Department of Electrical & Computer Engineering
North South University

CSE499B.02: Senior Design Project
Fall-2022

Secure The Quantum Communication using-BB84 and E91 Protocol BB84 (X, Z Basis), E91 (CHSH)

Submitted by:

Team Members	ID Number
MD. Romzan Ali	1912718042
Seaum Ibn Zaman	1811663042
Sadia Sharmin Swarna	1912986042
MD. Sakib Bin Swroar	1612367042

Submitted to:

Dr. Mahdy Rahman Chowdhury
Associate Professor
Department of Electrical and Computer Engineering
North South University

Declaration

It is hereby acknowledged that:

- No illegitimate procedure has been practiced during the preparation of this document.
- This document does not contain any previously published material without proper citation.
- This document represents our own accomplishment while being Undergraduate Studentsin the North South University

Sincerely,

MD. Romzan Ali	1912718042	
Seaum Ibn Zaman	1811663042	
Sadia Sharmin Swarna	1912986042	
MD. Sakib Bin Swroar	1612367042	

Approval

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope andquality as a dissertation.

……

Supervisor's Signature

Dr. Mahdy Rahman Chowdhury

Associate Professor

Department of Electrical and Computer Engineering

North South University

Dhaka, Bangladesh.

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope andquality as a dissertation.

……

Dr. Rajesh Palit

Professor & Chair

Department of Electrical and Computer Engineering

North South University.

Dhaka, Bangladesh.

Acknowledgment

Firstly, we are grateful to Allah for showering His blessings on us for being able to complete our senior design project on time.

Secondly, we are heartily thankful to our supervisor and mentor, Dr. Mahdy Rahman Chowdhurysir whose encouragement, motivation, and support from the initial and to the final level enabled us to develop a deeper understanding of quantum computing which has facilitated us in completingour quantum computing project within the limited time frame. In addition, his guidance and mentorship helped us in doing a lot of research. As a result, we have learned so many novel thingsabout quantum computing and so we are truly grateful to him. We would also like to express our special thanks to our research assistant, Syed Imad Uddin Shuvo who helped us in completing thisproject on time.

Lastly, we offer our felicitations to our parents, friends, and all our well-wishers for supporting and encouraging us in every way to successfully and timely complete our project.

MD. Romzan Ali
Seaum Ibn Zaman
Sadia Sharmin Swarna
MD. Sakib Bin Swroar

Abstract

A cryptographic solution that is impenetrable is generated by quantum cryptography because it strengthens the prime secrecy used in the distribution of quantum public key distribution. It is a well-known technology that uses the principles of quantum physics to enable safe communication between two entities. This research performs an analysis of BB84 and E91 Quantum Cryptography Security Protocols. Eavesdropping and noise are the main causes of bit error in quantum communication. However, the majority of quantum communication protocols only consider eavesdropping and overlook the impact of noise, leading to inaccuracies in eavesdropper detection. An effective noise analysis model is put out to examine the security of the quantum E91 protocol that Eckert introduced in the collective-rotation noise channel. Eavesdropping is detected using the qubit error rate increment. According to our investigation, when the noise level is roughly 2, the eavesdropper (Eve) can only obtain about 50% of the key from the connection. The findings demonstrate that the E91 protocol is secure in a collective-rotation noise environment and that the raw key is accessible, as we already knew and had demonstrated. A random encryption key was intended to be distributed using correlated polarization states of individual photons by (BB84**).** The no-cloning theorem which asserted that the polarization state of a single quantum system cannot be perfectly duplicated, was the source of its efficacy. Additionally, it was intimated that any attempt to duplicate the polarization condition would result in its modification or destruction. Errors in the anticipated correlation of the polarization states are the result of a measurement attempt on the distributed key. Such errors are identical to errors brought on by positively de-coherence. BB84 views any noise as proof of an eavesdropper. In reality, all distributed keys will initially have some noise, so traditional communication must be used to obliterate any information that an eavesdropper would have. It can be concluded that the E91 protocol is secure in the real noise environment, and Eve can only get parts of incomplete key, meaning that she cannot read the secret message in the quantum channel.

Keywords: Quantum cryptography, CHSH inequality, E91, BB84, Polarization, Quantum key distribution.

Table of Contents

1. Introduction:

The backbone of information security is cryptography, whose task it is to make sure that only authorized users like Alice and Bob can read the secure communication's secret message and that unauthorized users like Eve cannot. Without the key, it is impossible to decipher the secret message created through cryptography. The first QKD protocol, often known as the BB84 protocol, was introduced in 1984 by CH Bennett and Brassard. The BB84 protocol is simple to implement and avoids requiring quantum entangled states and retaining quantum particles by using four quantum single particle states. Later in 1991, Ekert proposed the E91 protocol, which is known as the QKD implementation employing the quantum entangled states investigated in the Einstein-Podolsky-Rosen (EPR) thought experiment.

The E91 protocol uses an EPR pair throughout the transmission, which separates the EPR pair and sends one particle to Alice and Bob individually, in contrast to the BB84 protocol in which Alice delivers quantum particles to Bob. EPR is tough to keep entangled, as we all know.

In the other words the E91 protocol requires more effort to implement than the BB84 protocol. However, a central source uses the E91 protocol to send one EPR particle to each of Alice and Bob. This resembles the structure of the traditional cryptography protocol. Since its release, the E91 has drawn a lot of interest. However, those techniques and assessments primarily consider eavesdropping and ignore the impact of noise, which cannot be ignored in actual practice. We must consider the noise in order to apply in the real world.

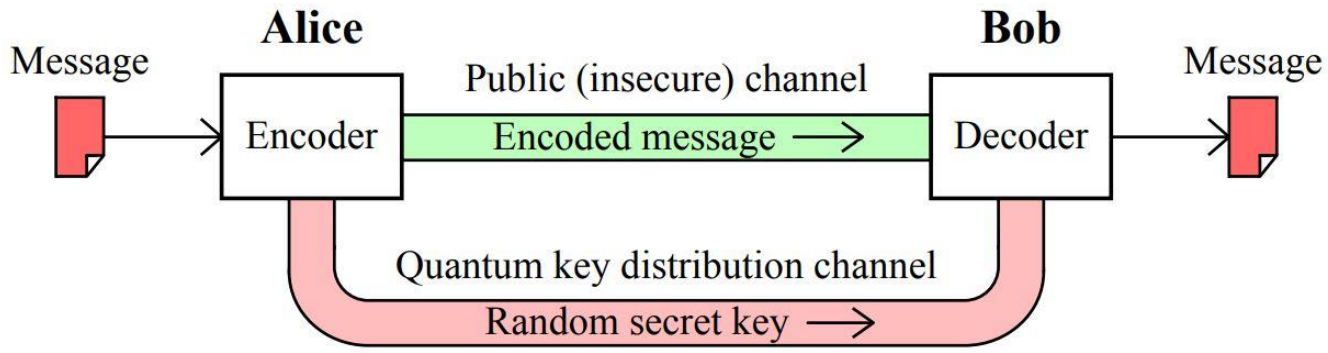
Despite the fact that BB84 and E91 use different quantum mechanical concepts, it is possible to evaluate the security of their distributed key by considering just on the relevant error percentage. Both protocols were seen as being equivalent because of this. However, the E91 protocol is secure in a noisy environment.[1]

2. Scenario of Quantum Cryptography:

Currently, communication is conducted using classical bits, allowing only classical cryptography to provide security. The two main areas of classical cryptography are public key cryptography, commonly referred to as asymmetric cryptography, and secret or symmetric key cryptography.[5]

The earliest type of cryptography is secret key cryptography, in which two parties share a secret key to both encrypt and decrypt their communications. While some secret key schemes, like one-time pads, are completely secure against an attacker with arbitrary computational capacity, they have the significant practical drawback of requiring two parties to first create a secret key in order to interact securely.[6]

Public key cryptography-based key distribution algorithms, like Diffie-Hellman, are frequently used to establish a secret key via an insecure channel. Public key cryptography does not require the establishment of a shared secret key before communication, in contrast to secret key cryptography.Instead, each party has a public key that may be shared freely and a private key that is kept hidden. If, for example, Alice wants to send a message to Bob, only Bob can decode the message using his private key because only Bob has access to Bob's public key. The security of public key cryptography methods is currently reliant on the unproven assumption of the complexity of some problems, such as integer factorization or the discrete logarithm problem, despite the fact that key exchange is not required.[1]



3. Overview of BB84 Protocol:

Proposed in 1984 by Bennett and Brassard — that's where the name comes from by the way, the idea is to encode every bit of the secret key into the polarization state of a single photon. A single photon's polarization state cannot be determined without destroying it, making this information "fragile" and inaccessible to the user. The photon must be detected by any listener (referred to as Eve), at which point she must either expose herself or send the photon again. But eventually, she will send a photon with the incorrect polarization state. Errors will result from this, and the eavesdropper will once more come to light.[2]

- Alice transmits a series of signals, each of which should include a single photon with a unique polarization.
- Alice encodes units into V-polarized photons while encoding zeros into H-polarized (horizontally) photons (vertically)
- But just 50% of the time does this occur. An arbitrary selection of the other half of the bits is encoded using a diagonal polarization basis. Then, "D" polarization equals zero and "A" polarization equals unity.

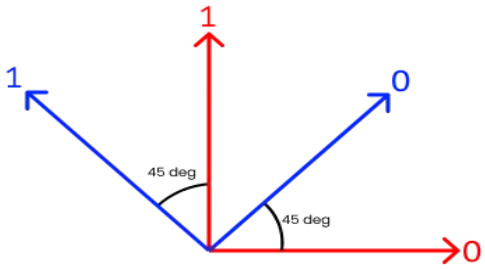


Fig.: Representation of photon polarization for BB84 protocol.

