Report on
Quantum Cryptography and Communications

Submitted by:
RA2011003011247 - Jatin Singhania
RA2011003011248 - Utkarsh Saboo
RA2011003011310 - Aryan Kumar Sinha
RA2011026010029 - R Shreyas
RA2011026010175 - Tanvi Gupta
RA2011026010260 - Akash R
RA2011026010411 - Pranshu Gupta
RA2011027010138 - Yuvraj Singh Nughaal
RA2011027010142 - Reshma Merin Thomas
RA2011033010083 - Viraj Vijay Phate(Team Head)

What is cryptography?

Cryptography is a method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it.

On the computer side of the story, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet, and confidential communications such as credit card transactions and email.

What is quantum cryptography?

Quantum cryptography is a method of encryption that uses the naturally occurring properties of quantum mechanics to secure and transmit data in a way that cannot be hacked.

Quantum cryptography is a system that is completely secure against being compromised without the knowledge of the message sender or the receiver. That is, it is impossible to copy or view data encoded in a

quantum state without alerting the sender or receiver. Quantum cryptography should also remain safe against those using quantum computing as well.

Quantum cryptography uses individual particles of light, or photons, to transmit data over fiber optic wire. The photons represent binary bits. The security of the system relies on quantum mechanics. These secure properties include the following:

- particles can exist in more than one place or state at a time;
- a quantum property cannot be observed without changing or disturbing it.
- whole particles cannot be copied.

These properties make it impossible to measure the quantum state of any system without disturbing that system.

Classical Cryptography and Modern Cryptography

What is Cryptography?

Cryptography is the art and science of making a cryptosystem that is capable of providing information security.

Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services.

Security Services of Cryptography

The primary objective of using cryptography is to provide the following four fundamental information security services. Let us now see the possible goals intended to be fulfilled by cryptography.

1) Confidentiality

Confidentiality is the fundamental security service provided by cryptography. It is a security service that keeps the information from an unauthorized person. It is sometimes referred to as privacy or secrecy.

Confidentiality can be achieved through numerous means starting from physical securing to the use of mathematical algorithms for data encryption.

2) Data Integrity

It is a security service that deals with identifying any alteration to the data. The data may get modified by an unauthorized entity intentionally or accidentally. Integrity service confirms whether data is intact or not since it was last created, transmitted, or stored by an authorized user.

Data integrity cannot prevent the alteration of data, but provides a means for detecting whether data has been manipulated in an unauthorized manner.

3) Authentication

Authentication provides the identification of the originator. It confirms to the receiver that the data received has been sent only by an identified and verified sender.

Authentication service has two variants −

- Message authentication identifies the originator of the message without any regard router or system that has sent the message.
- Entity authentication is assurance that data has been received from a specific entity, say a particular website.

Apart from the originator, authentication may also provide assurance about other parameters related to data such as the date and time of creation/transmission.

4) Non-repudiation

It is a security service that ensures that an entity cannot refuse the ownership of a previous commitment or an action. It is an assurance that the original creator of the data cannot deny the creation or transmission of the said data to a recipient or third party.

Non-repudiation is a property that is most desirable in situations where there are chances of a dispute over the exchange of data. For example, once an order is placed electronically, a purchaser cannot deny the purchase order, if non-repudiation service was enabled in this transaction.

Classical Cryptography

Classical Cryptography are concerned with developing algorithms which may be used to:

- conceal the context of some message from all except the sender and recipient (privacy or secrecy), and/or
- verify the correctness of a message to the recipient (authentication)

They form the basis of many technological solutions to computer and communications security problems

Classical cipher

In cryptography, a classical cipher is a type of cipher that was used historically but for the most part, has fallen into disuse. In contrast to modern cryptographic algorithms, most classical ciphers can be practically computed and solved by hand.

In contrast, modern strong cryptography relies on new algorithms and computers developed since the 1970s.

Types of classical ciphers

Classical ciphers are often divided into

1) substitution ciphers.
2) transposition ciphers

Substitution cipher

In a substitution cipher, letters (or groups of letters) are systematically replaced throughout the message for other letters (or groups of letters).

A well-known example of a substitution cipher is the Caesar cipher.

Transposition ciphers

In a transposition cipher, the letters themselves are kept unchanged, but their order within the message is scrambled according to some well-defined scheme. Many transposition ciphers are done according to a geometric design. A simple (and once again easy to crack) encryption would be to write every word backwards. For example, "Hello my name is Alice." would now be "olleH ym eman si ecilA." A scytale is a machine that aids in the transposition of methods.

Mordern Cryptography

Modern encryption is the key to advanced computer and communication security. This stream of cryptography is completely based on the ideas of mathematics such as number theory and computational complexity theory, as well as concepts of probability. In this chapter, you will learn about the different elements and characteristics of modern cryptography.

