University of Regina

Department of Computer Sciences

Winter 2020

CS 834 - Fundamentals of Computer Systems Security

Project Report

"Quantum Cryptography "

Submitted to Dr. Habib Louafi

By

Simranjeet Randhawa

Regina, April 15, 2020

Outline of the Project

- Introduction
- Classical Cryptography vs Quantum Cryptography
- Bits to Qubits
  - Representations of Qubits
- Quantum cryptography Fundamentals
  - Entanglement state
  - Key Distribution problem
  - Quantum No-cloning theorem
  - Heisenberg Uncertainty principle
- Quantum Key Distribution
  - Standard BB84 Protocol
    - Working Mechanism
    - Example
    - Protection against Eavesdropping
  - Ekert Protocol
    - Working Mechanism
    - Eavesdropping
- Security of Quantum Key Distribution
  - Eavesdropping attack
    - Individual
    - Collective
    - Joint
  - Assumptions of security in QKD
    - Quantum mechanics is correct
    - Authentication is secure
  - Security Proofs for QKD
    - Entanglement Distillation
- Proposed Secure System using Quantum Cryptography
- Quantum Bit Commitment Protocol
  - Commit
  - Reveal
- Quantum vs Post Quantum Cryptography
- Quantum secret sharing
- Mistrustful Quantum Cryptography
  - Quantum Coin Flipping
  - Quantum Commitment
- Conclusion
- Future Scope

Introduction to Quantum Cryptography

Quantum cryptography is one of the most trending and popular nowadays in the world of information security and technology. Quantum cryptography which also referred to as Quantum Encryption is about encrypting and modifying the messages in such a way that cannot be read by any other third party without any authorization consent. The main aim of the paper is to study the mechanism behind quantum cryptography and to know the recent innovations that occurred which contributes to protecting the system at its best. Quantum Cryptography has provided top-notch cryptographic solutions in terms of distributing the key among the authorized participants. It is one of the most popular technologies which has the capability of creating a secure communication channel among the different entities while applying all the significant concepts of quantum physics when exchanging messages. In Quantum Cryptography, a sequence of photons is used to transfer the messages from one entity to another over a fiber-optic channel. The message is sent in such a way over a fiber optic cable that enables the endpoints to evaluate the properties of the photons in which data is being transmitted and then a key is being extracted to decrypt the message. In this process, the sender sends the light particles which are photons via a polarizer which then further assigns a chosen bit among the other four possible polarization bits, which are the vertical, horizontal, 45 ° right and 45 ° left bits. The photons are then transmitted to the recipient side which also then divides the photons into two beams, which could be a diagonal, horizontal or vertical way to read the polarization of these photons. The receiver itself is not capable of deciding the beam splitters as mentioned but they have to guess which beam splitter would be appropriate to use. After that, the sender tries to match the series of polarizers that were used to transmit the photons in a particular order. Some of the photons are rejected which were interpreted using the incorrect beam splitter by the receiver and the rest of the bits which were interpreted using the appropriate beam splitter are then kept to create a key. The photons states are altered if they are copied or read by the eavesdropper. Hence the change will be sensed by both the receiver and sender-side if the eavesdropper tries to read, modify or make an identical copy of the photons. The Quantum Cryptography is dependent on two significant components of the quantum mechanics, naming Heisenberg uncertainty and the photon polarisation concepts. [1] Generally, the classical public-key cryptography is dependant on the complex mathematical proofs and algorithms which can be easily decrypted with the invention of intelligent quantum computers. In classical cryptography, there are high chances of an eavesdropper to read the contents of the message. The algorithm which can be used with quantum cryptography is a one-time pad that is considered to be more secure by using the random key. Today in the world where there are a lot of scams happening around us, like the message contents are modified by the unauthorized access and the content is not in its original state when sent via the sender to the receiver. Due to this severe issue, there is an urgent need for unbreakable and secure encryption techniques where the data does not change its original state. The introduction to quantum cryptography can lower the chances of altering the message, hence retaining the contents' original state. Thus, Quantum Cryptography via the QKD provides the best-fit solutions in protecting the data when sent to over an unreliable channel and this solution will last long in the coming future too.

Classical Cryptography as compared to Quantum cryptography

- **Classical Cryptography:**

Traditional Cryptography relies on the fundamentals of mathematics and also depends on the complexity of factorizing the large set of numbers. Traditional methods are dependent on the high rate difficulty of the mathematical problems to factorize the huge set of numbers. Techniques in classical cryptography:

1. **Symmetric Cryptography-** In this type of cryptography, a single or an individual key is used for the encryption and decryption of the data where the encryption key is used as a private key. In symmetric cryptography, the only limitation of it is that the private key should be shared among the authorized and authentic users, both the sender and receiver.

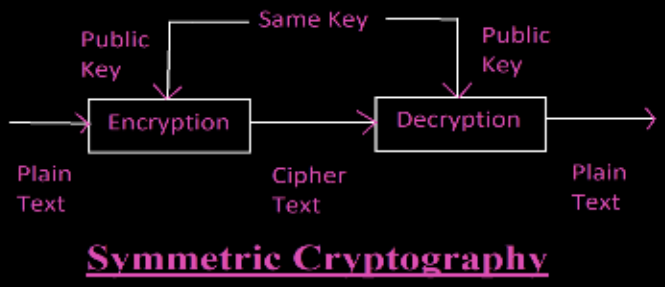

Figure 1. Symmetric Cryptography [1]

2. **Asymmetric Cryptography:** In this type of cryptography, it has a pair of keys that are the public and private key which is used to encrypt or decrypt the data. In this case, the message is encrypted using the receiver's public key and the receiver decrypts using the private key to decrypt the message that the sender has sent to it. This type of technique has overcome the issues of key distribution.