- Bob, the receiver, uses a standard setup to measure the polarization. If Bob employs the HV basis (further designated as "+"), he can discriminate between the H and V polarizations. But in 50% of the situations, Bob at random switches to AD (abbreviated as "X").
- Bob publicly declares the basis he used for each bit after a predetermined amount of bits have been transmitted (and all photons have been detected and destroyed!). Alice then reveals which instances they shared a base in. They discard the pieces where they used

many bases and save only the pieces where they used just one.[2]

- The length of the key is shortened twice as a result of this process (key sifting), but what is left is random and coincides for Alice and Bob.
- Then they look to see whether anyone was listening in. To do this, they compare a small portion of the key, like 10%. The 10% are then ignored, but this process is also open to the public. The key would be flawed if the eavesdropping occurred. The process is then carried out once more after discarding the entire key.
- An example of communicating 8 bits of a secret key is shown in the table below. There are just 4 bits remaining after key filtering.

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	X	+	+	+	X	+	X	X
Photon polarization Alice sends	D	V	V	H	A	H	D	A
Bob's random measuring basis	X	X	+	X	+	+	+	X
Photon polarization Bob measures	D	D	V	A	V	H	V	A
Shared secret Key	0		1			0		1

4. Heisenberg Uncertainty Principle on BB84 Protocol:

The security of quantum cryptography rests on several principles from quantum physics. The Heisenberg Uncertainty Principle (HUP), which asserts that in a quantum system, only one property of a pair of conjugate properties can be known with certainty, is the most fundamental of these principles. Heisenberg explained how any measurement of a particle's position could disrupt its conjugate property, its momentum. He was initially referring to the position and momentum of a particle. Therefore, it is impossible to know both attributes simultaneously and

with certainty. This idea can be used in quantum cryptography, however typically the conjugate qualities are determined by the polarization of photons on separate bases. This is because photons, which are probably the most practical quantum systems for communication between two parties wanting to perform key exchange, can be exchanged across fiber optic networks. BB84 is based on 'uncertainty principle' which states that unlike digital data, the quantum.

data cannot be copied or measured without disturbing it. Therefore, it would be difficult for the eavesdropper to establish both properties of the photon, making it impossible for him to send a precise duplicate value. Meanwhile it is impossible to perform an experiment on two components of the system that would violate the uncertainty principle as long as the two particles are entangled. We have a 100% chance of gaining the value of measuring with X basis if we encode with X basis and generate qubits; if we measure with Z basis, we have a 50% chance of <1| state and 50% chance of <0| state. When we create a qubit with only one basis, it has a 100% chance of gaining the same state.[4]

5. Overview of E91 Protocol:

Artur Ekert developed the first entanglement-based protocol in 1991 (E91). Ekert tested if Alice and Bob's shared state was (almost) maximally entangled by violating Bell's inequalities. E91 utilized the non-locality as a resource for QKD for the first time. It has the potential to offer supra-quantum security and can be utilized for device-independent cryptography. Bob and Alice share |Φ+> states (generated from an unknown sender). To violate CHSH, each of them must measure randomly in one of three bases. Different things happen when estimating the raw key and parameters. Nonlocality is the foundation of security. In this procedure, Eckert employed a single photon source that generates entangled photons. From each entangled pair, one photon goes to Alice and the other to Bob. Bob and Alice choose bases to measure the photons at random. In cases when they choose the same basis for each measurement, they will have correlated findings. They will have a bit-string binary that is correlated to one another once the photons that were measured using various bases have been removed. Alice and Bob can change their key to the shifted key by determining whether the entangled states were inversely or directly related to one

another. With the results of their third basis measurement of a photon, they can test Bell's Inequality to determine whether Eve is present. Someone might have eavesdropped on the quantum channel if the inequality contains. The two categories of quantum key distribution (QKD) algorithms are prepared and measure (P&M) and entanglement-based (EB). Distributing information-theoretically secure keys among two remote nodes is the same goal. To ensure the security of the algorithm, they are founded on many physical justifications.

Entanglement is the basis of Ekert's protocol. It is intended to base security on the so-called monogamy of entanglement, which states that if two particles (i.e., qubits) are entangled, they will not be entangled to any external system.[3]

6.Bell's Theorem and CHSH Inequality on E91 Protocol:

Bell's theorem was applied for the first time in Ekert's groundbreaking study to uncover the eavesdropping. Ekert proposed using Bell's theorem to identify the presence of eve in quantum communication, despite the fact that it was developed with the EPR conundrum in mind for the detection of local hidden variables.[4]

According to Bell's theorem, "There are quantum mechanical predictions that are incompatible with those of local hidden variable theories. Local hidden variable theories [LHVT], which are hypothetical physical theories based on the EPR assumptions of local causation and physical reality, were mathematically described by Bell by violating some inequalities (Bell inequalities), which are satisfied by LHVT. Bell's approach enables us to test these requirements empirically. The CHSH inequality is the most widely used experiment to test Bell's inequality, despite the fact that several others have been offered.[7]

The Clauser Horne Shimony Holt (CHSH) inequality is the violation of bell inequality and exceeds a certain value for entangled states due to the quantum mechanics which proves there is no hidden variable. This theory and experiment were awarded the Noble Prize in Physics in 2022. This is the first experimental proof that nonlocal quantum entanglement is real. [5]

7. No-cloning Theorem & Quantum Non-locality:

The No Cloning Theorem, which limits cloning of quantum state, is the key distinction between classical and quantum theory. According to the no-cloning theorem, it is impossible to duplicate a quantum state exactly with any nonzero probability value.

Super positions:

In quantum physics, a particle can be in multiple states at once because of the superposition of all of its potential states.

|A>=|A>+|A>

Transformations distribute.

Any change to a particle that in superposition of a state affects all of the states independently.

T (|A1>+|A2>) = T(|A>) +T(|A>)

It asserts that there are some non-local correlations and that they adhere to the relativistic causality principle. Quantum entanglement is a common example of such non-local correlation.[2]

8.Quantum Teleportation:

Quantum states are highly unstable, if they interact or collide with any other systems then it will lead in either losing their superposition properties or even destroying. When compared to quantum bits, classical bits can more easily fix errors if they do exist. The goal of quantum teleportation is to transmit information through a secure environment while using unknowable quantum states. If this application becomes a reality in the future, we will be able to teleport computer outputs so that they can be used as inputs (Spiller 1996). The quantum entanglement feature is used in teleportation. It facilitates the transmission of information from one location to another.[2]

For clarity of its use, we'll refer to the sender and recipient as Alice and Bob. Alice prepares an EPR pair (particles A, B), as well as particle C, which carries the information that has to be conveyed, throughout the preparation process. The outcome of Alice's subsequent joint

measurement—also referred to as a Bell measurement—with particles A and C is utilized to transfer. The quantum mechanics no-cloning principle is not violated by the procedure because the state of particle C is altered. After receiving the results of the Bell measurement from Alice using the conventional protocol, Bob can use his particle B to perform the unitary transformation on the results to get the state of particle A and the data stored in particle C. It requires certain elements, such as the Bell measurement and unitary transmission, but when other configurations are used, the method for achieving teleportation can differ.[4]

9.Quantum Channels:

For long distances, photon-based qubits and optical networks are used for quantum network communication. Broadband is supported via optical networks. Over an optical fiber link, quantum bits can be reliably and quickly transmitted.[5]

- **Fiber Optic Networks:**

Modern telecommunications technology can be used to develop and execute optical networks. An original photon source can be created at the transmitter by tightly attenuating a conventional telecommunication laser until the average number of photons per pulse is less than 1. A photo avalanche detector may be present on the receiver. Beam splitters and interferometers are used to regulate the phase and polarization of the light. Through constant parametric down conversion of entanglement-based protocols, entangled photons are produced.

- **Free Space Networks:**

Free space quantum networks are the foundation of fiber optic networks, however they rely on line of sight for communication. In comparison to fiber optic networks, free space networks offer greater bandwidth and faster data rates, and they do not suffer from polarization scrambling.

10. Quantum Entanglement:

The other important principle on which QKD can be based is the principle of quantum entanglement.

When a certain attribute of one particle is measured, the opposite state of the entangled particle will be seen instantly. This is possible when two particles interact. No matter how far apart the entangled particles are, this is true. However, it is impossible to know in advance what state will be observed, making communication via entangled particles impossible without discussing the observation over a classical channel. Eckert's protocol is based on quantum teleportation, which involves the exchange of information using entangled states and a classical information channel.[5]

11. Quantum Key Distribution (QKD):

Quantum Key Distribution (QKD) is a far more secure system than conventional cryptography systems since the information integrity is based on quantum mechanical principles rather than the computational complexity of the cryptographic algorithm. It functions by allowing two participants to securely share a secret key without any information being revealed to any eavesdropper. Once the key is shared and known by both parties, the transmitting side can begin encrypting messages with the shared key and broadcasting them while the receiving side decrypts the message using the key that is only known to them. The key is encoded as conjugate bases of a quantum state (or qubits) and communicated across a quantum channel, which is the distinguishing and essential feature of QKD. A quantum state cannot be simultaneously measured in two orthonormal bases, according to the principles of quantum physics. A random result is therefore noticed by the interceptor in any effort to intercept the quantum channel and measure a qubit because doing so destroys the qubit's quantum state. The destroyed qubit also alerts the receiver to an attempted interception. QKD is a very secure method for sharing key information because of these features.