Types of modern Cryptography

Different algorithms have come up with powerful encryption mechanisms incorporated in them. It gave rise to two new ways of encryption mechanism for data security. These are:

- Symmetric key encryption
- Asymmetric key encryption

Symmetric key encryption

Symmetric key encryption technique uses a straight forward method of encryption. Hence, this is the simpler among these two practices. In the case of symmetric key encryption, the encryption is done through only one secret key, which is known as "Symmetric Key", and this key remains to both the parties. The same key is implemented for both encodings as well as decoding the information. So the key is used first by the sender prior to sending the message, and on the receiver side, that key is used to decipher the encoded message.

One of the good old examples of this encryption technique is Caesar's Cipher. Modern examples and algorithms that use the concept of symmetric key encryption are RC4, QUAD, AES, DES, Blowfish, 3DES, etc.

Asymmetric key encryption

Asymmetric Encryption is another encryption method that uses two keys: a new and sophisticated encryption technique. This is because it integrates two cryptographic keys for implementing data security. These keys are termed as Public Key and Private Key. The "public key", as the name implies, is accessible to all who want to send an encrypted message. The other is the "private key" that is kept secure by the owner of that public key or the one who is encrypting.

Encryption of information is done through a public key first, with the help of a particular algorithm. Then the private key, which the receiver possesses, will use to decrypt that encrypted information. The same algorithm will be used in both encodings as well as decoding.

Examples of asymmetric key encryption algorithms are Diffie-Hellman and RSA algorithm.

Cryptography Primitives

Cryptography primitives are nothing but the tools and techniques in Cryptography that can be selectively used to provide a set of desired security services −

- Encryption
- Hash functions
- Message Authentication codes (MAC)
- Digital Signatures

Differences between modern and classical cryptography

Here are the marked differences between the classical as well as the modern encryption techniques:

Traditional Encryption	Modern Encryption
For making cipher text, manipulation is done in the characters of the plain text.	For making ciphertext, operations are performed on binary bit sequence.
The whole of the ecosystem is required to communicate confidentially.	Here, only the parties who want to execute secure communication possess the secret key.

These are weaker as compared to modern encryption.	The encryption algorithm formed by this encryption technique is stronger as compared to traditional encryption algorithms.
It believes in the concept of security through obscurity.	Its security depends on the publicly known mathematical algorithm.

Elements of Quantum Theory

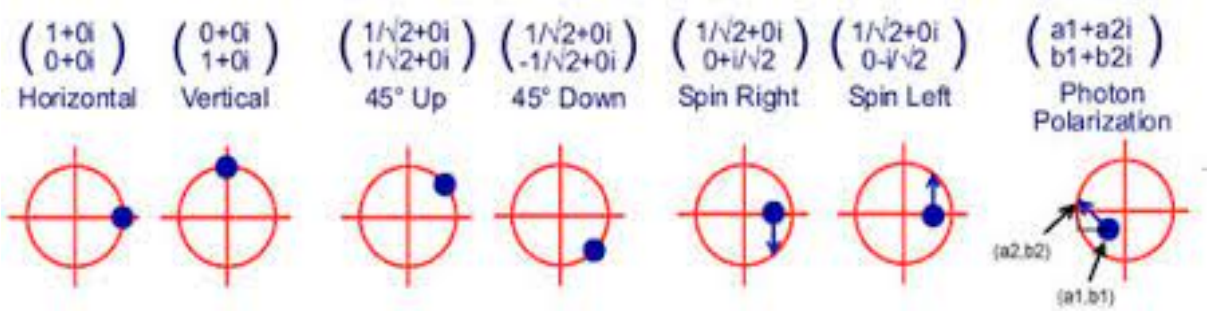
Light waves propagate in the form of small discrete particles(quanta) also known as photons.

Features:

1. Massless
   Meaning it has no rest mass.
2. They have energy
   Each photon carries a quantity of energy equal to the product of the frequency of vibration of that photon and Planck's constant.
3. Speed(c)
   The speed of light in a vacuum, commonly denoted as c, is a universal physical constant that is important in many areas of physics. The speed of light c is exactly equal to 299,792,458 meters per second.
4. Angular Momentum(spin)
   The spin angular momentum of light is the component of the angular momentum of light that is associated with the quantum

spin and the rotation between the polarization degrees of freedom of the photon.

The Spin carries the polarization.



Photon Polarization

The polarization of the photon is a direction in the plane normal to the direction of propagation.