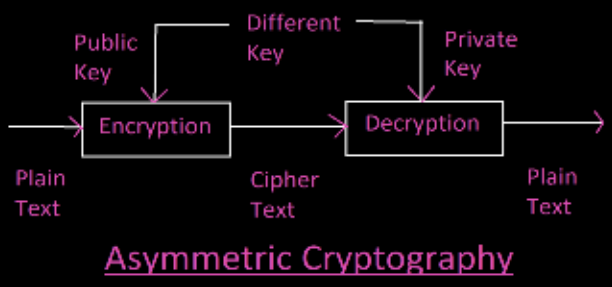

Figure 2. Asymmetric Cryptography [2]

- **Quantum Cryptography:**

It relies on the fundamentals of physics and also it is based on the quantum mechanics laws. This type of cryptography is very popular which stresses the basics of quantum physics as it allows two parties to communicate with each other securely. The Quantum Cryptography is dependent on two significant components of the quantum mechanics, naming Heisenberg uncertainty and the photon polarisation concepts. Generally, the classical public-key cryptography is dependant on the complex mathematical proofs and algorithms which can be easily decrypted with the invention of intelligent quantum computers. In classical cryptography, there are high chances of an eavesdropper to read the contents of the message.

The table given below distinguishes between classical cryptography and the Quantum cryptography:

Quantum Approach	Classical Approach
• Relies on the basics of Quantum mechanics • Sophisticated methodology • The digital signature is not required • 1 MBPS → Average bit rate • Storage of Bit → N-Bit string • It is capable of communicating within the range of ten miles • When this type of cryptography is at its beginners' level then it is tested partially, not fully • Relies on the fundamentals of laws of physics • The medium of communication is not independent • Cost is high	• Relies on the basics of mathematical calculations • Used widely • The digital signature is required • The bit rate is based on the computational power • Storage of Bit → 2N bit • It is capable of communicating within the range of million miles • This type of cryptography is tested and deployed • In this, when the computational power increases then it requires upgradation. • The medium of communication is independent • Cost is low

To get a secured communication between the authentic parties the basis of quantum physics is used. The Quantum key distribution uses the mechanics of Quantum to provide protected communication between the parties. This type of cryptography can also provide secure key distribution functionality by using the quantum mechanical properties of the particles.
Quantum Cryptography via the QKD provides the best-fit solutions in protecting the data when sent to over an unreliable channel and this solution will last long in the coming future too.

Bits to Qubits

'Bit' is the core unit of information in the field of computer science. The bit can be either 0 or 1, for instance, if there is a switch or capacitor that is charged so it will show 1 and if it is not charged, the value of the bit will be 0. There is a significant amount of possibilities to represent a Qubit physically as in the quantum system with at least two conditions can be used as a Qubit. For instance, the polarization of a particle of light can illustrate the qubit state.

- **Representation of Qubit**

In mathematical computation, the Quantum state is represented as → $|\psi)$, is considered to be a component of a finite-dimensional vector space. It is also known as the '*H*. →Hilbert Space'. A quantum state denoted by $|\psi)$ is viewed as a segment that is available in Hilbert space H.

Scalar product of $|\psi)$ and $|\varphi)$ is denoted by $(\psi|\varphi)$. It is helpful to manage standardized states, so we require $(\psi|\psi) = 1$ for all states $|\psi)$ that have physical importance [3]. The quantum simple of the bit is known as a qubit, which is gotten from quantum bit. A qubit is a component, in which we can present an orthonormal premise, comprising of $|0)$ and $|1)$ [3]. In contrast to its old-style partner, the state of quantum can be in any intelligent superposition of the premise state:

$$|\psi) = \alpha|0) + \beta|1) \quad (1)$$

where α and β are coefficients. We need to satisfy the following to satisfy the requirement of standard states:

$$|\alpha|^2 + |\beta|^2 = 1, \text{where } |\cdot| \text{ indicates the supreme worth.}$$

Quantum Cryptography Fundamentals

- **Entanglement state**

By direct interactions between the subatomic particles, the entanglement state is created. This type of interaction can be in different multiple forms. Among these, the most popular and common method is the spontaneous parametric down-conversion. This method is used to create a couple of photons which are intertwined in polarization. One of the possibilities is to establish the entanglement among the quantum arrangements that have not interacted directly via the entanglement exchange.

Quantum entanglement is known to be a quantum mechanical marvel in which the quantum conditions of at least two items must be portrayed concerning one another, even though the individual articles might be spatially isolated. This stimulates connections between noticeable physical characteristics of the frameworks. For instance, it is feasible to plan two substances in a solitary quantum state with the end goal that

when one is up, the other one will consistently be seen to be turned down and the other way around, this despite the way that it is difficult to anticipate, as per quantum mechanics, which set of approximations will be watched. Therefore, approximations performed on one framework appear to be quickly impacting different frameworks entangled with it. Be that as it may, quantum entanglement doesn't allow the transmission of traditional style data quicker than the speed of light. Simultaneously, it stimulates a part of the additional organized conversations concerning the hypothesis of quantum. The relationships anticipated by quantum mechanics and saw in the test, dismiss the standard of neighborhood authenticity, which is that data about the condition of a framework should just be intervened by collaborations in its prompt environment. Various perspectives on what is happening during the time spent quantum entanglement can be identified with various translations of quantum mechanics.