In 1984, Bennet and Brassard presented the first secure QKD protocol, which was given the initials BB84 in their honor. Key information was transmitted using photon polarization states through a quantum channel in conjunction with an unreliable public channel. Non-orthogonal quantum states, or polarization orientations of 0, 45, 90, and 135 degrees in the case of photons, are used to encode the key information. Here is a description of how the protocol functions using an example. The transmitter ‘Alice’ encodes each bit on one of two polarization bases, i.e.,

Rectilinear R, or Diagonal D, and uses either one pair, i.e., (0, 90) or (45, 135), of polarization states/directions to encode each bit. The receiver ‘Bob’ can use either one of the two polarization bases to measure the received photon and recover the bit, hence Bob has a 50% chance to recover the correct bits. After all photons are measured by Bob, both Alice and Bob communicate over a public channel, with Alice sending the basis of each photon she had sent and Bob sending the basis of all his measurements. They eliminate the measurement bits whose basis did not match and create a key with the remaining number of bits. To detect the presence of an eavesdropper, Bob and Alice can agree upon a pre-shared subset of the key bits, e.g., one third, and match that with their measured bits. If no errors are detected, then they commence encryption of their data with the shared key and can securely transmit over the classical channel.[6]

Basis	**0**	**1**
R	90	0
D	45	135

Quantum Transmission												
1. Alice prepares string of bits for transmission	1	0	0	1	0	0	1	1	0	1	0	0
2. Alice encodes each bit with random basis	D	R	D	R	R	R	R	R	D	D	R	D
3. Alice prepares photon polarization state/direction	135	90	45	0	90	90	0	0	45	135	90	45
4. Bob measures photon with random basis	R	D	D	R	R	D	D	R	D	R	D	D
5. Bits recovered by Bob (using random direction)	1	0	0	1	0	0	0	1	0	1	1	0
Public discussion of basis												
6. Bob sends measurement basis	R	D	D	R	R	D	D	R	D	R	D	D

7.Alice acknowledges correct bases			Ok	Ok	Ok			Ok	Ok			Ok
8. Shared information			0	1	0			1	0			0
9. Bob sends random key bits			0					1				
10. Alice confirms random key bits			Ok					Ok				
Outcome												
11. Secret key formed from remaining bits				1	0				0			0

Figure: BB84 protocol using two non-orthogonal bases and four polarization directions.

Polarization state (Bloch sphere):

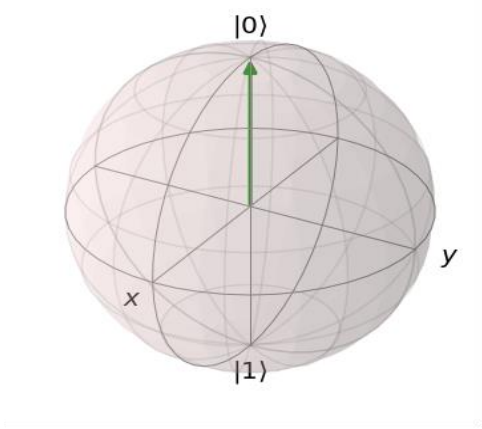


Figure: Photon_h (horizontally polarized photon (90 degree))

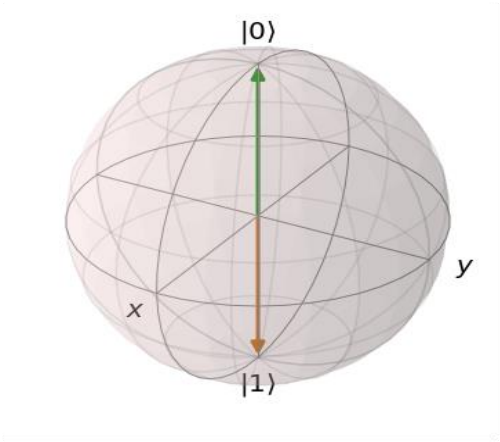


Figure: Photon_ v (vertically polarized photon (0 degree))

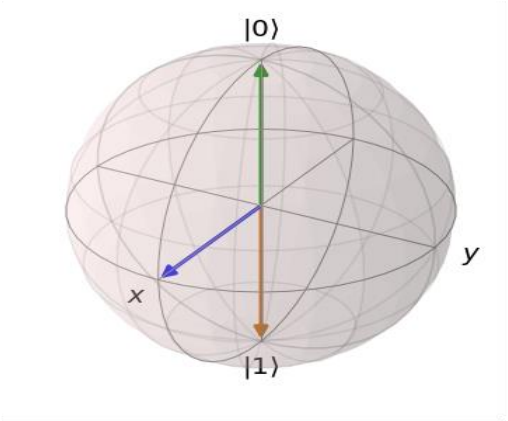
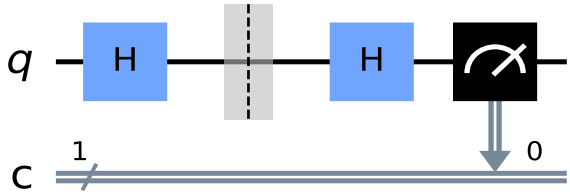


Figure: Photon_d45(diagonally polarized photon (45 degree))

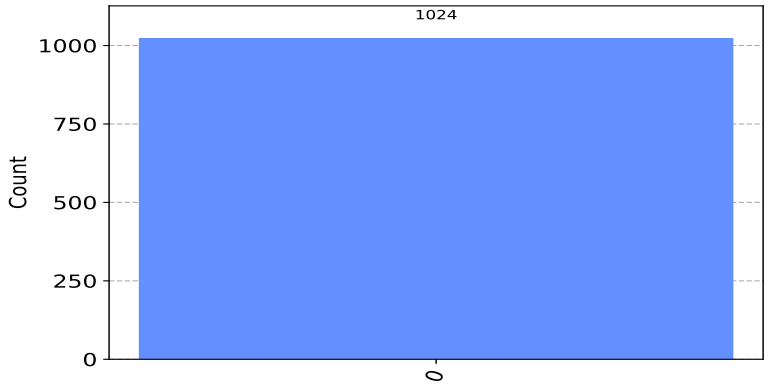
12. Quantum Key Distribution protocol using QISKIT:

Qubit state changes are detected by QKD. The qubit's state will probably change if Alice gives a qubit to Bob and Eve attempts to measure it before Bob.

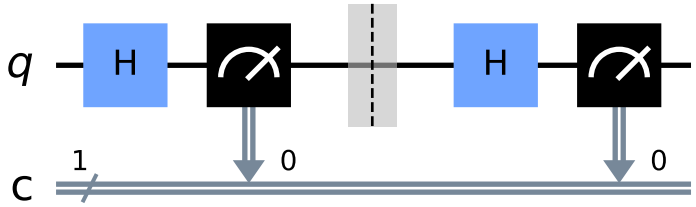
When Bob measures a qubit in the X-basis after Alice has prepared it in the state |+⟩ (0 in the X-basis), Bob will undoubtedly obtain a value of 0.

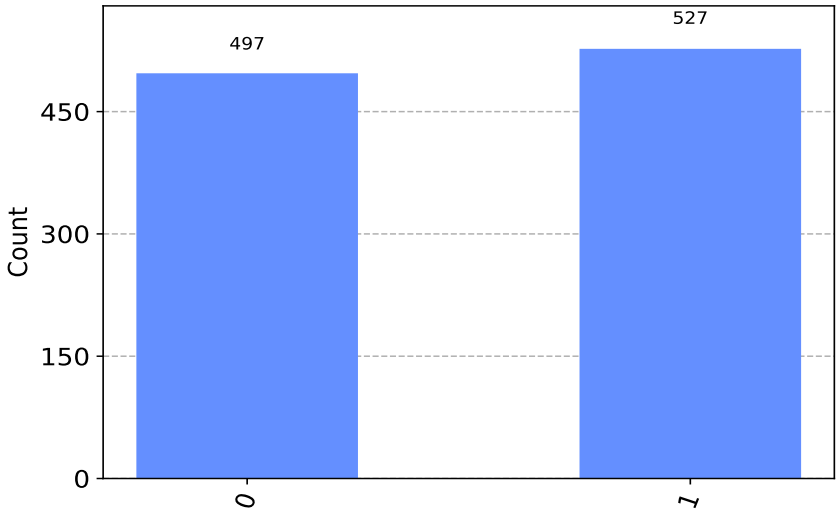


Here, in the first case, Alice sends Bob a qubit that measures along the X axis.



However, if Eve attempts to take a measurement of this qubit in the Z-basis before it reaches Bob, she will modify the qubit's state from |+⟩ to either |0⟩ or|1⟩, and Bob will no longer be assured to take a measurement of 0.





Here, we can see that Bob now has a 50% probability of measuring 1, and if he does, he and Alice will be aware that their channel isn't working properly.[5]

Step-by-step process:

Step-1

If Alice prepares a qubit in the state |+⟩ in the X-basis, it corresponds to a 0 in the X-basis. When Bob measures the qubit in the X-basis, he will be certain to measure a 0. This is because the state |+⟩ in the X-basis is an eigenstate of the X-basis measurement operator, meaning that when measured in the X-basis, the qubit will collapse to the state |+⟩ with probability 1.

It's important to note that if Bob measures the qubit in a different basis, such as the Z-basis, the outcome will be uncertain, and the result will be random. In this case, if Bob measures it in the Z-basis, he will obtain |+⟩ with probability 1/2 and |-⟩ with probability 1/2, this is due to the qubit is in superposition state, which means the qubit exist in both state |+⟩ and |-⟩.

Alice chooses a string of random bits, e.g.:

1000101011010100

And a random choice of basis for each bit:

ZZXZXXXZXZXXXXXX

Alice keeps these two pieces of information private to herself.

Step-2

If Eve attempts to measure the qubit in the Z-basis before it reaches Bob, she will disturb the state of the qubit and change it from |+⟩ to either |0⟩ or |1⟩. This is known as the "measurement problem"

in quantum mechanics. When Bob measures the qubit in the X-basis, he will no longer be certain to measure a 0, as the state of the qubit has been changed by Eve's measurement.

This is one of the key security features of QKD and BB84 protocol, as any attempt to intercept the qubit will be detectable. In the BB84 protocol, Alice and Bob can detect the presence of an eavesdropper by comparing a small portion of their key and checking for discrepancies. If there are discrepancies, it indicates that an eavesdropper has attempted to intercept the qubit and the key is discarded.

It's important to note that, Eve can't perfectly copy the state of qubit, as per the no-cloning theorem, which states that it is not possible to make an exact copy of an arbitrary unknown quantum state.

Alice then encodes each bit onto a string of qubits using the basis she chose; this means each qubit is in one of the states $|0\rangle$, $|1\rangle$, $|+\rangle$ or $|-\rangle$, chosen at random. In this case, the string of qubits would look like this:

$|1\rangle|0\rangle|+\rangle|0\rangle|-\rangle|+\rangle|-\rangle|0\rangle|-\rangle|1\rangle|+\rangle|-\rangle|+\rangle|-\rangle|+\rangle|+\rangle$

This is the message she sends to Bob.

