Quantum Key Distribution using BB84

Jay Patel	202003019
Piyush Parmar	202003038
Aditya Shah	202003045

Why we need a Quantum Cryptographic protocol ?

- Traditional cryptographic protocols are based on mathematical problems such as integer factorization, which are believed to be difficult to solve for classical computers, but quantum computers could potentially solve these problems using algorithms like Shor's algorithm.

- Quantum cryptographic protocols are based on the laws of quantum mechanics, which are different from the laws of classical physics.

Quantum Key Distribution

- Quantum key distribution (QKD) is a quantum cryptographic protocol that allows two parties to establish a shared secret key over an insecure channel, such as the public internet. The security of QKD is based on the laws of quantum mechanics, and it is believed to be secure against attack by quantum computers.

- BB84 is a protocol that allows us to perform QKD.

OTP (One Time Pad)

- (Classically) Used a stack of small very thin pages, each with a series or random numbers on them. After use, a page would be destroyed immediately.
- The Encryption-key has at least the same length as the plaintext and consists of truly random numbers(not auto-generated).
- Alice will take the XOR of OTP(key) and plaintext, this will generate a ciphertext which she will send to Bob.
- This ciphertext that has no relation with the plaintext when the key is unknown(for eavesdropper). At the receiving end, the same OTP is used to retrieve the original plaintext.

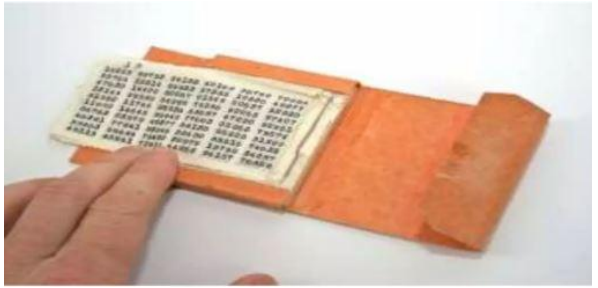


Figure : Classical OTP

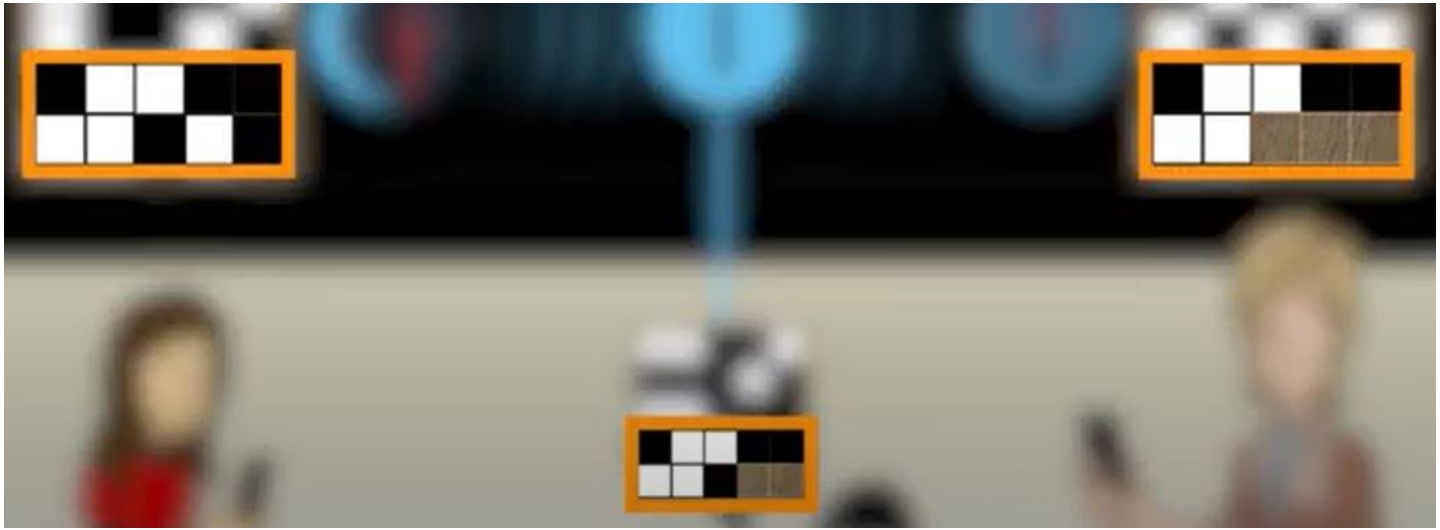
BB84

BB84 is a QKD protocol developed by Charles Bennett and Gilles Brassard in 1984. It is the first quantum cryptography protocol. The protocol uses the principles of quantum mechanics to generate a shared secret key between two parties. The key can then be used to encrypt and decrypt messages between the two parties. The protocol is resistant to attacks by eavesdroppers.

