's end but the Decoy State Protocol helps to avoid this by use of source that transmit at multiple intensity levels.
2. We can also check if there is a PNS attack on the communication line by observing BERs associated with each intensity levels.

1.7 Differential Phase Shift QKD Protocol (DPS-QKD):

Differential Phase Shift protocol is based on the fact that only a part of relative phase information of weakened coherent pulses can be recorded. The setup of this protocol can be seen in the diagram below (fig.7) :

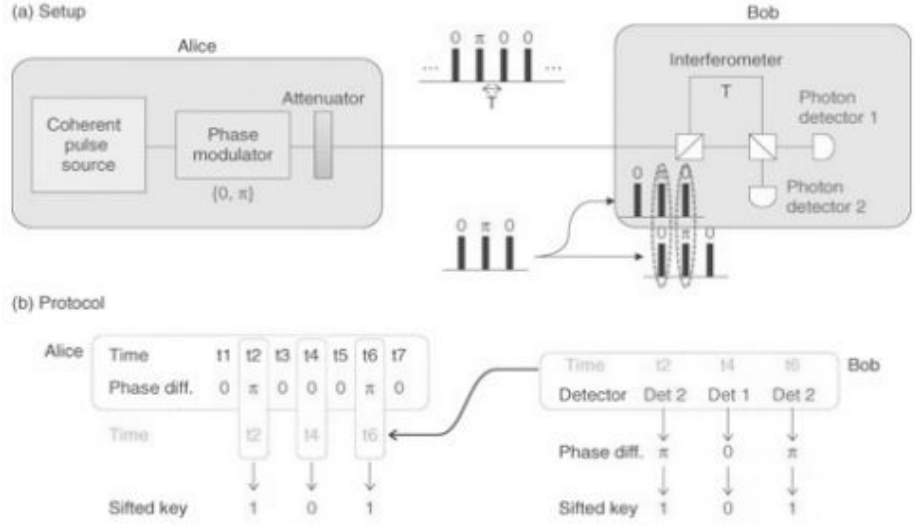

Figure 7: Differential Phase Shift Protocol

1. Firstly, the sender Alice will prepare a chain of coherent pulses and randomly modulates the relative phase of the pulses with 0 or pi.
2. After being weakened, these light pulses are transmitted to Bob such that the photons per pulse are less than 1.
3. Bob uses one-pulse delay interferometer to cause succeeding pulses to interfere and records the relative phase information with the help of photon detectors at the interferometer's output.
4. Since the light pulses are attenuated, only a part of the relative phase information would actually be readable but the derived information should match to the phase modulations by the sender.

5. Bob also records the timestamp information of the photons and which detector it clicked on (relative phase information).

6. Next step is that he generates a key by allocating bit 0 to relative phase 0 and bit 1 to relative phase pi. Bob then sends only the timestamp information to Alice who uses it along with her phase encoding records to generate a key. This key is called a sifted key.

7. Thus, after error correction and privacy amplification a secure key is obtained which can be used for securing the line of communication.

1.8 Coherent One-Way (COW) Protocol:

The basis of this Quantum Key Distribution protocol is that the information is actually encoded in time. Steps to conduct this protocol are:

1. Alice first sends bland pulses or pulses that have mean photon number $\mu<1$, typically $\mu=0.5$ (μ- pulse). The logical bits '0' and '1' are encoded in these two sequences of the pulses, 0-μ represents '0' and μ-0 represents '1'. Alice also sends μ- μ pulses as a decoy sequence for more protection.

2. Now to measure the key, Bob will record the time of arrival of the pulses on the detector D_B and he also monitors the channel via detector D_M.

3. Photons are detected on an unbalanced interferometer that has a path-length difference of T (pulse period).

4. For maintaining security, Bob will check the demographics on the detector D_M and also check for destructive interference of Decoy and logical sequences on the interferometer. If there is a break in coherence between two pulses as well as reduction of visibility, we can make out that there is an eavesdropper intercepting the signal. In this case the key is discarded to prevent any loss of information.

5. The time sequences help Bob to generate a raw key which is a combination of 0s and 1s.

6. Bob will then physically contact Alice and will only reveal the time sequences obtained on the monitor without revealing the actual key obtained. Alice will then check the sequence and tell Bob which of them were decoy sequences which will then be discarded.

7. Thus, after applying error correction and privacy amplification schemes, a secure key is generated that can be used to secure the line of communication.