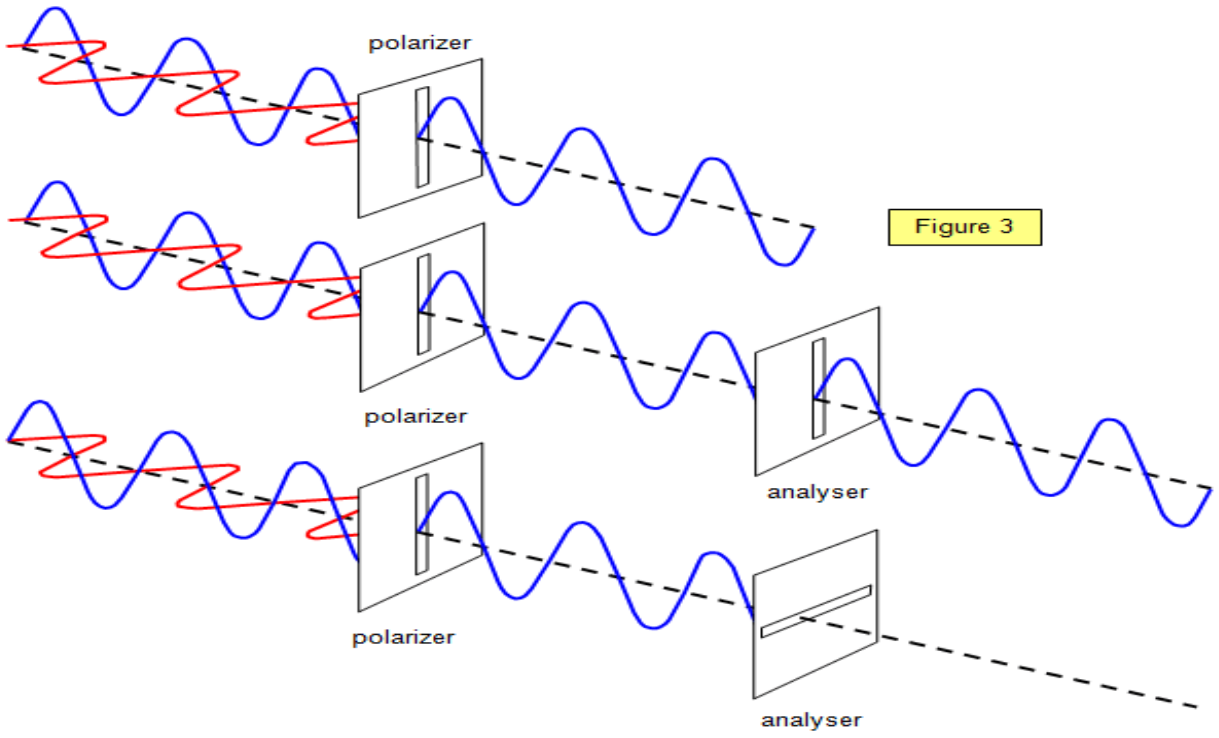
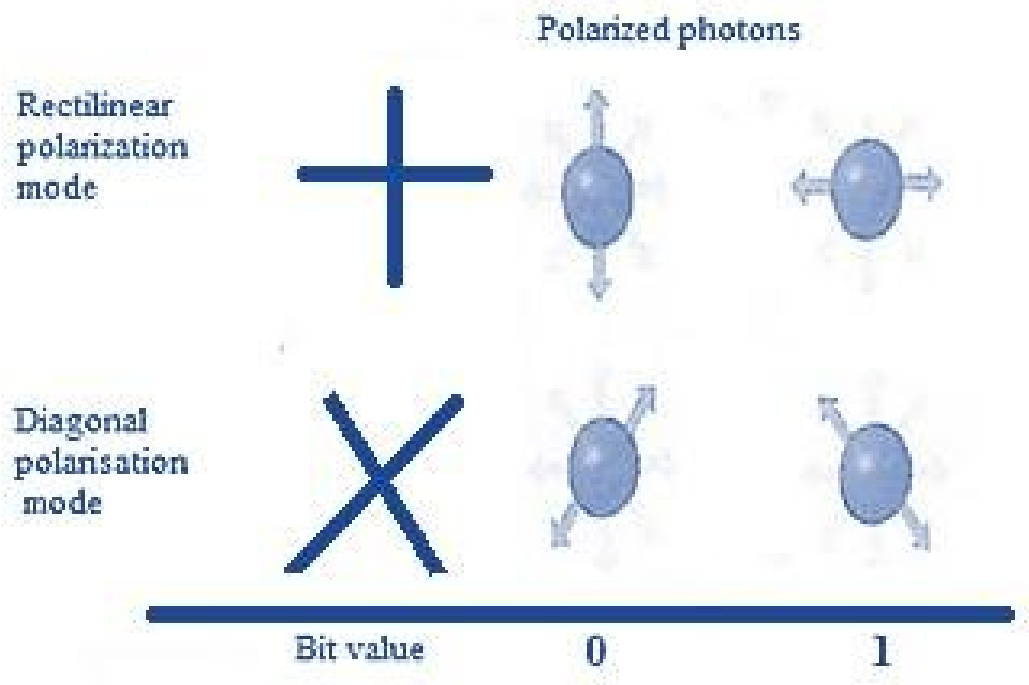


Figure 3

This happens using vertical and horizontal filters, there are even diagonal filters used in cryptography namely diagonal polarization filters.