Step -3.

We can see here that Bob now has a 50% chance of measuring 1, and if he does, he and Alice will know there is something wrong with their channel.

The quantum key distribution protocol involves repeating this process enough times that an eavesdropper has a negligible chance of getting away with this interception. It is roughly as follows:

Bob then measures each qubit at random, for example, he might use the bases:

XZZZXZXZXZXZZZXZ

And Bob keeps the measurement results private.

Step 4

Bob and Alice then publicly share which basis they used for each qubit. If Bob measured a qubit in the same basis Alice prepared it in, they use this to form part of their shared secret key, otherwise they discard the information for that bit.

Step 5

Finally, Bob and Alice share a random sample of their keys, and if the samples match, they can be sure (to a small margin of error) that their transmission is successful.

13. Pros and Cons of QKD:

Quantum key distribution is a one of the techniques used for exchanging keys between two users. Security is the main benefit of quantum communication. Quantum information protected by quantum cryptography is impenetrable due to the fact that any modification made to one particle of an entangled pair is immediately reciprocated by the other. The no cloning and no destroying theorem is another factor in this. Therefore, the information cannot be changed or destroyed. Quantum communication is slower over greater distances. Therefore, traditional communication is currently quicker and capable of spreading over the entire world. Longer distance quantum communication may be conceivable with satellite based QKD, but this hasn't been tested yet. A classical and quantum network must coexist side by side in order to convey quantum information securely, which necessitates some level of classical communication.

Despite these benefits, we currently lack the technology necessary to construct a quantum

computer. This is because the coherent state, which is essential to a quantum computer's operation, is destroyed the moment it is measurably impacted by its surroundings. Although efforts to address this issue have not been particularly effective, the search for a workable solution continues.

When compared to traditional cryptographic methods, QKD is superior in the following ways:

- Two quantum mechanical principles can be used to detect Eve's attempts to collect information.
- Because the error level is higher in this scenario, the quantum key distribution mechanism can detect eavesdropping.
- It is possible to identify the mistakes made when users communicate with one another.

- Since QKD continuously and randomly produces new private keys, it is nearly impossible to steal any key distributed using quantum cryptography.
- The QKD protocol improves data security.
- The actual information can never be revealed to any third party.
- Quantum physics' demonstrable laws are the foundation of QKD security.
- When it comes to security, QKD sounds too nice, but when it comes to practical factors, it takes a back seat. There are some implementation-related technical flaws.
- The QKD's limited range of a few hundred kilometers makes long distance transmission impractical, and quantum repeaters have little real-world use.

14. Quantum Networking and Quantum Internet:

The main goal of the quantum internet is the exchange of qubits. Qubits, which are represented by photons, may be transferred via one of three basic methods: fiber-optic cables, electromagnetic waves that pass through the atmosphere, or satellites in orbit. A clear line of sight must exist between the devices for an open-air transmission, even though it is the least expensive option. Even though the fiber-optic method makes use of a commonly utilized networking technology, qubit states quickly deteriorate with increased transmission distance, resulting in unexpected

transfers. One advantage of satellites for long-distance transmission is less interference in orbit. However, the satellite constellation's launch and maintenance are highly expensive.[1]

The quantum internet also requires the capability to send conventional bits. For instance, in quantum teleportation, a transferred qubit may be accurately recovered with just the transfer of two classical bits. Fortunately, the fiber-optic cables used to transmit qubits may also be used to transfer classical bits, regardless of whether the equipment on either end quantum is obviously or classical. This means that a significant chunk of the current internet's infrastructure can be moved to the next quantum internet.[5]

15. BB84 Protocol Explained:

The BB84 protocol is a quantum key distribution protocol that allows two parties, Alice and Bob, to establish a shared secret key that can be used for encrypting and decrypting messages.

In the BB84 protocol, Alice generates a string of random bits, representing the key, and encodes them into qubits by preparing them in one of two bases (X or Z) and one of two states ($|0\rangle$ or $|1\rangle$) corresponding to the bit value. She then sends the qubits to Bob who measures them in one of the bases he chooses randomly.

After the transmission of a large number of qubits, Alice and Bob publicly announce the bases they used for their measurements. They then keep only the results obtained using the same bases and discard the rest. These remaining results from the raw key.

Alice and Bob then use a technique called error correction and privacy amplification to extract a secure and secret key from the raw key. Error correction is used to correct any errors that may have occurred during the transmission, while privacy amplification is used to ensure that any information obtained by an eavesdropper is insignificant.

In the case of an eavesdropper, Eve, attempting to intercept the qubits, the disturbance caused by her measurements will be detected by Alice and Bob during the error correction and privacy amplification step, allowing them to discard the intercepted key and generate a new one.

It is important to note that, the pseudorandom key generation method you mentioned is not related to the BB84 protocol, it could be used for any other application.[7]

Step 1:

Alice generates her random set of bits:

The set of bits 'alice_bits' is initially only known to Alice. As she encodes them into qubits, it is then sent over to Bob. Bob then measures the qubits and records the measurement results, which is now only known to Bob. Any information that has been sent over Eve's channel, such as intercepted qubits, is also recorded in the table.

This table can be used to keep track of the information shared between the parties and to detect any eavesdropping attempts by Eve. By comparing the information known only to Alice and Bob, they can detect any discrepancies that may have been caused by Eve's measurements.

It's important to note that the protocol is secure only if the qubits are sent over a quantum channel, Eve can't intercept the qubits without being detected. If the qubits are sent over a classical channel, Eve can intercept the qubits and obtain a copy of the key without being detected.

Alice's Knowledge	Over Eve's Channel	Bob's Knowledge
alice_bits		

Step2:

Alice encodes each bit of the key on a qubit in either the X-basis or Z-basis at random. She then stores the choice of basis for each qubit in the variable 'alice_bases'.

The bit 'alice_bases' is used to keep track of which basis Alice used to encode each qubit. By using a random choice of basis for each qubit, it makes it more difficult for an eavesdropper, Eve, to intercept the qubits without being detected.

The encoding of the bit in the Z-basis or X-basis is done according to the value of the bit, if the bit is 0 then the qubit is encoded in the Z-basis and if the bit is 1 then the qubit is encoded in the X-basis.

After We can see that the first bit in alices_bits is 0, and the basis she encodes this in is the X -basis (represented by 1).

And if we view the first circuit in message (representing the first qubit in Alice's message), we can verify that Alice has prepared a qubit in the state |+⟩, and we can see that the fourth bit in alice_bits is 1, and it is encoded in the Z -basis, Alice prepares the corresponding qubit in the state |1⟩.

Alice generates two n-bit strings:

$$a = a_1 a_2 \dots \dots a_n$$

$$b = b_1 b_2 \dots \dots \quad b_n$$

Alice creates a quantum state according to these bit strings.

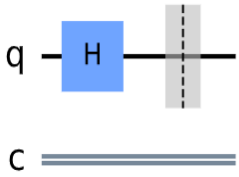
Alice's encoding:

	z-basis	***x-basis***	
$\|\psi\rangle=\bigotimes_{k=1}^{n}\|\psi_{a_k b_k}\rangle$	$\|\psi_{00}\rangle=\|0\rangle$	$\|\psi_{01}\rangle=\|+\rangle$	b_k=0; Z-basis
	$\|\psi_{10}\rangle=\|1\rangle$	$\|\psi_{11}\rangle=\|-\rangle$	b_k=1; X-basis

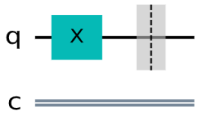
Alice's encode with basis and generate qubits.

	z-basis	***x-basis***
$\|\psi\rangle=\bigotimes_{k=1}^{n}\|\psi_{a_k b_k}\rangle$	$\|\psi_{00}\rangle=\|0\rangle$	$\|\psi_{01}\rangle=\|+\rangle$
	$\|\psi_{10}\rangle=\|1\rangle$	$\|\psi_{11}\rangle=\|-\rangle$

String a		**0**	**1**	**1**	**0**	**1**
String b		**1**	**1**	**0**	**0**	**1**
Basis		**X**	**X**	**Z**	**Z**	**X**
Encoded qubits		$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$



Alice has encoded qubit in the X-basis.



Alice has encoded qubit in the Z-basis.

This message of qubits is then sent to Bob over Eve's quantum channel:

Alice's Knowledge	Over Eve's Channel	Bob's Knowledge
alice_bits		
alice_bases		
Massage	Massage	massage

Step3:

Bob then measures each qubit in the X or Z-basis at random and stores this information:

The 'measure_message' applies the corresponding measurement to the qubits sent by Alice. The measurement is done in the same basis that Alice used to encode the qubits. The function

simulates the result of measuring each qubit and stores the measurement results in the variable 'bob_results'.

Bob also chooses the basis randomly, and the variable 'bob_basis' keeps track of the basis that Bob used to measure the qubits. After Bob's measurement, the qubits are decoded and the information is stored in the variable 'bob_results', which is now only known to Bob.

By comparing the results of Alice and Bob, they can detect any discrepancies caused by an eavesdropper's measurements. They also discard the results of the qubits that were measured in different bases. The remaining results from the raw key.

Since Bob has by chance chosen to measure in the same basis Alice encoded the qubit in, Bob is guaranteed to get the result 0. For the qubit, Bob's random choice of measurement is not the same as Alice's, and Bob's result has only a 50% chance of matching Alices'.

Bob generates his own random bit string.

$b' = b'_1 b'_2 \dots \dots b'_n$

Bob measures the received qubits according to b'.

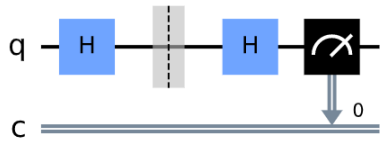
If $b'_k = 0$, Bob measures k^{th} in Z-basis.

If $b'_k = 1$,Bob measures k^{th} in X-basis.