1.9 BBM92 Protocol:

The BBM92 protocol is similar to the BB84 protocol but instead it uses entangled pair of photons produced in the state $|\psi^-\rangle$.

1. There is a source that produces entangled pair of photons, these photons are then split up and one is sent to Alice and one to Bob.

2. Alice and Bob measure the polarization of photons by using two non-orthogonal basis which are complementary to each other namely the Horizontal (H) and Vertical (V) basis where H=0° and V=90°. They can also use the +/- basis where (+)=+45° and (-)=-45°.

3. They measure the polarization of photons randomly using different basis. Then they will contact each other to check the basis used for measurement, if they used same basis to measure then that reading is saved.

4. The basis need to be in anti-correlated form to make the secret key and the rotational variance of $|\psi^-\rangle$ explains that Alice and Bob will experience anti-correlation only in H/V basis or the +/- basis. This can be seen through the equation:

$$|\psi^-\rangle = 1/\sqrt{2}(|HV\rangle - |V\,H\rangle) = 1/\sqrt{2}(|+-\rangle - |-+\rangle)$$

5. Then they will contact each other to discuss which basis were used correctly and discard the ones that were different since they would lead to uncorrelated results. Thus, they get a set common basis they used for measurement of the photons.

6. Then Alice and Bob will assign H or + a bit value of 0 and V or – a bit value of 1 thus giving them a set of string of 0s and 1s that forms the raw key.

7. The security of this protocol, same as the BB84 protocol, depends on the inviolability of rules of Quantum Mechanics namely the Heisenberg Uncertainty principle and the No-Cloning theorem.

1.10 Six-State Protocol:

Six-State protocol was given by Pasquinucci and Nicolas Gissin in 1999 in their report "Incoherent and coherent eavesdropping in the Six-State protocol of quantum cryptography." Six-State protocol can be conducted in the following way:

1. First Alice sends Bob photons that are polarized using any one of the three basis as shown in the figure (fig.8). These photons are then transmitted to Bob via an optical fibre line.

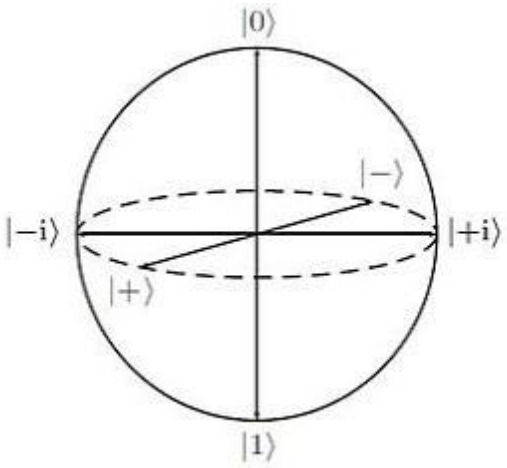

Figure 8: - 3 different basis of transmission for Six-State Protocol.

2. Bob will then measure the polarization of photons randomly using one of the three filters.

3. The probability of measuring the correct polarization state is 1/3.

4. Then Alice and Bob will contact each other on an unsecure but authenticated line of communication to compare the filters used without revealing the key obtained. The bits measured using same filters are saved and after applying error correction schemes, a secret key is generated.

5. Six-State protocol produces more errors during attempted eavesdropping thus making it easier to detect eavesdropping because the eavesdropper has to choose from three different possible basis. Thus, this system can provide a higher level of security.

2. Threats to Quantum Lines of Communication:

Figure 9: Image of an Eavesdropper

2.1 Intercept and Resend:

Intercept and resend is based on a 50% success probability for the Eavesdropper. As Alice sends the key to Bob, the Eavesdropper in the middle will intercept and will randomly try to measure the quantum states as he does not know the correct orientation in which Alice actually sent them. Thus, he might be able to get a success rate of 50%. Then the Eavesdropper will pass on the quantum states that she measured to Bob, just like the eavesdropper Bob will randomly measure the photons as he does not know the orientation in which they are sent. Thus, if the Eavesdropper successfully measured and passed all the orientations correctly then he might be able to get the key (probability of this is only 50%). Also the probability of Alice and Bob dissimilarity and identifying the presence of Eve on comparing n bits publicly is given by the formulae:

$$P(d)= 1-(3/4)^n$$

2.2 Man in the Middle Attack:

Just like any other classical protocols, Quantum Key distribution is also resistless to Man in the Middle attacks because one cannot authenticate whether you are sending the information to the right person. For this, the two communicating parties can have a pre-decided secret key that can be used for secure authentication schemes.