A polarizing filter blocks photons whose polarization is perpendicular to the orientation of the filter and transmits photons whose polarization is aligned with the filter.



When we use the BB84 algorithm for QKD, we arbitrarily choose which of two filters (bases) to use when detecting a photon: rectilinear or diagonal. If you choose rectilinear filter, you can detect polarization with certainty if the photon is rectilinear, i.e., either vertically or horizontally polarized or if you choose Diagonal polarisation filter, you can detect polarization with certainty if the photon is rectilinear, i.e., diagonally polarized.

Sending and receiving of photons

EAVESDROPPER EVE

- If Eve uses the filter aligned with Alice's she can recover the original polarization of the photon.
- If she uses the misaligned filter she will receive no information about photon.
- Also she will influence the original photon and be unable to retransmit with the original polarization.
- Bob will be able to deduce Ave's presence.

BINARY INFORMATION

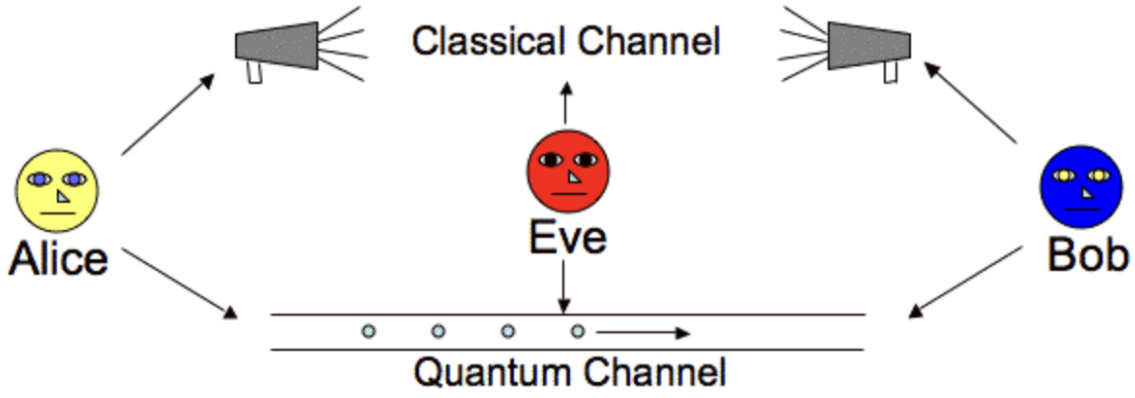
- Each photon carries one qubit of information.
- Polarization can be used to represent a 0 or 1.
- In quantum computation this is called qubit.
- To determine the photon's polarization the recipient must measure the polarization by passing it through a filter.
- A user can suggest a key by sending a stream of randomly polarized photons.
- This sequence can be converted to a binary key.
- If the key was intercepted it could be discarded and a new stream of randomly polarized photons.

THE MAIN CONTRIBUTION OF QUANTUM CRYPTOGRAPHY

- It solved the key distribution problem.
- Unconditionally secure key distribution method proposed by Charles Bennett and Gilles Brassard in 1984.
- The method is called BB84.
- Once key is securely received it can be used to encrypt messages transmitted by conventional channels.

Quantum Cryptography Key Distributions

Quantum key distribution and other protocols use quantum mechanics principles to provide an unconditionally secure public-key cryptosystem. These protocols can even detect the presence of an eavesdropper in the system who is attempting to learn the key.



The concepts from quantum mechanics that make QKD so useful so useful include:

1. Heisenberg's Uncertainty Principle: This principle states that in a quantum system, only one property of a pair of conjugate properties like position and momentum can be known with certainty (a plausible measurement of a particle's position will disturb its speed). Quantum cryptography takes advantage of this by using the polarization of photons (as photons can be exchanged over fiber optic links) on different bases as the conjugate properties.