- **One time pad and key distribution problem:**

One time pad is a technique in quantum cryptography where the message is translated into binary forms in terms of 0's and 1's. Also, in this, the key should be of a similar length of the message. Key and message bits are then further combined using the XOR method. This method converts the plain text into ciphertext. The below equation states:

$$c_i \equiv m_i + k_i \pmod 2,$$

where c_i = Ciphertext, m_i = Message and k_i = key

Following properties of the key **MUST** satisfy to make the ciphertext unbreakable or hard to decrypt:

- Key → truly random
- Key → similar length of the plain text
- Key → not be reused in any of the iterations in one-time pad process
- Key → secret and private

Considering a situation where Alice desires to send a memo to Bob, Alice sends a ciphertext to Bob via an unreliable channel. During this transmission, anyone in the channel including an eavesdropper receives an identical copy of the ciphertext regardless of knowing the key. The eavesdropper then tries to extract the original message from the ciphertext but it gets difficult for them as the ciphertext is truly random and does not give any hints about the plain text. However, the decryption that takes place at Bob's end will use the key shared by Alice too and therefore Bob will perform XOR operation to between the bits of ciphertext and the key to extract the original plain text or message. The one- time pad technique is considered to be unbreakable but has a disadvantage too where it requires to use a random string of secret key which must be of the same length of the message. Hence, the onetime pad system replaces the issue of a safe and safe technique for correspondence to the issue of key distribution. Quantum mechanics, accordingly, offers an answer for the key distribution issue where an encryption key is produced among the sender and the receiver by utilizing non-orthogonal quantum states. Quantum non-cloning theorem is part of Quantum mechanics where it states that is nearly impossible for the attacker or eavesdropper to generate another matching replica of the quantum state. In this

situation, if the eavesdropper tries to make any attempt to get the key then according to the QKD technique, it will create a disturbance and this will notify Alice and Bob.

- **No-cloning theorem:**

It is a technique where it is nearly impossible to generate a similar instance of an arbitrary unknown quantum state. A system's state can be entangled with another system. The condition of one framework can be entangled with the condition of another framework. For example, one can utilize the controlled-NOT gate and the Walsh–Hadamard entryway to entangle two qubits. This isn't cloning. No all-around characterized state can be credited to a subsystem of an entangled state. Cloning is a procedure, the aftereffect of which is a distinguishable state with indistinguishable elements. The no-cloning theorem is normally expressed and demonstrated for pure states; the no-cloning theorem sums up this outcome to blended states. The no-cloning theorem has a period turned around double, the no-erasing theorem. Together, these support the understanding of quantum mechanics as far as a class hypothesis. This detailing, known as straight out quantum mechanics, permits, thus, an association with being produced using quantum mechanics to direct rationale as the rationale of quantum data hypothesis (in a similar sense that old-style rationale emerges from Cartesian closed category).

- **Heisenberg Uncertainty principle**

In Heisenberg Uncertainty principle where it is likely to encrypt the data into the quantum characteristics of a photon in a manner that any of the effort to observe and monitor them will create a disturbance in them which is detectable. This is known to be a Heisenberg Uncertainty principle. This principle guarantees that estimating one property that keeps the observer from at the same time knowing the estimation of other property.

Quantum Key Distribution

BB844 Protocol

- **Working Mechanism**

Generally in QKD, the authorized parties like Sender Alice and Receiver Bob fetch the quantum states and later on they measure it. They impart (all correspondence structure ahead is traditional) to identify which of their estimation outcomes could prompt secret key bits; some are disposed of in a procedure called sifting because the estimation settings were incompatible.[4] Error correction is then performed and afterward gauge a security value which portrays the amount of information an eavesdropper may have regarding their key information. If this sum is over a certain threshold, then they prematurely end as they can't ensure any mystery at all. On the off chance that it is underneath the threshold, security intensification is applied to press out any remaining information the intruder may have, and show up at a mutual secret key [4].

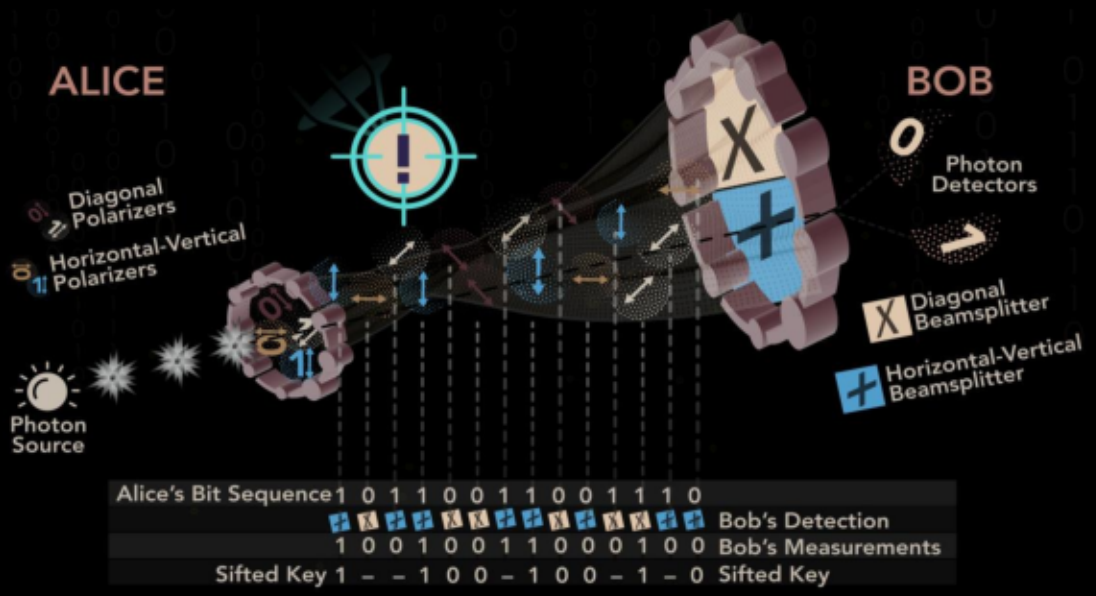

Figure 3. Quantum Key Distribution [3]

1. The sender sends photons via a polarizer or a filter that assigns a random one polarization out of four possibilities and bit designations. Horizontal (bit Zero), 45 degrees left (bit Zero), Vertical (One bit), or 45 degrees right (One bit).
2. Through the two beam splitter mode, the photons transported to the receiver. The polarization of each photon is read horizontally, vertically or diagonally. The recipient doesn't know what beam splitter should be used so, therefore, it requires to find out the appropriate beam splitter which can be used.
3. Once the set of photons is sent over the channel then the receiver conveys a message to the sender to let him know what beam splitter was used for each of the photons in the same order in which the photons were received. Later the compare the information and the order of the polarizers that were utilized to deliver the key. Also, the photons that were sent using the incorrect beam splitter are then discarded and the following set of bits becomes the key.