2.3 Trojan Horse Attacks:

In Trojan Horse Attacks, the Eavesdropper sends in bright-light through the quantum channel and tries to study the back reflections of the quantum states.

2.4 Denial of Service:

As we know that Quantum Key Distribution is conducted via dedicated optical fibre lines, a denial of service attack can take place by simply cutting or blocking the transmission lines. This has been motivating the scientists to develop alternate methods of transmission of the keys.

2.5 Security Proofs:

If we assume that the Eavesdropper has unlimited resources such as a classical and quantum computers then more efficient attacks are possible, but BB84 protocol is secure to most of these attacks but some conditions that are mandatory for that are:

- The eavesdropper cannot access Bob and Alice’s decoding and encoding devices.

- Numbers generated for the keys should be truly random.
- The classical channel of communication should be authenticated to make sure it is secure.
- Message should be coded by the one-time-pad systems.

2.6 Photon Number Splitting Attack:

In BB84 protocol, the photons are send via attenuated laser beams that have very less number photons like 1 or 2 photons per pulse. If the photons that are send via the laser are more, then the Eavesdropper can store the extra photons in the quantum storage and pass the remaining to Bob. Then the eavesdropper can listen to the encoding basis get the key hence will get access to the information. One very simple solution to this attack is use of single photon source instead of attenuated laser.

3. Various QKD tools being developed:

3.1 Quantum Oblivious Transfer (QOT):

Oblivious Transfer (OT) is a tool in which Alice sends Bob two pieces of information in such a way that Bob can only choose to see one of them and Alice does not get to know which message did Bob actually open. One-out-of-Two OT has been very useful in developing many other cryptographic contraptions on classical bit systems. Now with the introduction of quantum technology, oblivious transfer can be done on photon level thus making the system more sophisticated and resistant to attacks.

3.2 Quantum Signatures (QS):

Digital/Electronic signature has nowadays been a very popular field of cryptography to prevent forgery of signatures. In this, there is private key which is used to create a signature and the person creating the signature only has it. There is also a public key that is a general key and can be used by any other person to check if the signature is authentic but this key cannot be used to change the signature on the message. It is very difficult to decipher the private key from the public key because of large computational power required to decrypt the code but with development of quantum computers, these private keys can easily be deciphered. Thus, quantum cryptography can be used to make quantum signatures that are highly secure and cannot be forged.

3.3 Quantum Bit Commitment (QBC):

A commitment scheme is a cryptographic tool in which two parties are involved and one makes a commitment to the other but in such a way that the commitment is not revealed until a particular time. It is required to make sure that the committing party do not change or step-back on their commitment. This scheme can be implemented on a bit level by sending the commitment in the form of bits via a fibre line only to be revealed later. This is very useful in protocols such as flicking of coin, safe computation and zero-knowledge proofs.

3.4 Quantum Authentication:
Quantum Authentication is a cryptographic tool in which two parties, Alice and Bob want to exchange information. Alice wants to send a memo ‘M’ which is semi-important such as a news report to be published. But there is an Eavesdropper who is trying to change the memo ‘M’ or prevent Bob from receiving the memo. Now Alice sends Bob a key ‘K’ using qubits (polarized photons) via a fibre line. Alice sends the memo in the form [M,Rk(M)], Bob will get the memo in the form [M’,F] and he will check if F=Rk(M’).

If it is correct then Bob will be sure that he got the right memo and it hasn’t been tampered with. The function Rk mustn’t be weak otherwise the eavesdropper can easily guess it.

3.5 Quantum VPNs:

VPN is a tool that helps to create a private server across a public server such that programs can run inside it as if the two computers were on a common network. Currently, these VPNs have end-to-end encryptions via classical encryption systems such as the RSA system. In the near future these systems will not be safe and quantum VPN will take over to provide a more secure network. Microsoft has already taken an opensource initiative called "PQ Crypto-VPN" to develop algorithms for Quantum encrypted VPNs.

4. Breakthroughs in QKD Technology:

4.1 QKD in daylight:

ETRI that is the Electronics and Telecommunications Research institute has recently been able to send photons in the daylight. As we know that polarized photons or qubits are very sensitive to light and it can change the data encoded on the photon thus this is a major breakthrough in this technology. Specifications of this development are as follows:

- ETRI developed and used a polarization encoding chip for this experiment that was able to reduce the disturbance caused to the photons by the sunlight thus they were able to conduct this experiment successfully with secure key rate of 142.94kbs and bit error of 4.26% during the day over a stretch of 275m.