The protocol is provably secure, relying on two conditions:

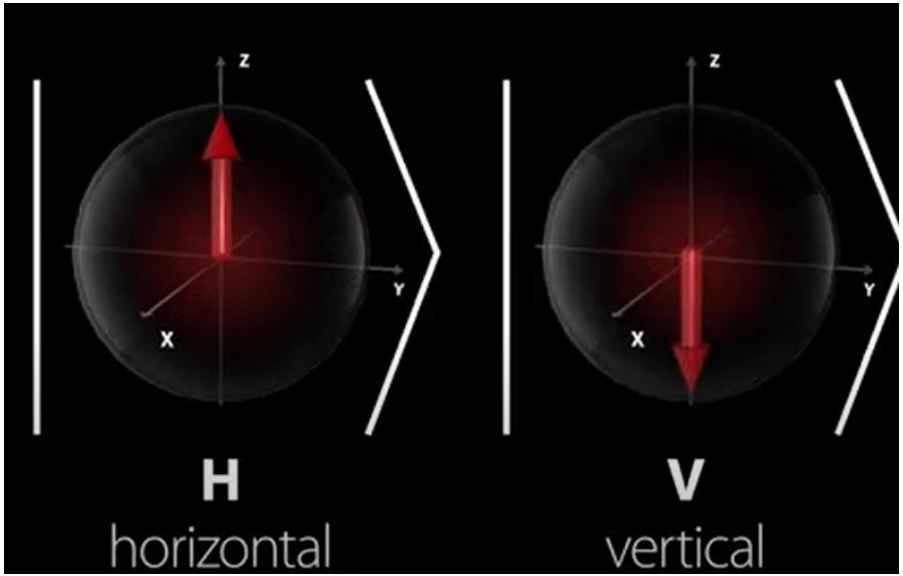
- **No Cloning Theorem:** It is impossible to create identical copies of an unknown quantum state.
- The existence of an authenticated public classical channel.


BB84-protocol
H - - V V
H + - V +
H V + + -
V H + H V
H V + V +
H - V + V
H V - +



Photons as Qubits

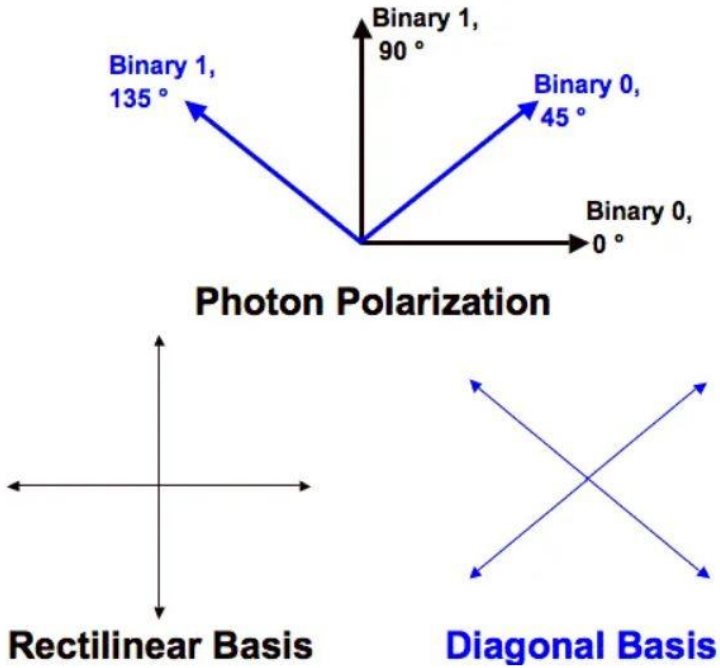
- Photons have quantum properties and can be transmitted through fiber optics and, therefore, can be used to encode the secret key.
- Photons are qubits for their state of polarization. A light wave is an electromagnetic wave where the plane occupied by the electric field is perpendicular to the plane occupied by the magnetic field. And the direction of propagation of the wave is orthogonal to these two planes.
- When a light wave is polarized, it oscillates on a single plane. We can use polarizers and wave plates like half-wave plates and quarter-wave plates to polarize light.



- We will take 2 polarization basis: rectilinear and diagonal. Again Rectilinear polarization will have 2 states: horizontal(H) and vertical(V). And Diagonal polarization is also of two kinds: diagonal(D) and anti-diagonal(A).
- The two states of rectilinear polarization, horizontal and vertical, are represented as $|H\rangle$ and $|V\rangle$. The two states of diagonal polarization, diagonal and anti-diagonal, are described as $|D\rangle$ and $|A\rangle$.
- Now, we can consider $|H\rangle$ and $|V\rangle$ as $|0\rangle$ and $|1\rangle$ on the Z-axis and $|D\rangle$ and $|A\rangle$ as $|+\rangle$ and $|-\rangle$ along the X-axis.