The basis of Quantum cryptography is that there are a couple of physical characteristics that are associated in a way that when determining a property restrict the monitor concurrently identifying the other's value. It is based on the uncertainty principle is a simple probabilistic connection of the measure of position and the motion of an element with no absolute precision.

- **Example**

Quantum cryptography uses the quantum key distribution (QKD) approach. The sender transfers the photons via a polarizer where: Vertical (1 bit), Horizontal (0 bit), Right 45°(1 bit) or Left 45°(0 bit). Photons are received at the receiver end, which then uses beam splitters to analyze each photon's polarization. When the surge of photons has been sent, the receiver tells the sender which beam splitter (diagonal or rectilinear) was utilized. The sender contrasts that data and the order of polarizers used to send the key.

The particles of photons that were read utilizing an incorrect beam splitter are disposed of, and the subsequent arrangement of bits turns into the key.

BB84 protocol gives adequate security which is related to the quantum no-cloning theorem. Also if we apply the QKD in real-time then Alice and Bob are required to calculate the upper bound of the eavesdropper's data quantitively by analyzing the quantum bit error and other given values. The limitation and challenge of this approach are that eavesdroppers can attack in a way that is way beyond our thoughts and imagination.

Alice's bit sequence	0	1	1	1	0	1	0	0	0	1
Alice's basis	+	x	+	+	x	+	x	x	+	x
Alice's photon polarization	→	↖	↑	↑	↗	↑	↗	↗	→	↖
Bob's basis	+	+	x	+	-	x	x	+	+	x
Bob's measured polarization	→	↑	↖	↑	→	↗	↗	↑	→	↖
Bob's sifted measured polarization	→			↑			↗		→	↖
Bob's data sequence	0			1			0		0	1

Figure 4. Example showing how the sequence is decided

In the above figure, Alice sends the bit sequence and sets the basis of it in 'x' & '+'. Concerning Alice's basis, she randomly sets the photon polarization with horizontal, vertical and diagonal arrows. On the other hand, Bob also sets his basis randomly as 'x' or '+' and then measures polarization random polarizer with horizontal, diagonal and vertical arrows. Based on it, Bob's calculate the data sequence

- **Protection against Eavesdropper**

Alice's basis	Alice's bit	Alice's photon	Eve's basis	Correct	Eve's photon	Eve's bit	Correct
{↑,→}	1	↑	{↑,→}	Yes	↑	1	Yes
			{↗, ↖}	No	↗	1	Yes
					↖	0	No
	0	→	{↑,→}	Yes	→	0	Yes
			{↗, ↖}	No	↗	1	No
					↗	0	Yes
	1	↗	{↑,→}	No	↑	1	Yes
					→	0	No
			{↗, ↖}	Yes	↗	1	Yes
{↗, ↖}	0	↖	{↑,→}	No	↑	1	No
					→	0	Yes
			{↗, ↖}	yes	↖	0	Yes

Figure 5. Protection against Eavesdropper

Eavesdropper, Eve arbitrarily selects a basis for computation and measurements. Now Eve needs to send every photon again to Bob. This act will certainly interrupt with an error. If an eavesdropper tries to alter the photon's quantum state, then an error is generated. The error alerts Alice and Bob of the existence of an eavesdropper. Sharing key procedure starts again – Alice sends a new key to Bob. Bob will catch it as there will be an increased error rate at his end. It is also possible in this case that Eve snoops a smaller number of photons to reduce the chances for error occurrence. In this case, Eve would still have a limited amount of information about the key

Ekert Protocol

- **Working Mechanism**

The Ekert protocol is proposed by Artur Ekert which is a concept where we use the pair of photons. The photons are then distributed in a certain way that Alice and Bob both receive at least one photon from each of the photon pairs. The protocol is based on entanglement properties, the first one is that the entangled states are connected in such a way that when Alice and Bob measure their states regardless of direction, there is a 100% probability of the same answer. The equivalent is credible if the two of them degree some other pair of reciprocal (orthogonal) polarizations. This requires the two far off gatherings have accurate directionality synchronization. Be that as it may, the specific outcomes are arbitrary; Alice can't be expected on the off chance that she (and consequently weave) gets vertical polarization or flat polarization. Any endeavor at eavesdropping using eve demolishes those connections such that Alice and Bob can hit upon. The equivalent is genuine if the two of them degree some other pair of integral polarizations. This requires the two inaccessible gatherings have definite directionality synchronization. Be that as it may, the specific outcomes are irregular; Alice can't be expected on the off chance that she (and subsequently bounce) gets vertical polarization. Any endeavor at eavesdropping using eve wrecks those connections such that Alice and Bob can hit upon. This protocol consists of a private calculation before detecting the existence of Eve.