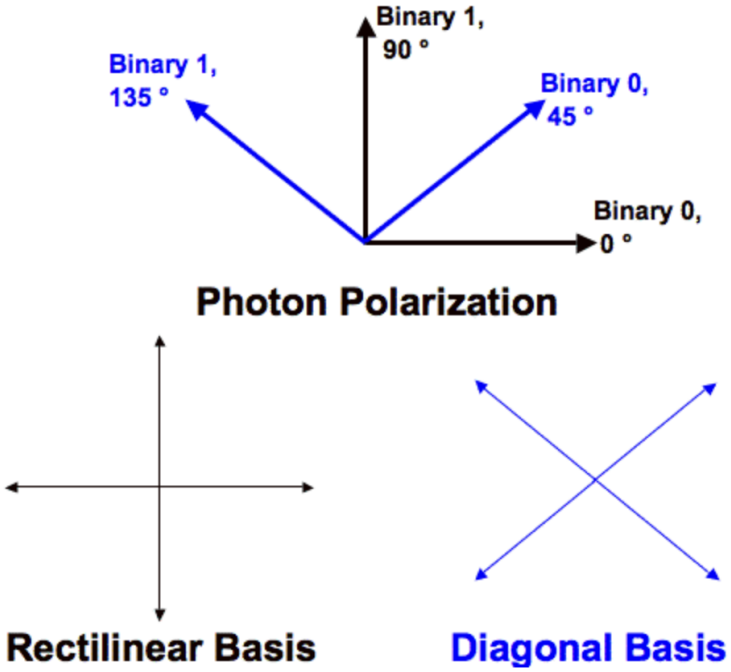
2. No Cloning Theorem: Indirectly following the last principle states that it is impossible to create identical copies of an unknown quantum state. Due to this, it is possible to find out if someone interrupted the quantum channel during the vital transmission.

3. Quantum Entanglement: Regardless of the distance, two quantum particles can entangle. When a particular property is measured in a

particle, a correlated state of the property will appear on the other particle. Quantum Teleportation uses entanglement for communication via a classical information channel.

BB84 Protocol Explanation

For the BB84 protocol, we define polarization of 0° on the rectilinear basis or 45° on the diagonal basis as binary 0. Similarly, a binary 1 an be 90° on a rectilinear basis and 135° on a diagonal basis.



Bits are encoded in the polarization state of a photon.

In the first step, Alice and Bob communicate over a Quantum Channel. Alice randomly selects a string of bits and a string of bases (rectilinear or diagonal) of equal length. Then she transmits a photon for each bit with the corresponding polarization through an optical fiber (or other channels that allows sending photons) to Bob.

Bob randomly chooses a basis for each photon to measure its polarization. If Bob selects the same basis as Alice for a particular photon, he will correctly find the bit Alice wanted to share as he measured the same polarization. If he doesn't guess correctly, he will get a random bit.

Alice and Bob communicate over a classical public channel in the second step. Bob tells Alice the bases he used to measure each photon. Alice informs Bob of the bases he guessed correctly to measure the encoded bits. After that, Alice and Bob remove the encoded and measured bits on different bases. Now, Alice and Bob have an identical bit-string, the **shifted key**.

Alice's bit-string	1	0	0	1	1	0	1	0	0	1
Alice's encoding basis	+	×	×	+	×	+	+	+	+	+
Alice's polarization	V	D	D	V	A	H	H	H	H	H
Bob's measurement basis	+	+	×	+	+	×	+	+	+	×
Bob's polarization	V	V	D	V	H	A	H	H	H	D
Shifted Key	1	1	1	1	0	1	0	0	0	0

BB84 protocol up to this point

To check the presence of Eve, Alice and Bob can share a few bits from the shifted key, which are supposed to be the same. Any disagreement in the compared bits will expose the presence of Eve.

Let's look at an example where Eve managed to intercept some of the photons used in the quantum channel.

Alice's bit-string	1	0	0	1	1	0	1	0	0	1
Alice's encoding basis	+	×	×	+	×	+	+	+	+	+
Alice's polarization	V	D	D	V	A	H	H	H	H	H
Eve's measurement basis	×	×	+	×	+	+	×	+	×	+
Eve's polarization	D	D	V	A	V	H	D	H	A	V
Bob's measurement basis	+	+	×	+	+	×	+	+	+	×
Bob's polarization	H	H	A	H	V	D	H	H	V	D
Shifted Key	0	1	1	0	1	0	0	0	1	0

BB84 protocol when Eve interferes with some photons

Due to the presence of Eve, despite having six identical bases, only one of Alice's and Bob's bits match. Which revealed the presence of Eve in the channel. In this case, Alice and Bob will have to transmit the photons again using another Quantum Channel.

Eve's Escape Probability

Eve has no way to know the bases Alice used to encode the bits before Alice reveals her coding bases in the classical channel. So, Eve needs to guess the bases to measure the photons. If she measures incorrectly, information encoded on the other bases will be lost. Again Eve cannot replicate the states of the intercepted photons before sending them to Bob. Based on probability, if Eve eavesdrops on **n** bits, she will go undetected **(3/4)^n** times. In our case of 10 bits, Eve's escape probability is 0.0563, which is very small.

Key Distribution: B92

INTRODUCTION

Quantum key distribution protocol B92, proposed by Charles Bennett in 1992, makes it possible for two entities, the Sender and the Receiver, to establish a perfectly secret, common and unique key sequence using polarized photons – qbits, and also can detect the Eavesdropper that intercepted the quantum channel.