Axis Notations

For the BB84 protocol, we define polarization of 0° (H) on the rectilinear basis or 45° (D) on the diagonal basis as binary 0. Similarly, a binary 1 can be 90° (V) on a rectilinear basis and 135° (A) on a diagonal basis.



BB84 protocol

- 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.
- In first step, Alice 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.
- In second step, Alice and Bob communicate over a classical public channel. 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.

Bit Value	Alice Basis	Alice State	Bob Basis	Bob State	Measured Bit
0	+	H	+	H	0
0	+	H	x	D or A	0 or 1
0	x	D	+	H or V	0 or 1
0	x	D	x	D	0
1	+	V	+	V	1
1	+	V	x	D or A	0 or 1
1	x	A	+	H or V	0 or 1
1	x	A	x	A	1

Bit Value	Alice Basis	Alice State	Eve Basis	Eve State	Bob Basis	Bob State	Measured Bit
0	+	H	+	H	+	H	0
0	+	H	+	H	x	D or A	0 or 1
0	+	H	x	D or A	+	H or V	0 or 1
0	+	H	x	D or A	x	D - A	0 - 1
0	x	D	+	H or V	+	H - V	0 - 1
0	x	D	+	H or V	x	D or A	0 or 1
0	x	D	x	D	+	H or V	0 or 1
0	x	D	x	D	x	D	0

Bit Value	Alice Basis	Alice State	Eve Basis	Eve State	Bob Basis	Bob State	Measured Bit
1	+	V	+	V	+	V	1
1	+	V	+	V	x	D or A	0 or 1
1	+	V	x	D or A	+	H or V	0 or 1
1	+	V	x	D or A	x	D - A	0 - 1
1	x	A	+	H or V	+	H - V	0 - 1
1	x	A	+	H or V	x	D or A	0 or 1
1	x	A	x	A	+	H or V	0 or 1
1	x	A	x	A	x	A	0

Examples

Bit Value	Alice Basis	Alice State	Bob Basis	Bob State	Measured Bit
1	+	V	+	V	1
0	x	D	+	V	1
0	x	D	x	D	1
1	+	V	+	V	1
1	x	A	+	H	0
0	+	H	x	A	1
1	+	H	+	H	0
0	+	H	+	H	0

Bit Value	Alice Basis	Alice State	Eve Basis	Eve State	Bob Basis	Bob State	Measured Bit
1	+	V	x	D	+	H	0
0	x	D	x	D	+	H	1
0	x	D	+	V	x	A	1
1	+	V	x	A	+	H	0
1	x	A	+	V	+	V	1
0	+	H	+	H	x	D	0
1	+	H	x	D	+	H	0
0	+	H	+	H	+	H	0

Presence of Eve

- 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.

- As shown in the above example, due to the presence of Eve, despite having five 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.

Escape Probability

- If the length of the string of bits sent by Alice is n. Then n/2 bits will get discarded due to the basis mismatch of Alice and Bob.
    - **If Eve is present** then out of the remaining n/2 bits nearly half of them means n/4 will be correct and the others will be incorrect
    - **Else** then all the remaining n/2 bits will be correct
- So on an average the escape probability(probability of not getting detected) of eve for each individual bit is (1 - 1/4) = 3/4. Therefore for n bits the escape probability of eve would be $(3/4)^n$
- In above example there are 8 bits therefore the escape probability is roughly $(3/4)^8$ = 0.1001

Weaknesses of Quantum Cryptography

- Quantum Cryptography is not perfectly secured when used with faulty equipment and in a noisy environment (which may lead to bit-flip, phase errors, or measurement errors).
- In practical implementations of quantum key distribution protocols, such as BB84, hardware limitations prevent the perfect generation and detection of single photons. As a result, coherent light sources, such as lasers, are often used instead.
- The use of coherent light sources introduces vulnerabilities, such as the Photon Number Splitting (PNS) attack. In a PNS attack, Eve intercepts a small number of photons from each bit-transmission for measurement while allowing the remaining photons to continue to Bob. This enables Eve to measure the intercepted photons without disturbing Bob's photon measurement, potentially compromising the security of the key exchange.
- Can be prevented by decoy-state technique (Alice transmits each qubit with random intensity.Alice announces intensity level publicly.Bob can detect PNS attack by monitoring the bit error rate(Associated with each intensity level).

Code Link

https://colab.research.google.com/drive/1KH1b9UgzA2RMdnWwZvQDJ4XHEwpHTKBv?usp=sharing