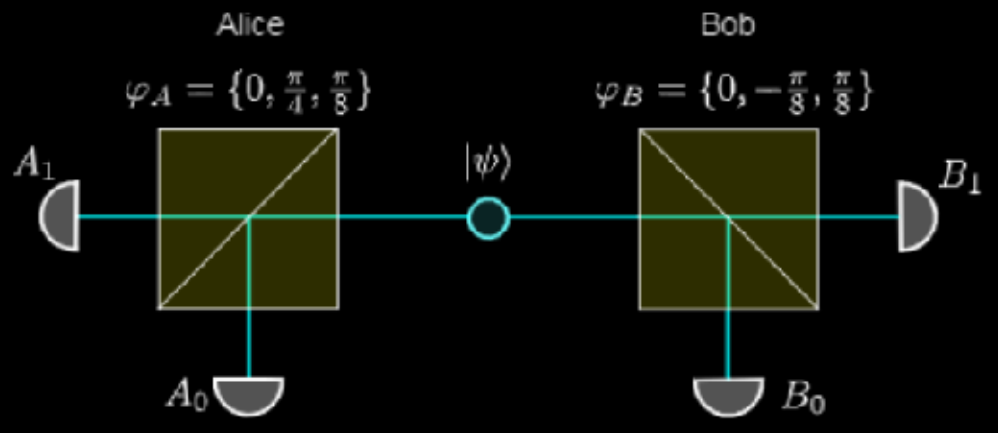

Figure 6. Ekert Protocol [5]

Alice and Bob arbitrarily switch their estimation settings. Sets related with indistinguishable estimation settings (φA=φB) are utilized to create a corresponded key, while those related to non-indistinguishable estimation settings (φA not equivalent φB) are utilized to check the infringement of Bell disparity (and the security of the key).

The dimension degree includes Alice calculating each photon she gets the use of some basis from the set. They maintain their collection of foundation alternatives personal until measurements are completed.

- **Protection against Eavesdropping:**

In Ekert Protocol, the presence of eavesdropper, the parties that are communicating compute the style of statistic display which is found using the concept of correlation coefficients between the sender and receiver basis. The Bell test experiments can be conducted and if the intruder has fed some disruption to the neighborhood devices then the attacker can be detected because of the violation of Bell theorem.

Security of QKD

Proofs of security are significant. We need a security proof as a genuine QKD framework is inadequate without proof because we can never make certain about how to create a safe key and how secure the last key truly is. After the qubit trade and premise compromise, Alice and Bob each have a filtered key. In a perfect world, these keys are indistinguishable. However, all things considered, there are in every case a few errors, and Alice and Bob must apply some traditional data preparing protocols, similar to error correction and security intensification to their information. The main protocol is important to acquire indistinguishable keys and the second to get a mystery key. The issue of listening is to discover protocols which, given that Alice and Bob can just quantify the QBER, either furnish Alice and Bob with an undeniably secure key or stop the protocol and illuminate the clients that the key conveyance has fizzled [6]. This is a sensitive issue at the convergence of quantum material science and data hypothesis. It contains a few spying issues, contingent upon the exact protocol, the level of admiration one concedes, the mechanical force one expects Eve has, and the accepted devotion of Alice and Bob's hardware. It is understood that a total examination of spying presently can't seem to be accomplished.

Eavesdropping attacks

- **Individual attacks:**

Eve in this attack plays out attack on every sign autonomously. The catch resend attack is a case of an individual attack. Let's assume the basic case of a block resend attack by a spy Eve, who quantifies every photon in a haphazardly picked premise and afterward resends the subsequent state to Bob. For example, if Eve plays out a rectilinear estimation, photons arranged by Alice in that diagonal bases would upset by Eve's estimation and offer arbitrary responses. At the point when Eve resends straight-lined photons to Bob, on the off chance that Bob plays out a diagonal estimation, at that point,

he will find arbitrary solutions. So because the two bases are picked arbitrarily by every gathering, such a block resend assault will generate a bit error rate which is promptly perceptible by Alice and Bob. Advanced attacks in contradiction of QKD do occur.

- **Collective**:

In Collective attacks, Eve autonomously couples to an auxiliary quantum framework, usually known as an ancilla, and advances the joined sign/ancilla unitarily. She can impart the subsequent signs to Bob, yet keep all ancilla herself. In contrast to the instance of distinct assaults, Eve delays her decision of estimation. Simply after hearing the open conversation among Alice and Bob, does Eve settle on what estimation to do on her ancilla to remove data which is related to the final key.

- **Joint**:

According to a joint attack, rather than connecting with every sign autonomously, Eve regards all the signs as a private quantum framework. She at that point merge the signed framework concerning her ancilla and develops the consolidated sign and ancilla framework unitarily [4]. She listens to the public conversation among Alice and Bob previously settling on which estimation to make on her respective ancilla. Also, the joint and collective attacks, the standard supposition that will be that Eve gauges her test simply after Alice and Bob have finished the entire public conversation about premise compromise, error correction, and security enhancement.

Some Assumptions about security in QKD:

- **Quantum Mechanics is correct**

The related assumption necessitates that any of the eavesdroppers are restricted by the laws of quantum mechanics, even though inside the domain there are no additional limitations past the eavesdropper's powerlessness to get to the devices. Specifically, we permit the eavesdropper to consume randomly huge quantum processing innovation, undeniably more remarkable than the present structure.

- **Authentication is secure**

It is considered to be a significant worry of those estimating quantum key distributions. In request to be secured against a man-in-the-middle attack, a significant part of the old-style correspondence in QKD should be authenticated. It can be accomplished with unrestricted security using short shared keys, or public-key cryptography used by computational security.

Security proof of QKD:

- **Entanglement distillation:**

Entanglement distillation also is known as entanglement purification conventions is the change of N duplicates of a subjective entangled into some number of roughly unadulterated Bell sets, utilizing just neighborhood tasks and old-style correspondence (LOCC). Quantum entanglement distillation can right now the degenerative impact of loud quantum channels [failed verification] by changing recently shared less entangled sets into fewer maximally entangled sets.