The unconditional security of the B92 quantum key distribution system, has been demonstrated only for mathematical models. In practice, this unconditional security cannot be achieved due to the technical imperfections of the devices, used for polarization or the

reading of polarization of the photons, involved in the exchange of quantum keys.

The security of the quantum key distribution systems is also given by the effectiveness of the method of detecting possible attacks.

There are also several methods of detecting attacks on quantum key distribution systems, but the most reliable is the Quantum Bit Travel Time (QBTT) detection method.

B92 QKD PROTOCOL – ESSENTIALS

In B92 quantum key distribution system, Sender will encode classical bits in qbits polarized in two non-orthogonal states, figure 1 and Receiver will measure the qbits, in order to decode the bits, in all four states used in BB84 protocol, figure 2 and figure 3.

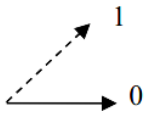


Fig. 1 – *Sender's* nonorthogonal polarization states

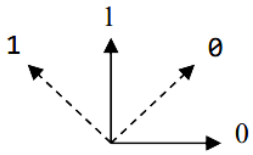


Fig. 2 – *Receiver's* measurement states

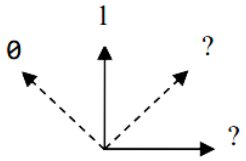


Fig. 3 – *Receiver's* interpretation states

According to the laws of quantum mechanics, no type of measurement can distinguish between two polarized photons in non-orthogonal bases, as a result the corresponding bits cannot be identified with certainty. On the other hand, any attempt to intercept the transmitted qbits will alert the two communicating parties.

To implement the B92 quantum key distribution system, the Sender and Receiver will use for the bit coding respectively for photon reading the convention set out in the table 1.

Table 1. Polarization states for *Sender* and *Receiver*

Sender		
Base	L	D
State	0°	45°
Qbit	→	↗
Bit	0	1

Receiver				
Base	L	D	L	D
State	0°	45°	90°	135°
Qbit	→	↗	↑	↖
Result	0	0	1	1
Bit	?	?	1	0

Steps of the B92 protocol:

1. Sender create a random bit string noted s.

2. Sender, use polarization states (0o, 45o) to represent bits in s.

3. Sender, using a special equipment, creates a sequence p of polarized photons – qbits, according to table 1.

4. Sender sends the qbits p to Receiver over the quantum channel.

5. Receiver, for each received qbit, randomly chooses a polarization base (linear "L" or diagonal "D").

6. Receiver, using a special equipment, measures each received qbit with respect to the basis chosen in step 5. According to table 1 for each qbit detected as a ‘0’ announce the Sender and eliminate it from s'.

7. If Receiver detects ‘0’ then s' =?

If Receiver detects ‘1’ then s' = 0 if b' = L or s' = 1 if b' = R

8. Sender eliminate from s the corresponding bit where the Receiver detected ‘0’.

IMPLEMENTATION OF B92 PROTOCOL WITHOUT EAVESDROPPER:

For the software simulation of B92 quantum key distribution protocol without eavesdropper, the Sender and the Receiver will communicate through different TCP/IP ports and sockets, via a switch, that will simulate the quantum and classical channel. This software application consists of 4 objects: Sender, Receiver, Quantum Channel and Classic Channel. At the end of the quantum transmission, the Sender and the Receiver will communicate through the classical channel and execute the steps: Detecting Eavesdropper presence, Secret key reconciliation and Privacy amplification.

HARDWARE SETUP:

Block diagram of B92 protocol without *Eavesdropper* implementation is presented in figure 4.

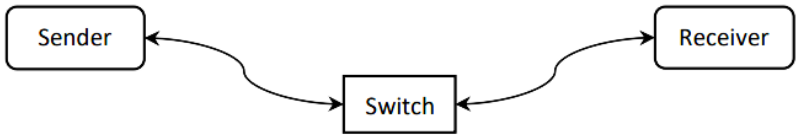


Fig. 4 – Hardware implementation of B92 protocol without Eavesdropper

To implement the B92 protocol without Eavesdropper we used: 2 workstations and 1 switch or router. Each workstation represents the Sender and the Receiver. Static IP are used so that workstations can communicate through the switch. Specific simulation software is installed on each workstation.

For this simulation, each of object *(Sender, Receiver, Quantum Channel* and *Classic Channel)* play different role, as shown in figure 5.