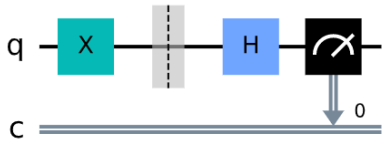
If k^{th} outcome is +1, then key=0

If k^{th} outcome is -1, then key=1

	z-basis	*x-basis*
	$\|\psi_{00}\rangle = \|0\rangle$	$\|\psi_{01}\rangle = \|+\rangle$
	$\|\psi_{10}\rangle = \|1\rangle$	$\|\psi_{11}\rangle = \|-\rangle$



Bob decoded qubit in the X-basis.



Bob decoded qubit in the Z-basis.

Bob keeps his results private.

Alice's Knowledge	Over Eve's Channel	Bob's Knowledge
alice_bits		
alice_bases		
Massage	massage	massage
		bob_bases
		bob_results

Step 4:

After Bob has made his measurements, Alice publicly reveals through the channel which qubits were encoded in which basis. This is done by sending the information stored in the variable 'alice_bases' over the channel. Bob then uses this information to compare his measurements with the bases used by Alice.

By comparing the bases used by Alice and Bob, they can determine which qubits were measured in the same basis, and which ones were not. They then discard the results of the qubits that were measured in different bases, as these results will not be used to form the final key. The remaining results from the raw key.

It's important to note that this information is sent over the channel that Eve can listen, but as Alice and Bob knows which qubits were sent in which basis, Eve will not be able to know which qubits were sent in which basis, so Eve will not be able to know the key.

Alice reveals (through Eve's channel) which qubits were encoded in which basis:

Alice's Knowledge	Over Eve's Channel	Bob's Knowledge
alice_bits		
alice_bases		
Massage	massage	massage
		bob_bases
		bob_results
	Alice_bases	Alice_bases

And Bob reveals which basis he measured each qubit in:

Alice's Knowledge	Over Eve's Channel	Bob's Knowledge
alice_bits		
Alice_bases		
Massage	massage	massage
		bob_bases
		bob_results
	Alice_bases	Alice_bases
bob_bases	bob_bases	

If Bob happened to measure a bit in the same basis Alice prepared it in, the entry in bob_results will match the corresponding entry in alice_bits, and they can use that bit as part of their key. If they measured in different bases, Bob's result is random and not correlated with the key and they both throw that entry away.

The function 'remove_garbage' you mentioned is used to remove the bits that were measured in different bases. The function compares the bases used by Alice and Bob and discards the bits that were measured in different bases. The remaining bits form the raw key.

This step is essential for the security of the protocol, as it ensures that any information obtained by an eavesdropper, who may have intercepted and measured the qubits in a different basis, is discarded.

After this step, Alice and Bob are left with a raw key that they can use to extract a secure and secret key through the process of error correction and privacy amplification.

After removing the bits that were measured in different bases, Alice and Bob are left with a raw key. They then use the remaining bits to form their secret keys.

Alice's Knowledge	Over Eve's Channel	Bob's Knowledge
alice_bits		
alice_bases		
Massage	massage	massage
		bob_bases
		bob_results
	Alice_bases	Alice_bases
bob_bases	bob_bases	
alice_key		bob_key

Alice String a		**1**	**0**	**0**	**1**	**1**
Alice String b		**1**	**0**	**1**	**1**	**0**
Alice Basis		**X**	**Z**	**X**	**X**	**Z**
Alice Encoded qubits		$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$
Bob String b’		**1**	**1**	**1**	**0**	**0**
Bob’s basis		**X**	**X**	**X**	**Z**	**Z**
Key		**1**	**0/1**	**0**	**0/1**	**1**

When $b_k = b'_k$,keep the bits $a_{k,}key$. Otherwise discard bits.

Shared key: 101

Step5:

After the process of error correction and privacy amplification, Bob and Alice have a secret key that they can use to encrypt and decrypt messages. To make sure the BB84 protocol has worked correctly, they compare a random selection of the bits in their keys.

This step is known as the key verification step. By comparing a random selection of the bits in their keys, Bob and Alice can detect any discrepancies that may have occurred during the transmission of the qubits. If there are discrepancies, it indicates that an eavesdropper has attempted to intercept the qubits and the key is discarded.

This step is important for the security of the protocol, as it ensures that any attempt to intercept the qubits will be detected. If the key verification step is successful, it indicates that the key is secure and can be used for encrypting and decrypting messages.

It's important to note that the key verification step is only done once, and any subsequent encryptions are done using the same key. The key will be discarded if the verification step fails.

After the key verification step, Alice and Bob both broadcast the results of their key verification publicly. This is done to ensure that any discrepancies that may have occurred during the transmission of the qubits are detected, and to prevent the use of a compromised key.

The bits used for key verification are no longer secret, and they are removed from the secret key. The remaining bits in the key are still secret and can be used to encrypt and decrypt messages.

It's important to note that the key verification step is an optional step, and it can be skipped, but doing so would decrease the security of the protocol. Key verification is a way to ensure that the key is secure and that any attempt to intercept the qubits has been detected.

Alice's Knowledge	Over Eve's Channel	Bob's Knowledge
alice_bits		
alice_bases		
Massage	massage	massage
		bob_bases
		bob_results
	Alice_bases	Alice_bases
bob_bases	bob_bases	

alice_key		bob_key
bob_sample	bob_sample	bob_sample
alice_sample	alice_sample	alice_sample

If the protocol has worked correctly without interference, their samples should match.

If their samples match, it means (with high probability) alice_key == bob_key. They now share a secret key they can use to encrypt their messages.[6]

Alice's Knowledge	Over Eve's Channel	Bob's Knowledge
alice_bits		
alice_bases		
Massage	massage	massage
		bob_bases
		bob_results
	alice_bases	alice_bases
bob_bases	bob_bases	
alice_key		bob_key
bob_sample	bob_sample	bob_sample
alice_sample	alice_sample	alice_sample
shared_key		shared_key

16. Entanglement based Quantum Key Distribution:

Above we saw about the BB84 single photon-based quantum key distribution protocol. There we had two communicating parties say Alice and Bob that use a public quantum channel to establish a secret key. What Alice does is she prepares qubits in four different states at random. The states can be either $|0\rangle$,$|1\rangle$, or they can be $|+\rangle$, or $|-\rangle$, and then she transmits these states to Bob. Then Bob randomly measures them either in X or Z basis. In our way of approach, After the measurement is finished, Alice and Bob exchange information about the preparation bases and the measurement bases, and if these coincide.

They keep results for those measurements, and that forms the basis for their secret key and if they dedicate a portion of the security key to eavesdropper detection, they can do that due to non-orthogonality of the original encoded qubit states. We imagined that there's an eavesdropper, Eve, and she cannot know the preparation basis. Considering the case that she does have information about the bases in which Alice prepared the original qubits. She can intercept the first qubit, and she knows that this qubit was prepared in the Z basis, therefore she measures it in the Z basis and obtains the corresponding classical bit and then she just resends the photon back to Bob. She intercepts the second qubit, and again because she knows the information about Alice's preparation basis, she measures in the appropriate basis, which in this case is the X basis, and because the case is minus, she obtains a classical bit one. And she repeats this procedure so on and so forth. She measures in the Pauli Z basis for the third qubit, she obtains a classical bit zero, and then resends that qubit back to Bob. So, what she is doing, is although, she's measuring these qubits, she is not disturbing them at all because she's always measuring in the same bases in which they were prepared. So, in this way, she can actually build up a secret key that's perfectly correlated with the key that Alice and Bob are sharing. This is a big problem because then the whole procedure of BB84 fails. Even though Alice and Bob, they can try and detect Eve as they would in the normal protocol, but she has not disturbed any of the qubits. Therefore, they will never detect her presence.

On the other hand, in entanglement-based quantum key distribution protocol, it relies on a pre-shared entanglement between Alice and Bob. We will assume that Alice and Bob can communicate over a classical channel, and also that there is some source of entangled states, and

this source generates multiple copies of entangled state and distributes it to Alice and to Bob. Even though the main source of the pre shared qubits is eve, the connection between Alice and Bob remains intact due to the monogamy of entanglement, so the protocol still remains secure in the sense that Alice and Bob can easily detect an eavesdropping Eve. This protocol is known as E91 protocol.

17. Monogamy of Entanglement:

Monogamy of entanglement is a very fundamental property of quantum states, and it constrains how correlated multiple qubits can be. Monogamy of entanglement is the fundamental property in quantum physics where it cannot be freely shared between arbitrarily many parties. In order for two qubits to be maximally entangled, they must not be entangled with any third qubit. Even if the qubits are not maximally entangled, the degree of entanglement between them limits the extent to which either can be entangled with the third. Monogamy is closely related to no cloning property and is purely a feature of quantum correlations. Monogamy of entanglement has broad range of application starting from quantum mechanics, black hole physics, and quantum cryptography and mostly on quantum key distribution.

E91 protocol is mostly focused on the property of monogamy of entanglement. The connecting parties has qubits that are entangled. If they are maximally entangled, there is no chance of third party to interfere this connection. Even though they are not maximally entangled, the existence of the third party is distinguishable. Due to this property, the ‘monogamy of entanglement’, E91 protocol has been more secure than BB84 protocol.

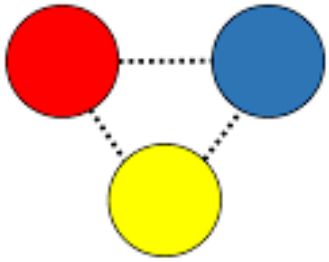


Fig: 1

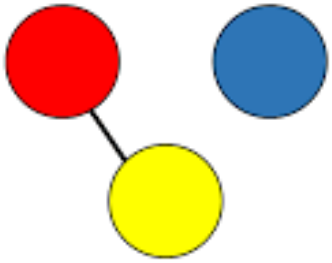


Fig: 2

Here, in figure 1, none of the qubit pairs are maximally entangled so they share each of them with each other. But in figure 2, red and yellow are maximally entangled. So, they share no connection with blue.[9]

18. Steps for Entanglement based QKD protocol:

A) Establishing a secret key:

The first step is to establish a secret key. We have to use an entangled state of two qubits. So, let's consider the case where Alice and Bob are sharing a Bell pair. The state is described by this state, $|\psi^+\rangle$, which is an equal superposition of basis states |01> and |10>. If we measure these qubits in the same basis, the outcomes will be correlated or anti-correlated depending in which basis they are measured. The probability of these outcomes is uniformly random. Starting in this Bell state $|\psi^+\rangle$, and both Alice and Bob measure in the X basis.