Proposed Secure System using Quantum Cryptography :

It is successfully proven that OTP is difficult and nearly impossible to break. As the OTP has flawless secrecy characteristics (i.e. perfect secrecy). It also allows the efficient ways for encryption and decryption. Encryption and decryption are carried similarly by using OTP. In OTP both Message or ciphertext bytes are XOR to the secret key bytes. Where Bytes are computed one by one and the output is as follows:

- As a key creation, QKD doesn't give independent security services all alone.
- It is subsequently significant, from incorporating QKD in security infrastructures, to figure out how QKD can be joined with other cryptographic structures.
- For symmetric key frameworks, it is shared data as a key, while in asymmetric frameworks every hub has its secret key while exchanging a synchronizing public key.
- The principle issue with the OTP is key dispersion. QKD is one way (and potentially the most encouraging) to take care of the issue of sharing a huge enough, random key to use with the OTP.

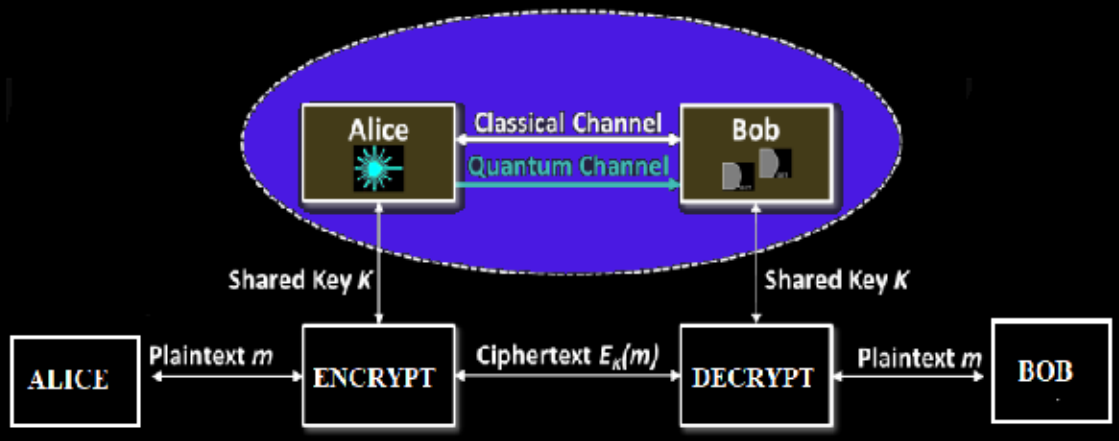

Figure 7. Proposed System

Advantage of using a one-time pad with QKD is that it can securely be reused multiple times unless the eavesdrop is recognized, and, preparing, some portion of the limit of these uncompromised broadcasts could be utilized to send new arbitrary bits along with which to replace the one-time pad when an attacker is caught.

For example, let us consider a situation where two users share a finite secret key of an insecure channel of communication to communicate privately till they can.
Whenever it is assumed that the eavesdropper is not detected then it must be assumed that communication is linear assuming P, not NP for building a secure system. Therefore, we have to show that with the use of strongly quantum coding with its communication with the help of appropriate error noticing codes, the dispatcher and the receiver can easily reuse the same JJ and KK keys indeterminately until a snoop is identified. But the security is not outright there is a small chance of eavesdropper that the entire quantum key KK can be guessed correctly. These might lead the eavesdropper on all the communication without detection and to break the reused JJ key in a usual manner as well as the is a chance of an eavesdropper to learn a few bits of the KK key and seize and decrypt a few bits of the data however these risks don't increment with the multiple times where a secure key is used again [2].
To guarantee that no keys are reused after the identification of eavesdropping the two users or parties should carefully exchange the utilization of each key else it might prompt eavesdropper a simple method to block and assimilate a message from A without sending it to B and afterward trust that B will utilize a similar key on the accompanying message. The impact of engrossing a message is along these lines equivalent to that of ruining it through eavesdropping neither one of the parties reuses the key with which it was sent.

Further, we have three types of implementable paradigms for cryptographical security:

1. **Informational:** where the attacker does not have a sufficient amount of information to decrypt the original message (or let's say a plaintext from the ciphertext).
2. **Computational Complexity:** In this case, the attacker might face a challenge where he is unable to solve the mathematical problem to derive the plaintext from the ciphertext.
3. **Quantum:** The laws of physics are hard to understand for the attacker to learn the data needed to rederive the plaintext without disturbing the system detectably.

For example, An OTP uses the “Informational ” prototype, while AES encryption uses the “Computational Complexity” prototype. Mostly all the cryptographical systems which are used nowadays rely on the “Computational Complexity” prototype. But there is one limitation or say the assumption that it might be difficult for the attacker to solve the problem and the evidence is that “many skilled and knowledgable people have tried to solve the problem and were unable to solve it ”. Whereas, Quantum crypto helps to solve this problem by relying on the laws of physics; those laws which are heavily tested and it would appear as solid reasoning than any other assumption which specifies the mathematical problem is too difficult to solve.
In any case, if we pair QKD with a symmetric cipher, correctly, we will no longer need to depend on which could be more grounded than a computational complexity presumption; if the attacker can tackle the numerical issue related with the symmetric cipher, he has broken the security. [7] But, paring QKD with a symmetric cipher provides a solution that might be worse for both worlds. There might be some implementation difficulties (not to mention the potential side-channel attacks) that we

face with quantum crypto while giving a system that is not stronger than any conventional cryptography.
On the contrary, if we do not use a symmetric cipher and instead we use exclusive-or the distributed bits with the plaintext bits (practically equivalent to what an OTP does), we can get the system which is stronger than the conventional crypto. It might be stronger in practice because of the side-channel attacks that are found on QC implementations and whether that expanded strength is worth the extensively high implementation cost which is now a different matter.