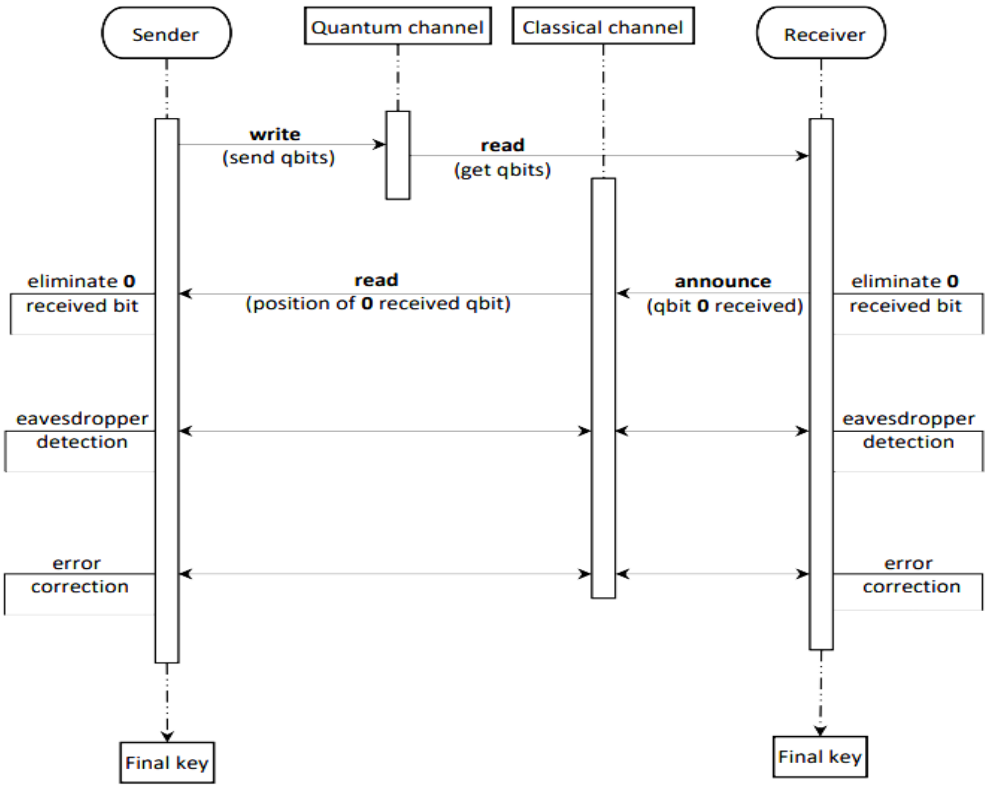


Fig. 5 – Software protocol of B92 without eavesdropper

Quantum Key Distribution: E-91.

The E-91 principle was proposed by Arthur Ekert in 1991, which uses the Bell states emitted by a common source, distributed between Alice and Bob, who then use the randomly chosen polarization bases. Then Alice interprets H, D states as 0 and V, A states as 1. Then Bob should do the opposite to obtain the same key if the state $|\Psi(-)\rangle$ is used.

The important principle on which QKD is based is the principle of quantum entanglement. Two particles can become entangled such that when a particular property is measured in one particle, the opposite state will be observed on the entangled particle instantaneously. This is true regardless of the distance between the entangled particles. It is impossible, however, to predict before measurement what state will be observed thus it is not possible to communicate via entangled particles without discussing the observations over a classical channel. The process of communicating using entangled states, aided by a classical information channel, is known as quantum teleportation and is the basis of Ekert's protocol.

The following steps give the procedure for the Quantum E-91 protocol:

1. The source center chooses the EPR pair(Entangled Bell State) $|\varphi+\rangle=(1/\sqrt{2})(|00\rangle+|11\rangle)$, sends the first particle $|\varphi+\rangle_1$ to Alice, and the second particle $|\varphi+\rangle_2$ to Bob.
2. Alice measures with a direction randomly chosen between {0, π/8, π/4}, whereas Bob measures with a direction randomly chosen between {−π/8, 0, π/8}. They record the measurement

result and broadcast the measurement basis which they used, through the classical channel.

3. Thus, Alice and Bob now know each other's choice. They divide the measurement result into two groups: one is the decoy qubits G_1 where they choose different measurement basis and another is the raw key qubits G_2 where they choose the same measurement basis.
4. The group G_1 is used to detect whether there is eavesdropping. To detect eavesdropping, they can compute the test statistic *S* using the correlation coefficients between Alice's bases and Bob's. If there is an error in the value of *S,* which means that there is also an eavesdropper, Alice and Bob will conclude that the quantum channel is not safe and they will interrupt this communication and start a new one.
5. If the quantum channel is safe, G_2 can be used as the raw keys because Alice and Bob can receive the same measurements. Both Alice and Bob agree that the measurement $|0\rangle$ represents the classical bit O,

while the measurement |1⟩ represents the classical bit 1, and thus get their key string.

There are many other modern and more advanced protocols today as well but the E-91 protocol is one of the most fundamental protocols that define the basis of Quantum Key Distribution.