Then we can compute the probabilities of all four possible outcomes. So, the probability that both Alice and Bob obtain a correlated result of |++>, is given by a half. The probability that they get an outcome |-- >, is also a half, and the other two probabilities therefore have to be 0. So, in this way, when Alice measures state +, Bob always measures state |+>. When Alice measures state |->, Bob always measures state minus. So, in terms of their classical bits that they get as the

outcomes of their measurements, they always get either |00> with probability a half, or |11> with the same probability of fifty percent.

So, in this way, they can establish a secret random correlated key. If they measure in the z basis, the scenario is very similar, although now the results are anti-correlated. So, the probability that they get both of them get state |00> is 0, same for the probability of obtaining the state |11> which is 0. And with equal probability they either get the state |01> or |10>. So always, when Alice measures zero and she's measuring in the Z basis and Bob also measures in the Z basis, she knows that he always gets the state one, and vice versa, if she measures the state one, Bob will always measure state zero. So, in this case, the classical key that they get is anti-correlated as well, just like the quantum results. So, Alice either has zero and Bob has one with probability fifty percent, or it's vice versa, Alice has one and Bob has zero. Well, but they know that they are both measuring the Z basis, so all that Bob needs to do is flip his bit and they again establish a correlated secret random key which they can use to encrypt their data.

B) Verifying Entanglement:

The second step is to verify that they have an entangled state. Entangled states can be used to generate a correlated random key. But also, there is a very important second step which was not present in the BB84 protocol, and that is that entanglement can be used for security as well, namely maximally entangled states are guaranteed to be secure due to something known as "monogamy of entanglement" which has been stated above. In particular, if Alice and Bob share a maximally entangled state, then we are guaranteed that they cannot share any correlations with a third party, such as Eve.

So, in terms of security this is very important because if they can demonstrate and verify that they have a maximally entangled state, they are automatically demonstrating that whatever key they establish is secure and Eve does not have any information about their secret key.

In general, there is a trade-off. So, if Alice and Bob share some entanglement, they will share some correlations with Eve. So, the stronger the entanglement that they share, the less correlated they are with Eve, until, to the point where they are maximally entangled and therefore, they share

no correlations with Eve. So, stronger entanglement between Alice and Bob- it implies more secure key between Alice and Bob.

We use something known as CHSH inequality to verify if two parties have maximally entangled key. Let's consider four classical random variables, denoting them as A, a, B, and b, and they all can have values plus one or minus one. We form the function with these random variables. We take B and b, and we add them together and multiply by the value of A. We also take B and b and take the difference between them and multiply by a, and then we sum the two together. Total result we can get for this expression is plus two, and the minimum value that you can get is minus two.

We are constantly generating these random variables- A, a, and you are interested on average what expression do we get here and that will be constraint. So, we are taking average values from the expression, and we are adding it with this expression, and we take the absolute value of the whole sum, and that is constrained to be less or equal to two.

The maximum they can get is two. The minimum they can get is minus two. So those are the two extremes, and the expectation value will be somewhere in between depending on the details of the probability distributions for this random classical variable. What we get is the following expression which we are going to denote by this "S", and refer to it as CHSH expression, and that as we said must be less or equal to two. And this inequality is known as the CHSH inequality. So, any classical random variable A, a, B, b, they must satisfy this constraint. This is for the classical case. [9]

Mathematical Expression:

$$\boldsymbol{A}, \boldsymbol{a}, \boldsymbol{B}, \boldsymbol{b} = +\mathbf{1}\ \boldsymbol{or}\ -\mathbf{1}$$

$$\boldsymbol{A}(\boldsymbol{B}+\boldsymbol{b}) + \boldsymbol{a}(\boldsymbol{B}-\boldsymbol{b}) = -\mathbf{2}\ \boldsymbol{to}\ +\mathbf{2}$$

$$|<\boldsymbol{A}(\boldsymbol{B}+\boldsymbol{b})> + <\boldsymbol{a}(\boldsymbol{B}-\boldsymbol{b})>| <= \mathbf{2}$$

$$\boldsymbol{S} = |<\boldsymbol{AB}> + <\boldsymbol{Ab}> + <\boldsymbol{aB}> - <\boldsymbol{ab}>| <= \mathbf{2}$$

In the quantum case, we can consider A, a, B, b, to be the measurement outcomes in a certain basis on some state psi. The expectation value of an observable where Alice measures A and Bob measures B is given by this expression. Taking the tensor product of the observables A and B, we compute the following expectation value with respect to the state psi. For some quantum states we can actually violate the CHSH inequality. By violating, we mean that we can obtain a value that's larger than two. So then, what it means is we can use this expression to detect entanglement. In particular, in an experiment when we measure and compute these various expectation values, and then we sum them up in this manner and we obtain a CHSH expression which is less than two, then we can say maybe the states are classically correlated. But, if we measure a CHSH expression which is larger than two, then we can, in fact, say that definitely these states are entangled. And in quantum mechanics, the CHSH expression can go all the way up to a value of two times the square root of two. This happens for maximally mixed states.

Let's say we take one of the Bell pairs, $|\psi^+\rangle$, and we know that it's a maximally entangled state. And for the measurement settings, we consider the following- A is the Pauli Z observable, a is the X observable, and B and b are given by these combinations of Z and X, so these are just rotated measurement bases. Then, we can just go through the algebra of computing the expectation values, and what we get is, in fact, that for a maximally entangled state, we obtain this CHSH expression of two root two. So, this gives us a way of verifying entangled states, and particularly verifying maximally entangled states, which is very important for entanglement based QKD protocol. So, if we can demonstrate that we violate the CHSH inequality maximally, meaning the CHSH expression is two root two, then we can certify that, in fact, the state that

Alice and Bob share is a maximally entangled state. That then allows us to tell that they are not correlated with Eve due to monogamy of entanglement, and therefore we can guarantee the security of their secret random key.[9]

19. E91 Protocol Explained:

Alice and Bob can communicate over a classical channel, and they share multiple copies of a maximally entangled state. These copies can be generated by Eve herself. Then, Alice and Bob randomly choose a measurement basis in which they measure their qubits. Alice's measurement setting or measurement basis A1, corresponds to measurement in the Z basis. If she does that, she projects the state either into a zero or into a one. She can also measure in the X basis, given by the horizontal direction. Or she can measure by a rotated basis A3, which is a linear combination of Z+X. Bob, on the other hand, can measure also in the Z basis given by B1, or in this rotated basis B2 which is Z - X, or in the basis B3 which is over here given as Z+X. If both Alice and Bob measure the entangled state in the same basis, they can use that information via classical channel. We need some rotated bases such as this A3, and B2, and B3, in order to compute the CHSH expression and see if it violates the classical CHSH inequality in order to establish that Alice and Bob are really sharing an entangled state. So, in order to establish the key, Alice measures either in A1 or A3, and Bob measures in B1 or B3. So, they randomly measure their multiple copies of entangled states, and then they exchange information about the basis of their measurements. In some other cases, they will not measure in bases that coincide. They don't discard these results, instead they use them to compute the CHSH expression and check if they get the corresponding violation of the classical CHSH inequality. In particular, they look for scenarios where both of them measure (A1, B3), or (A1, B2), (A2, B2), or (A2, B3).

So, visually it does correspond to Alice looking for cases where she measures in the Z basis and in the X basis, and Bob measures in this rotated bases B2 and B3, and then they use those measurement results to compute the following expression, which is just the sum of expectation values where Alice measured B1 and Bob measured B2, Alice measured A1 and Bob measured B3, and so on. So, this way, they don't need to discard any information like in BB84, but they really get to use it to calculate either the secret correlated key or the CHSH violation.

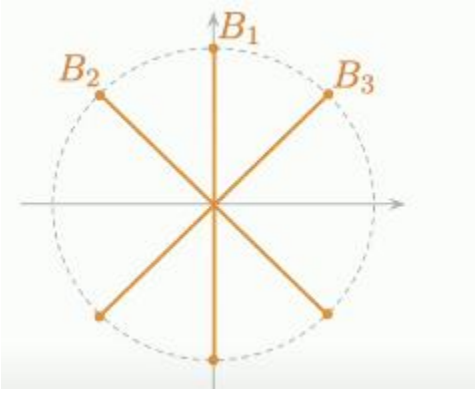
And if they obtain a CHSH expression of less or equal to two, it is okay. We cannot conclude that we have an entangled state or not, but it's safer to just abort. Monogamy of entanglement ensures that if they have an entangled state, then Eve is not strongly correlated with either of them. And in particular, if they have a maximally entangled state, then Eve is not correlated with Alice and Bob at all, so they are looking for as strong a violation as they can get. And if they have a CHSH expression larger than two, then they conclude that they are sharing an entangled state. Therefore, we can proceed with the protocol.[11]

A1=Z B1=Z

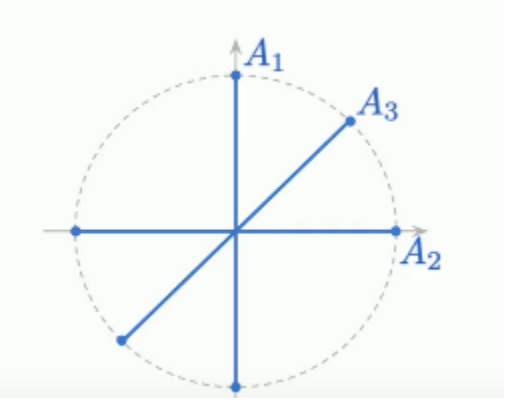
A2=X B2= 1(Z-X)/√2

A3=1(Z+X)/√2 B3=1(Z+X)/√2

Bases may vary based on consideration.