Authentication in System: The authentication can be provided using the concept of hashing. For illustration, Initially, Alice and Bob exchange the secret key (k) among them which must be long enough to validate messages sent to each other during the first QKD round. Alice sends the message m_A with its authentication tag :

$$t_A = f_k(mA),$$

where f_k is a hash function recognized by (k) to Bob. Upon receiving the message-tag pair (mA, tA). The authenticity of mA by comparing tA with a tag that is generated for the received message using f_k [5]. If they are similar, at that point Bob can be sure, that the message originated from Alice; else, he dismisses the message.

Quantum bit commitment protocol

It is about the mistrusting gatherings between the sender and receiver, Alice and Bob, which should give the accompanying usefulness:

- During a commit stage, the sender sends info a worth X (e.g bit) and the receiver get an affirmation that the sender has committed to a worth (regardless of learning the genuine estimation of X).
- Afterward, in an introductory stage, the sender can choose to disclose the worth X to the receiver.

The usefulness can be described as follows: To commit to a worth X, Say Tom composes X on a piece of paper, secures the paper in the safe, and sends the safe to Jerry while keeping the key. To open the commitment, Tom essentially sends the way to Jerry who opens the safe and peruses the estimation of X. Bit commitment is a significant cryptographic crude as it very well may be utilized as a structure obstruct for different assignments, for example, secure coin-flipping. Bit commitment can be acknowledged traditionally in a computationally secure. All the more accurately, the protocols are either computationally covering up (in which case it is just computationally secure from Alice's perspective) or computationally authoritative (computationally secure from Bob's perspective) [3]. Also, it isn't difficult to demonstrate that data hypothetically secure bit commitment protocols can't exist traditionally. Strangely, it could be demonstrated that the equivalent is valid on the off chance that we permit Alice and Bob to utilize quantum mechanics.

Quantum vs Post-quantum cryptography

Post Quantum Cryptography	QKD
Easily deployable on traditional computers and also considered to be quantum-resistant	Quantum security otherwise called quantum encryption or quantum cryptography is the act of tackling the standards of quantum mechanics to support security and to identify whether an outsider is eavesdropping on interchanges.
Guarantees mathematical complexity when compared with public-key cryptosystems	Quantum encryption exploits essential laws of physics, for example, the observer impact, which states that it is difficult to recognize the area of a substance or particle without changing that particle.
It provides security against quantum attacks and the effects of Grover's & Shor's algorithms.	It provides secure key distribution and can be used with other symmetric algorithms.
It relies on the computational assumption that requires a test of time and usually a larger key size.	Requires specific infrastructure i.e optical fibers, quantum channel, line of sight, etc.

Quantum secret sharing:

With the blast in the quantum calculation, it appears to be conceivable, even likely, that quantum states will turn out to be very significant and important. It may, in this way, be valuable to have some method for sharing secret quantum states just as secret traditional information. Likewise, quantum secret sharing may permit us to exploit the extra intensity of quantum calculation in securely conveyed calculations.

Considering the associated basic model, sharing a three-state quantum trio (a qutrit) among three individuals:

- |0> - > |000> + |111> + |222> |
- |1> - > |012> + |120> + |201>|
- |2> - > |021> + |102> + |210> |

There is no problem in what the encoded state is, any single individual is similarly liable to end up holding |0>, |1>, or |2>, so he has no data about the encoded state. Then again, any two individuals can undoubtedly recreate the secret. For example, Alice and Bob, holding shares an and b, register (b-a) mod 3. By doing this quantum precisely, they can unravel the stage also, subsequently reproducing the state, regardless of whether it is in a quantum superposition. This is along these lines a case of a ((2, 3)) quantum threshold plot: any two individuals can recreate the secret, however, one individual alone has no data. Truth be told, we can make a ((k, n)) quantum threshold

plot for any k and n, as long as n < 2k. The explanation behind this imperative is the No-Cloning Theorem, which states that it is difficult to duplicate a quantum state. On the off chance that we had a ((k, 2k)) threshold plot, we could utilize it to encode a state, take two arrangements of k offers, and use them to remake two duplicates of the first state. Since we know this is inconceivable, no such plan can exist.

Mistrustful Quantum Cryptography

In mistrustful cryptography, the two parties don't confide in one another. For instance, Alice and Bob team up to play out some calculations where the two parties enter some private data sources. Be that as it may, Alice doesn't believe Bob and Bob don't confide in Alice. Hence, secure execution of a cryptographic task requires the calculation, Alice can be ensured that Bob has not cheated and Bob can be ensured that Alice has not cheated either. Instances of errands in mistrustful cryptography are commitment techniques and secure calculations, the last including the further instances of coin flipping and unaware exchange.

Key distribution doesn't have a place with the territory of mistrustful cryptography. Mistrustful quantum cryptography contemplates the territory of mistrustful cryptography utilizing quantum frameworks. As opposed to quantum key distribution where unrestricted security can be accomplished dependent on the laws of quantum physics, on account of different undertakings in mistrustful cryptography, no-go theorems are demonstrating that it is difficult to accomplish unambiguously secure protocols dependent on the laws of quantum physics. Be that as it may, a portion of these assignments can be executed with genuine security if the protocols, not just adventure quantum mechanics yet also unique relativity. By the examination, there cannot be genuinely secure quantum protocols for one-out-of-two unmindful exchange and other secure two-party calculations. Nonetheless, unequivocally secure protocols for coin flipping and bit-commitment.