- The encoding chip helped to miniaturize many components of the QKD system thus making the system usable in various other fields and technologies. These miniaturized QKD systems provide secure networks communication at such light weight thus can be very useful in other developing technologies such as Unmanned Aircraft Vehicles (UAV) and self-propelled vehicles.

4.2 Continuous-Variable QKD:

Continuous-Variable Quantum Key Distribution (CV-QKD) is another breakthrough in QKD technology because unlike the traditional QKD systems, CV QKD can be executed over common optical telecommunication elements over larger distances. Unlike the traditional QKD systems, CV-QKD makes use of fragile coherent laser vibrations.

- Recently tests were conducted in China on CV-QKD by Yichen Zhang, Song Yu, Hung Guo and their colleagues at Beijing University of Posts and Telecommunications and Peking University in the cities of Xi'an and Guangzhou on commercial fibre lines. In both the tests, the fibre lines were "dark", that is the fibre lines were free from any congestion or traffic. Secret Keys were transmitted over a distance of 30km in Xi'an and over a distance of 50km in Guangzhou breaking the prior record of 17km. They also broke the prior record of 0.3kps of key transmission rates (KTR) and achieved a KTR of 6kps.

4.3 Controlling the travel of Photons:

The National University of Singapore (NUS) has revealed that they had been working with Singlet on a project of Quantum Key Distribution and have had a breakthrough in it. They recently announced that while transmission of photons in Quantum Key Distribution, they can co-ordinate the travel of pairs of photons (one for each party) through separate fibre lines. They also mentioned that without using this technique the photon order might change while transmission thus making it difficult for the communicating parties to agree upon an encryption key.

uring 5G Networks

4.5 QKD in securing 5G Networks: A research was carried out by High Performance Networks (HPN) research group at the University of Bristol and they proposed a solution of providing 5G technology with ultra-low-latency and high-bandwidth communication. This can be done by coalition of infrastructure virtualization and quantum technologies.

As we know that the soon to be introduced 5G networks will mostly rely on software architecture so any attempts of hacking with an intention to damage this network could affect the whole internet. Thus, to ensure secure and fast internet speeds development of fully programmable virtualisation platforms in coalition with quantum technologies was proposed.

The proposed quantum 5G network could work across multiple advanced 5G operator's networks since it uses compliant virtualisation technologies.

5. Future Market for Quantum Cryptographic tools:

Quantum Cryptographic tools will be required to fulfil the needs of a number of industries, these include:

5.1 Banking and Finance:

Banks constantly need to update their security systems to keep in pace with the developing technologies (such as Quantum Computers) since they have to ensure availability of quick and reliable data and provide secure net banking options.

Figure 11: Banking and Finance:

5.2 Cloud and Data Warehousing : As we know that a lot of companies are shifting to cloud storages rather than having their own data centres thus requirements of fast and secure means of transmission of data has become a must to make sure company's sensitive data is protected.

Figure 12: Cloud and Data Warehousing

Government and Defence: With the development of Quantum Computers, confidential data of a country would be considered less secure and could be subject to cyber strikes. Thus, to ensure security of this crucial data, Quantum Cryptography is required.

Figure 13: Government and Defence

5.4 Critical Infrastructure: Since crucial control systems like SCADA (Supervisory control and data acquisition) are now more closely meshed with the internet hence additional security is required for their protection against cyber-attacks.

Figure 14: Critical Infrastructure

55 Healthcare: Healthcare data contains crucial information about a patient which could be misused at a large extent thus we need to ensure that this data remains secure even during its transmission over a network.

Figure 15: Healthcare

Figure 16: Telecommunication

5.6 Telecommunication: Telecommunication is the basis of means of communication and passing of vital information such as news articles to be published or stock market news that take place across telecommunication networks every day. Thus, requirement of secure and fast means of telecommunication demands the creation of quantum means of telecommunication.

6. Economic Growth Forecast:

- Quantum Cryptography is anticipated to grow rapidly due to its demands in various industries because of rising privacy and data concerns.

- Major companies currently providing Quantum Cryptographic services are:
  ID Quantique (Switzerland), MagicQ Technologies (USA), Toshiba (Japan), Quintessencelabs (Australia), Crypta Labs (UK) etc.