Alice’s measurement bases on Bloch sphere



Bob’s measurement bases on Bloch sphere

20. Difference between BB84 and E91(Security Issues):

BB84 is based on the indistinguishability of single photons prepared in non-orthogonal bases, and the other one is using entanglement based QKD. For security reasons sometimes we ask the question- when is the secret key generated? In the case of the BB84 protocol, it's generated when Alice generates her random string right at the beginning of the protocol. She generates two random n-bit strings. One is to encode the information about the basis of preparation, and the other one about the states in this basis.

So, if she chooses Z basis, is it a zero or a one, if she chooses the X basis, is it a + or a -. So, the key- the secret key exists right from the beginning before any communication between Bob and Alice take place. So that means that a clever Eve can actually find a way how to obtain some information about this secret bit string. In particular, one can consider a very paranoid scenario where the random number generated that Alice is using to generate a random bit string was actually produced by Eve and is in some way correlated with Eve, therefore whatever bits-random bit string that the device produces, that information gets passed on to Eve. It poses a huge security risk for BB84 protocol. Whereas in the E91 protocol, the secret key is really generated after the entangled pairs of qubits are measured. Secret key generation happens only after Alice and Bob measure them in their random bases. So, in that sense, we can say that the key is unconditionally secure, and we see that entanglement is very essential for security.[12]

21. Effect of noise in E91:

Ideally in the theory there is no noise in E91. In real life Alice and Bob will not be able to generate a perfectly correlated key, meaning that either noise or the tinkering of Eve will introduce some inconsistencies into the key, and therefore the key will be nearly identical. Even if Eve is not trying to actively eavesdrop and disrupt the protocol, still due to inherent noise in the system, these keys will not be perfectly correlated. So, what then Alice and Bob have to decide, they must decide on the acceptable security risk even if the keys are not perfectly correlated. If the correlation is not a hundred percent, but it's very close to hundred percent, it

still can be used this to do something useful and use it for a secret communication. If they do that, then they have to engage in two more protocols.

One is called the "information reconciliation". That takes the initial secret key that's not perfectly correlated and produces a more correlated key. So, it's increasing the correlation between Alice and Bob in their secret key. And furthermore, they also can perform “privacy amplification", where they take their generated secret key, and they produce a shorter key which is more secure. So, they are basically trying to eliminate any possible correlation with Eve.[9]

22. E91 in real world experiments:

One experiment was performed over free space, meaning that the entangled photons traveled through air, and it was done over a distance of hundred and forty-four kilometers between two islands in the Canary Islands, one was La Palma and the other one Tenerife. And these photons were produced by spontaneous parametric down-conversion process, so the entire pair of photons was encoded in the polarization of the photons. And the obtained CHSH violation, it was of 2.508. A different, more recent experiment was done over a distance of hundreds of kilometers, but it was done in a lab and over optical fiber. So, the fiber was very long and the one distance that was tested was three hundred and eleven kilometers over standard fiber, and the other distance was four hundred and four kilometers over an ultra-low loss fiber, and the obtained bitrate for the secret key was of the order of 10^{-3}, or 10^{-4} for the longer distance. Now, these bit rates don't actually include the information reconciliation and privacy amplification part, so if we wish to use this scheme in real life, we would actually have to perform information reconciliation and privacy amplification, which would further drop the bit rate. And another fantastic experiment was performed with satellites, where the satellite actually distributed entangled pairs between two ground stations, and the ground stations were 1120 km apart. The light travels in a straight line, whereas using a satellite we can overcome the complication of curved earth's surface to establish a quantum key over much longer distances. So, the total distance was over 1000 km, and this measured CHSH violation was 2.56, and

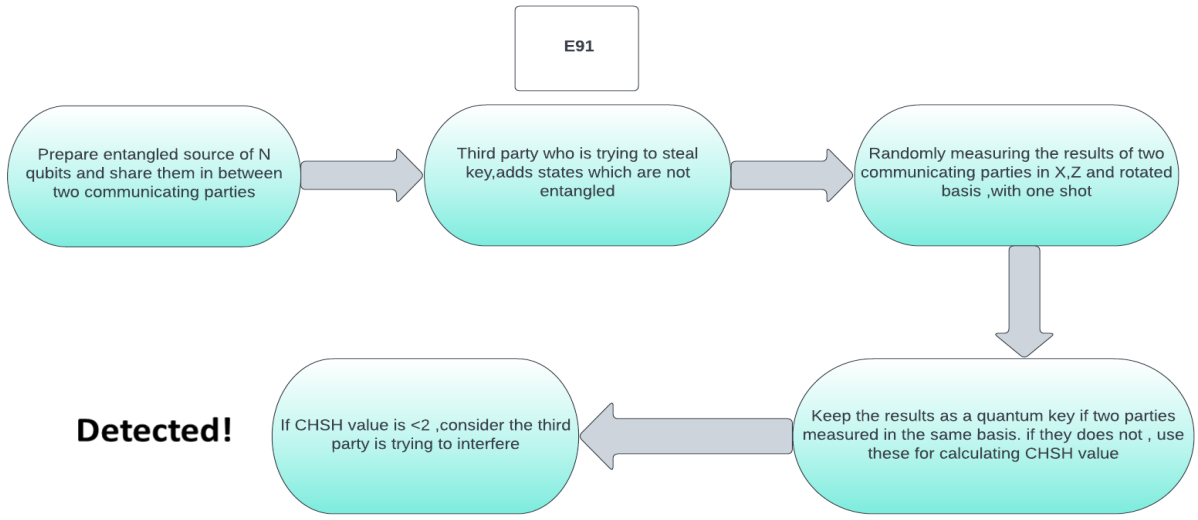
the obtained bit rate was 0.12 bits per second. These results estimated that that would have been around eleven orders of magnitude less efficient than using the satellites. [12]

23. Our Approach with E91 based QKD Security:

E91 protocol is much safer than BB84 protocol due to the monogamy of entanglement, but we created a hypothetical situation where a third party is trying to break the entanglement by mixing states and telling the communicating parties that they have entangled pairs. But we solve it by simulating and implementing the E91 protocol and measuring its CHSH value each time they try to communicate, making the QKD much safer.

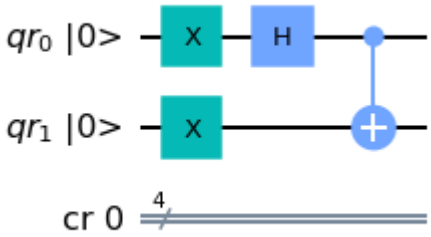
In E91, two parties communicate using N entangled qubits sharing $|\psi^+\rangle$ state, which can be shared by a third party as well. Instead of sharing entangled qubits, the third party is mixing non-entangled states into the system and provoking the two communicating parties to use this channel. After X, Z, and rotated basis measurements, the result will give a correlated key to be distributed among two parties for encryption and decryption. Bases not used in key generation will be used to calculate the CHSH inequality value and show if the value is less than 2. Measuring the value each time two parties communicate can detect eavesdropping.[13]

24. System diagram of Quantum Protocol:

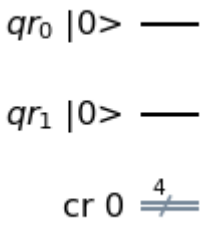


25. E91 Protocol Procedure:

We created a singlet of 2 quantum registers with 2 qubits shared $|\psi^+\rangle$state between Alice and Bob. Then we created singlets of n times. We took a variable called percentage of singlet to add entanglement percentage. The first quantum register qr0 contains Alice's qubit and qr1 contains Bob's qubit.



Then we created |00> state and shared this between Alice and Bob. The amount of impurity shared by eve is number of singlets*(1-percentage of singlet)



Then we measured randomly by appending the measurement circuits with singlet and impurity circuits. The following are the circuits for measurment in :

A_1=X basis

A_2=W basis=1(Z+X)/√2

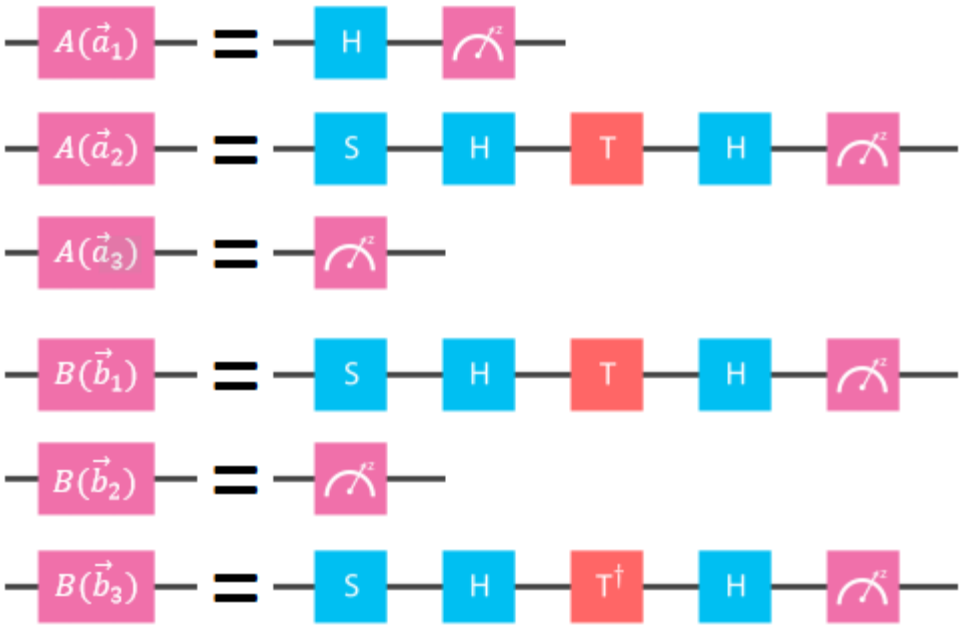
A_3=Z basis

B_1=W basis=1(Z+X)/√2

B_2=Z basis

B_3=V basis=1(Z-X)/√2

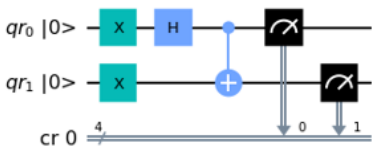
Here, W and V are rotated basis. A is Alice's measurement circuits and B is Bob's measurement circuits.