- **Quantum Coin Flipping**

Quantum coin flipping is kind of a protocol that is utilized between the two parties, who cannot trust each other. Both parties are then required to communicate with each other through a quantum channel and share the information by transferring qubits. It is one of the protocols that is considered to be a secured means of communication between the two distrustful participants but it is very challenging to accomplish this physically.

- **Quantum Commitment**

Quantum Commitment protocols are used when there is an exchange of information between the distrustful participants. This technique let the one-party i.e Alice set a certain value (commit) in a way where Alice is not allowed to make any modifications in the value while also at the same time making sure that the receiver i.e Bob is not able to learn any information regarding that specific value until and unless Alice discloses it.

Conclusion

Unlike any computational encryption, quantum cryptography utilizes the principles of quantum mechanics to encode information and hence making it practically invulnerable. In Quantum Cryptography, a sequence of photons is used to transfer the messages from one entity to another over a fiber-optic channel. The message is sent in such a way over a fiber optic cable that enables the endpoints to evaluate the properties of the photons in which data is being transmitted and then a key is being extracted to decrypt the message. Also, QKD doesn't give independent security services all alone. [8] It requires OTP which has flawless secrecy characteristics (i.e. perfect secrecy). Also, the Advantage of using a one-time pad with QKD is that the key can securely be reused multiple times unless the eavesdropper is recognized. The below graph shows the different QKD schemes and how the distance affects the Bitrate:

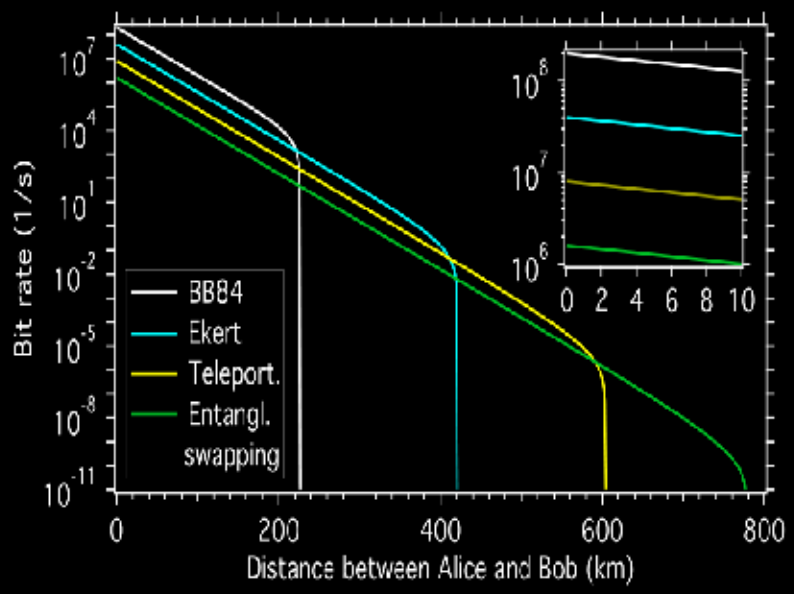

Figure 8. Bit rate vs Distance in QKD [3]

The introduction to quantum cryptography can lower the chances of altering the message, hence retaining the contents' original state. Thus, Quantum Cryptography via the QKD provides the best-fit solutions in protecting the data when sent to over an unreliable channel and this solution will last long in the coming future too.

Future Scope

In the future, Another possible choice is to use the other symmetric encryption technique for the messages and later use the QKD for the key's distribution only. Secondly, Another solution could be expected to be a blend of post-quantum algorithms like lattice-based encryption for the initial step of communication to safely trade keys. Later then utilizing symmetric encryption for the most significant messages.

While current QKD progression requires a photon to be directly transmitted and that the limitation will not last forever.

Shortly, QKD could benefit from quantum entanglement. Also with the post-quantum gaining importance, it can be possible to use public-key algorithms and build a more secure system. Like for instance, the lattice-based post-quantum technique is gaining popularity Post-quantum cryptography refers to cryptographic algorithms (usually public-key algorithms) which are secure from quantum computers.

References

[1] C. Elliott, "Quantum cryptography," in IEEE Security & Privacy, vol. 2, no. 4, pp. 57-61, July-Aug. 2004.Kruse, W., and Heiser, J. Computer Forensics: Incident Response Essentials. Addison-Wesley, Boston, 2002.

[2] V. Padamvathi, B. V. Vardhan and A. V. N. Krishna, "Quantum Cryptography and Quantum Key Distribution Protocols: A Survey," 2016 IEEE 6th International Conference on Advanced Computing (IACC), Bhimavaram, 2016, pp. 556-562.

[3] M. Moizuddin, J. Winston and M. Qayyum, "A comprehensive survey: Quantum cryptography," 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), Abha, 2017, pp. 98-102.

[4] 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.

[5] V. L. Kurochkin and I. G. Neizvestny, "Quantum cryptography," 2009 International Conference and Seminar on Micro/Nanotechnologies and Electron Devices, Novosibirsk,2009, pp. 166-170.

[6] C. Chen, G. Zeng, F. Lin, Y. Chou and H. Chao, "Quantum cryptography and its applications over the internet," in IEEE Network, vol. 29, no. 5, pp. 64-69, September-October 2015.

[7] L. Kai, L. Yuanyuan, H. Kehai, and H. Xiao-Ying, "A Quantum Secret Sharing Scheme with High Efficiency Based on the Bell States," 2012 Fourth International Symposium on Information Science and Engineering, Shanghai, 2012, pp. 418-421.

[8] H. M. Elkamchochi, R. A. Elattar, and A. H. Abd-Elhamied, "A New Symmetric Key Quantum Cryptographic Algorithm," 2007 National Radio Science Conference, Cairo, 2007, pp. 1-13.