Quantum Cryptography is a new revolution in the world of secure communication and as the research continues, the day is not very far when we will be successful in using it for highly secure communication.

State of the Quantum computation Technology

- Although Quantum computers have yet to demonstrate their advantage, the hardware development is steadily progressing to the point where organizations can experiment with it through the cloud.
- With multiple technology pathways developing in parallel, an exciting period of steady technology advances is beginning with tangible roadmaps to track progress and align industry uptake.
- Two approaches to build a Quantum computer - superconducting qubits and trapped ions have currently reached a more advanced level of development than others, though it is likely

that multiple hardware platforms will be able to either catch up or otherwise play a role in the future.

- Even though today's imperfect quantum computers have not yet demonstrated a quantum advantage and cannot run many promising industry applications, they can already be accessed for research, pilots and business use case assessments.
- Invent the high physical infrastructure requirements to create environments in which quantum computers operate, most users will get access to the technology via the cloud, and likely paired with other traditional cloud computing services.

Current issues plaguing the progress

1. **High-quality qubits:**

We need to make qubits that we will be able to generate useful instructions or gate operations for on a large scale.The current qubit system generates errors when running operations between two qubits at a rate that is far higher than what we would need to effectively compute. After a certain number of instructions or operations, today's qubits produce the

wrong answer when we run calculations. The result we get can be indistinguishable from noise.

2. **Interconnect technology for quantum computers:**

How to scale up the number of qubits within a quantum chip. Today, we require multiple control wires, or multiple lasers, to create each qubit.
It is difficult to believe that we could build a million-qubit chip with many millions of wires connecting to the circuit board or coming out of the cryogenic measurement chamber.

3. **Fast qubit control and feedback loops**

In order to implement complex algorithms, including error correction schemes, we need to prove that we can control multiple qubits. That control must have low-latency—on the order of 10's of nanoseconds.

4. **Error correction:**

We need to implement error correction algorithms that check and then correct for random qubit errors as they occur.These are complex instruction sets that use many physical qubits to effectively extend the lifetime of the information in the system. Error correction has not yet been proven at scale for quantum

computing, but it is a priority area of our research and one that is a prerequisite to a full-scale commercial quantum system.

Advantages of Quantum Cryptography:

1. Virtually Un-hackable
2. Simple to use
3. Offers multiple methods for security – there are numerous quantum cryptography protocols used. Like QKD, quantum-coin flipping, position-based quantum cryptography, device-independent quantum cryptography, etc., Moreover these protocols can be combined with classical methods to enhance the implementation of these protocols

Note:

- High-bit rate QKD system was created by The University of Cambridge and Toshiba Corp. using the BB84 quantum cryptography protocol.
- Several commercial companies like Toshiba, ID Quantique, Quintessence, MagiQ Technologies Inc., also developed commercial QKD systems.

4. Less resource needed to maintain it
5. Used to detect eavesdropping in quantum key distribution – on reading of data by third party, quantum state changes thus modifying the expected outcome for the users
6. Provide secure communication – as it is based on laws of physics it is more sophisticated and secure method of encryption

7. People believe in it. Thus, various projects have been done on it. Moreover, many prestigious institutions are investing both in terms of manpower and wealth on it

Disadvantages of Quantum Cryptography:

1. The signal is currently limited to 90 miles
2. Expense – requires its own infrastructure, using fibre optic lines and repeaters
3. Could replace a lot of jobs
4. Range – maximum range is less except in Terra Quantum (40,000 km)
5. Changes in polarization and error rates - change in photons during polarization in transmit, which is proportional to increase in error rates
6. Number of Destinations – keys cannot be sent to two or more locations
7. It will take time for its full deployment and replacement

Conclusion:

1. Quantum Cryptography promises to revolutionize secure communication by providing security based on the fundamental laws of physics, instead of the current state of mathematical algorithms or computing technology.
2. The devices for implementing such methods exist and the performance of demonstration systems is being continuously improved.

3. Within the next few years, if not months, such systems could start encrypting some of the most valuable secrets of government and industry.
4. Quantum Computers are in early phases and need more developments which in time will simultaneously decrease disadvantages and increase advantages.
5. Quantum Cryptography Field with several limitations and disadvantages still it is steadily growing.

6. As traditional cryptography is based on mathematics, quantum cryptography is based on laws of physics thus making it more difficult to decrypt and its potential can be increased by clubbing it with traditional systems.
7. People believe in it but it will take around 20 years or more for its full deployment and in replacing it with traditional technologies that is 2040s and so on can be the era of Quantum, where it can dominate all the classical technologies available in the world.
8. While the capabilities that Quantum Cryptography offer are powerful, a hybrid solution will likely be the best approach.
9. For short term, Post-Quantum Cryptography looks more promising as a widely deployed solution.