- Quantum Cryptography is approximated to raise profits of about 640 million dollars($) between a forecast period from 2017 to 2023 expanding with a Compound Annual Growth Rate (CAGR) of 14%.

- Geographical division of markets for Quantum Cryptography includes Asia Pacific, Europe, North America, Middle East, Latin America and Africa. These are on the basis of technological advancements, uses, components, vertical and services. North America is predicted to be one of the biggest markets for Quantum Cryptographic tools because of its wide adoption of cloud computing and rising security issues. The major markets in North America for these cryptographic tools are Canada, United States of America and Mexico. Even though Asia Pacific lags behind North America in terms of technology but it is projected to grow at the fastest rate in the coming years and major markets of Asia Pacific include India, China and Japan. Europe is also very advanced thus could be a possible vender for the cryptographic tools, major markets of Europe include United Kingdom(UK), Germany and France.

7. Drawbacks:

- Quantum cryptography is expensive to conduct and with its current technology in use it cannot be considered cost effective.

- Qubits are very sensitive and can be effected by minute noises and vibrations such as sunlight, sound, cuts and turns in the wire etc. This can change the spin of the polarized photon(qubit) thus changing the data encoded on it.

- Wastage of a lot qubits occurs during Quantum Error Correction schemes thus leaving only few qubits to perform the actual computational task.

- Quantum Cryptography cannot be conducted over long distances because longer the distance, larger the noise that can affect the qubits and change their polarization.

Conclusion:

Advancements in field of mathematics and development of quantum computers has led to reduction in security of the classical cryptographic systems such as RSA, AES etc thus, it has become mandatory to develop the technology of quantum cryptography that provide secure means of transmission of information and is resistant to attacks by eavesdropper. In this research report we have discussed about the different Quantum Key Distribution protocols for transmission of information that can be used in different situations for providing security against different types of threats that can compromise our classified information. For example: Decoy State Protocol provides better security against a PNS (photon number splitting) attack.
This research report also talks about the different QKD tools being developed such as Quantum Signatures, Quantum Authentication Schemes and Quantum VPNs etc used in various industries. In the end, we have also discussed about the different breakthroughs in this technology, the future market for this technology and how this technology could grow with a Compound Annual Growth Rate (CAGR) of 14% between a forecast period of 2017-23. Thus after analysing the pros and cons of this technology, I would suggest that this technology holds the key to the future of secure transmission systems and could prove to be the protagonist in this new era of privacy.

References:

1. M. S. Sharbaf, "Quantum Cryptography: A New Generation of Information Technology Security System," *2009 Sixth International Conference on Information Technology: New Generations*, Las Vegas, NV, 2009, pp. 1644-1648. doi: 10.1109/ITNG.2009.173
   URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5070885&isnumber=5070575