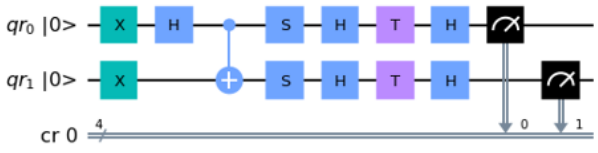
We run the circuits using 1 shot because we want 1 result. After randomly measuring the circuits, we get 0 or 1 which are converted to -1 and +1 afterwards. In This pattern we create the random secret key.

After appending and measuring the result secret keys are generated. For that basis which did not match are used for measuring CHSH measurement.

Circuits for key generation

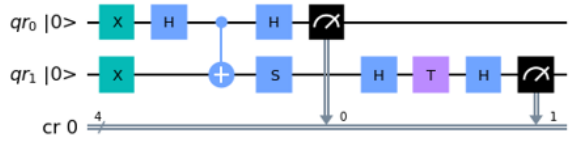


Alice and Bob both in Z basis

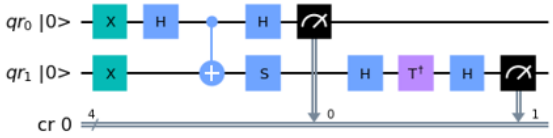


Alice and Bob both in $1/\sqrt{2}(Z+X)$

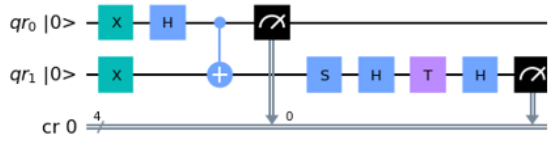
Circuits for measuring CHSH



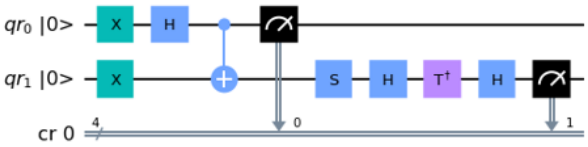
Alice in X ,Bob in 1/√2(Z+X)



Alice in X ,Bob in 1/√2(Z-X))



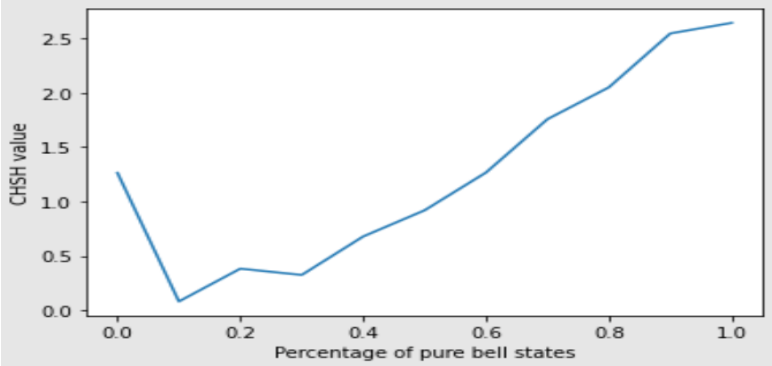
Alice in Z ,Bob in 1/√2(Z+X)



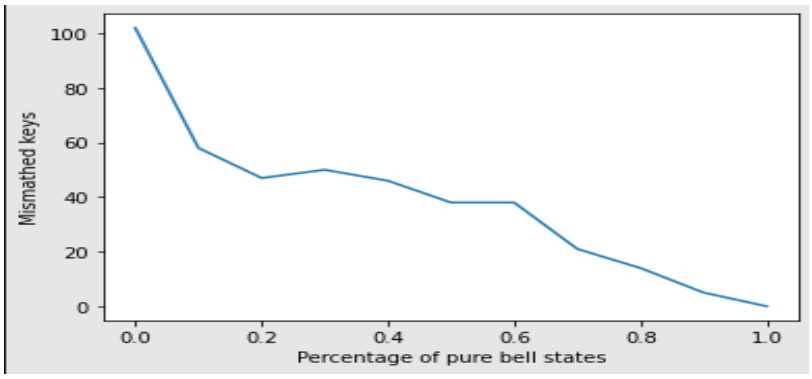
Alice in Z ,Bob in 1/√2(Z-X))

After finding the CHSH value we plotted the graph and made some comparison which are in the result section.

26. Result and Analysis:



We experimented Eve's eavesdropping ability by giving N qubits of Non EPR states at the beginning and then increased the entanglement (percentage of pure bell/EPR state) between two communicating parties. For CHSH value of 2 (the starting range of entanglement), we get nearly 80% of EPR state, meaning 20% Non EPR state doesn't cease communication.



Due to noise caused by Eve in the communicating system we do not get a correlated secret key. When qubits are Non EPR/Non entangled key mismatch is highest and for maximally entangled state of qubits key mismatch is 0. In an acceptable communication range 18% key mismatch is ignorable.

27. Financial Model:

Quantum communication's financial scalability is a significant but largely unexplored area in cryptography. Quantum cryptography would have a transformative influence on the economy. Scientists have demonstrated that QKD works, but it is not widely used due to significant technological limitations. There is also evidence that a long distance, noisy channel can be used for the secure transmission of a quantum key. Governments have historically kept military data secret. Quantum cryptography offers practical uses for both governments and militaries. On the other hand, quantum cryptography uses the concepts of quantum mechanics to transmit secure messages. Public key encryption can guarantee confidentiality, and encryption is used in electronic money schemes to safeguard traditional transaction data such as account numbers and transaction amounts using these secured quantum protocols. Quantum cryptography may be implemented into current networks and could increase internet security.

28. Future Possibilities:

In order to safeguard healthcare information in wireless communication, the system should eventually integrate a more mathematical and computational technique. Strong security on wireless body sensor networks is offered by a novel upgraded BB84 and E91 quantum cryptography protocol in healthcare applications.

29. Conclusion:

Quantum cryptography protocols such as BB84 and E91 contribute to solve the problem of keys distribution. Classical and quantum channels are both used in quantum cryptography protocols to distribute the key. BB84 protocol was the first to propose the use of quantum principles, making it potentially unbreakable. Protocol E91 added the use of quantum entanglement. Therefore, the analysis of the results allowed for the validation of the final key size for the BB84 technique. Moreover, without making any assumptions about the abilities of a potential eavesdropper, two parties can securely establish a secret key when given access to an insecure quantum and classical channel. This is because no eavesdropper can accurately measure the quantum state being sent without changing the state in some observable way, thanks to the laws of quantum mechanics. This work included an overview of the most well-known QKD techniques found in the literature and briefly defined these basic principles. These included Eckert's method employing quantum entanglement and the BB84 protocol and its derivatives, which derive their security from Heisenberg's Uncertainty Principle. Additionally, this research provided a brief overview of a few methods for achieving real-world QKD. However, it was found that the E91 procedure had a discrepancy that was smaller than what had been statistically predicted. The E91 protocol is considered to be safer as an outcome.

30. References:

1. Sharma, A.; Ojha, V.; Lenka, S. Security of entanglement based version of BB84 protocol for Quantum Cryptography. In Proceedings of the 2010 3rd International Conference on Computer Science and Information Technology, Chengdu, China, 9–11 July 2010; Volume 9, pp. 615–619.

2. Chong SK, Hwang T. "Quantum key agreement protocol based on BB84" Opt Commun 2010; 283(6): 1192–1195.

3.Li J, Chen YH, Pan ZS, et al. Security analysis of BB84 protocol in the collective-rotation noise channel. Acta Physica Sinica 2016; 65(3): 030302.

4.T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, “Quantum cryptography with entangledphotons,” Phys. Rev. Lett. 84, pp. 4729–4732, May 2000.

5.C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, “Optimal eavesdropping in quantumcryptography. i. information bound and optimal strategy,” Phys. Rev. A 56, pp. 1163–1172, Aug 1997

6.Mina, M.Z.; Simion, E. "A Scalable Simulation of the BB84 Protocol Involving Eavesdropping. In Innovative Security Solutions for Information Technology and Communications"; Springer: Cham, Switzerland, 2021; pp. 91–109.

7. A. K. Ekert, “Quantum cryptography based on bell’s theorem,” Physical Review Letters 67, pp. 661–663,Aug 1991.

8. Mahmud, Naveed, et al. "Securing and auto-synchronizing communication over free-space optics using quantum key distribution and chaotic systems." Quantum communications and quantum imaging XVI. Vol. 10771. SPIE, 2018.

9. Dong Yang, A simple proof of monogamy of entanglement, Physics Letters A, Volume 360, Issue 2, 2006, Pages 249-250
10.Daniel Collins, Nicolas Gisin, A relevant two qubit Bell inequality inequivalent to the CHSH inequality, Journal of Physics A: Mathematical and General, Volume 37,Issue 5,2004

11. Ling A, Peloso M, Marcikic I, Lamas-Linares A, Kurtsiefer C. Experimental E91 quantum key distribution. Advanced Optical Concepts in Quantum Computing, Memory, and Communication. 2008 Feb; 6903:69030U.

12. Hong KW, Foong OM, Low TJ. Challenges in quantum key distribution: A review. In Proceedings of the 4th International Conference on Information and Network Security 2016 Dec 28 ; pages 29-33

13. Cui D, Mehta A, Mousavi H, Nezhadi SS. A generalization of CHSH and the algebraic structure of optimal strategies. Quantum. 2020 Oct 21;4:346.

14. Giampouris D. Short review on quantum key distribution protocols. GeNeDis 2016: Computational Biology and Bioinformatics. 2017, Pages 149-57.