2. No-cloning theorem. (2019). Retrieved from https://en.wikipedia.org/wiki/No-cloning_theorem
3. Heisenberg uncertainty principle formula | Example Of Heisenberg uncertainty rule. (2019). Retrieved from https://byjus.com/heisenberg-uncertainty-principle-formula/
4. Applications - ID Quantique. (2019). Retrieved from https://www.idquantique.com/quantum-safe-security/applications/
5. Scientists exchanged quantum information on daylight in a free-space quantum key distribution. (2019). Retrieved from https://www.sciencedaily.com/releases/2018/12/181207125154.htm
6. Global Quantum Cryptography Market Analysis - Industry Trends,. (2019). Retrieved from https://www.openpr.com/news/1761440/Global-Quantum-Cryptography-Market-Analysis-Industry-Trends-Market-Size-and-Forecast-to-2025.html
7. Project, Q. (2019). QKD (B92 protocol). Retrieved from https://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/cryptography-b92/B92_photons.html
8. Quantum Oblivious Transfer. (2019). Retrieved from https://www.tandfonline.com/doi/abs/10.1080/09500349414552291?journalCode=tmop20
9. Quantum Authentication. (2019). Retrieved from https://www.perimeterinstitute.ca/personal/dgottesman/qauthentication.html
10. Quantum Digital Signatures. (2019). Retrieved from https://www.perimeterinstitute.ca/personal/dgottesman/qsig.html
11. Commitment scheme. (2019). Retrieved from https://en.wikipedia.org/wiki/Commitment_scheme
12. Quantum Cryptography Market 2019 Global Trends, Size, Segments and Growth by Forecast to 2023. (2019). Retrieved from https://www.marketwatch.com/press-release/quantum-cryptography-market-2019-global-trends-size-segments-and-growth-by-forecast-to-2023-2019-01-30
13. Quantum key distribution. (2019). Retrieved from https://en.wikipedia.org/wiki/Quantum_key_distribution
14. Post-quantum Cryptography VPN - Microsoft Research. (2019). Retrieved from https://www.microsoft.com/en-us/research/project/post-quantum-crypto-vpn/
15. Virtual private network. (2019). Retrieved from https://en.wikipedia.org/wiki/Virtual_private_network
16. Abrams, L. (2019). Microsoft Adds Post-Quantum Cryptography to an OpenVPN Fork. Retrieved from https://www.bleepingcomputer.com/news/microsoft/microsoft-adds-post-quantum-cryptography-to-an-openvpn-fork/
17. KMB09 protocol. (2019). Retrieved from https://en.wikipedia.org/wiki/KMB09_protocol
18. Quantum digital signature. (2019). Retrieved from https://en.wikipedia.org/wiki/Quantum_digital_signature
19. Ilic, N. (2007). *The Ekert Protocol* (pp. 1-4). Waterloo, ON, Canada N2L 3G1: Department of Physics, University of Waterloo. Retrieved from http://www.ux1.eiu.edu/~nilic/Nina's-article.pdf
20. List of quantum key distribution protocols. (2019). Retrieved from https://en.wikipedia.org/wiki/List_of_quantum_key_distribution_protocols
21. Kartalopoulos, S. (2009). *K08: a generalized BB84/B92 protocol in quantum cryptography* (pp. 1-8). Tulsa, OK 74135, U.S.A.: Williams Professor in Telecommunications Networking, the University of Oklahoma 4502 E, 41st Street. Retrieved from https://onlinelibrary.wiley.com/doi/pdf/10.1002/sec.111
22. Scott Pakin, P. (2019). The Problem with Quantum Computers. Retrieved from https://blogs.scientificamerican.com/observations/the-problem-with-quantum-computers/
23. March: quantum cryptography | News | University of Bristol. (2019). Retrieved from http://www.bris.ac.uk/news/2019/march/quantum-cryptography.html
24. Barbaschow, A. (2019). Researchers in Singapore demonstrate new quantum key distribution technique over Singtel's fibre network. Retrieved from https:// https://www.zdnet.com/article/researchers-in-singapore-demonstrate-new-quantum-key-distribution-technique-over-singtels-fibre-network/
25. Griffin, M. (2019). Chinese researchers hack "Unhackable" quantum encryption, reveal method – Fanatical Futurist by International Keynote Speaker Matthew Griffin. Retrieved from https://www.fanaticalfuturist.com/2019/03/chinese-researchers-crack-unhackable-quantum-encryption-and-reveal-method/
26. Lopes, Minal. (2015). On the performance of quantum cryptographic protocols SARG04 and KMB09. Proceedings - 2015 International Conference on Communication, Information and Computing Technology, ICCICT 2015. 10.1109/ICCICT.2015.7045661.
27. Decoy state. (2019). Retrieved from https://en.wikipedia.org/wiki/Decoy_state
28. Tokura, Y., & Honjo, T. (2019). Quantum Cryptography | NTT Technical Review. Retrieved from https://www.ntt review.jp/archive/ntttechnical.php?contents=ntr201109fa8.html
29. Xavier, G., Ferreira da Silva, T., Vilela de Faria, G., Temporão, G., & von der Weid, J. (2019). *Practical random number generation protocol for entanglement-based quantum key distribution* (pp. 1-10). R. Marquês de São Vicente 225 – Rio de Janeiro - Brazil: Center for Telecommunication Studies, Pontifical Catholic University of Rio de Janeiro. Retrieved from https://arxiv.org/ftp/arxiv/papers/0810/0810.0483.pdf
30. Six-State Protocol. (2019). Retrieved from https://en.wikipedia.org/wiki/Six-State_Protocol

31. Erven, Chris. (2019). On Free Space Quantum Key Distribution and its Implementation with a Polarization-Entangled Parametric Down Conversion Source.
32. Access Date-19 June 2019, Retrieved from https://www.osapublishing.org/DirectPDFAccess/2A47C851-F61D-4061-61223182A98735A1_183725/oe-17-16-13326.pdf?da=1&id=183725&seq=0&mobile=no