**Quantum Cryptography**

In the modern internet world, sharing of data is very much common and essential. Sharing of important data in a secure way is very much essential. This modern world is full of advantageous technological improvements but it is also equally very unsecure to transfer data and information to others. This is where the traditional cryptography comes in handy!

**Cryptography**

Cryptography is the process of encrypting data, or converting plain text into scrambled text so that only someone who has the right “key” can read it. This traditional cryptography uses mathematical algorithms to encrypt and decrypt data accordingly, which takes millions of years to find the right key when trying to hack.

This is more useful, till the invention of “Quantum Computing”.

As per google, quantum computing is referred to a field of computer science that uses quantum physics to solve complex problems faster than classical computers.

These quantum computers use “Qubits” rather than the “Bits” which is 0’s and 1’s.

Qubits are the fundamental building blocks of quantum computing. They can exist in multiple states at once (**superposition**) and can be interconnected (**entangled**), allowing quantum computers to perform complex calculations much faster than classical computers.

“The researchers came up with a new idea of cryptography, the one that’s not just hard to break but impossible to break” which is Quantum Cryptography.

To know about the quantum cryptography, we should be familiar with the quantum mechanics and its 4 basic principles.

**Quantum mechanics**

Quantum mechanics is the study of how tiny things, like atoms and smaller particles, behave. These particles don’t follow the normal rules of the world we see every day, and they do some really strange things. The main idea of the quantum cryptography is started with the photons which has special property called the “SPIN”. They tend to spin in multiple directions while transferred in a filter known as beam splitters.

**Polarized photon**

When light is polarized, its waves are restricted to oscillating in a specific direction. For instance, if light is polarized vertically, its electric field oscillates up and down. If it’s polarized horizontally, the oscillation is side to side.

**Quantum Cryptography**

Quantum cryptography, by extension, simply uses the principles of quantum mechanics to encrypt data and transmit it in a way that cannot be hacked.

The main idea is emerged from the singe principle “Heisenberg’s Uncertainty Principle” which states that, you can’t know absolutely everything about the state of quantum particle. It’s not because you’re not smart enough or your equipment is not good enough, it’s just because the nature keeps something hidden.

While the definition sounds simple, the complexity lies in the principles of quantum mechanics behind quantum cryptography.

**Principle of quantum mechanics**

* The particles that make up the universe are inherently uncertain and can simultaneously exist in more than one place or more than one state of being.
* Photons are generated randomly in one of two quantum states.
* You can’t measure a quantum property without changing or disturbing it.
* You can clone some quantum properties of a particle, but not the whole particle.

**Working of Quantum Cryptography**

With Quantum cryptography, the key is the stream of photons. photons which has special property called the “SPIN”. They tend to spin in multiple directions while transferred in a filter known as beam splitters.



We have 4 filters:

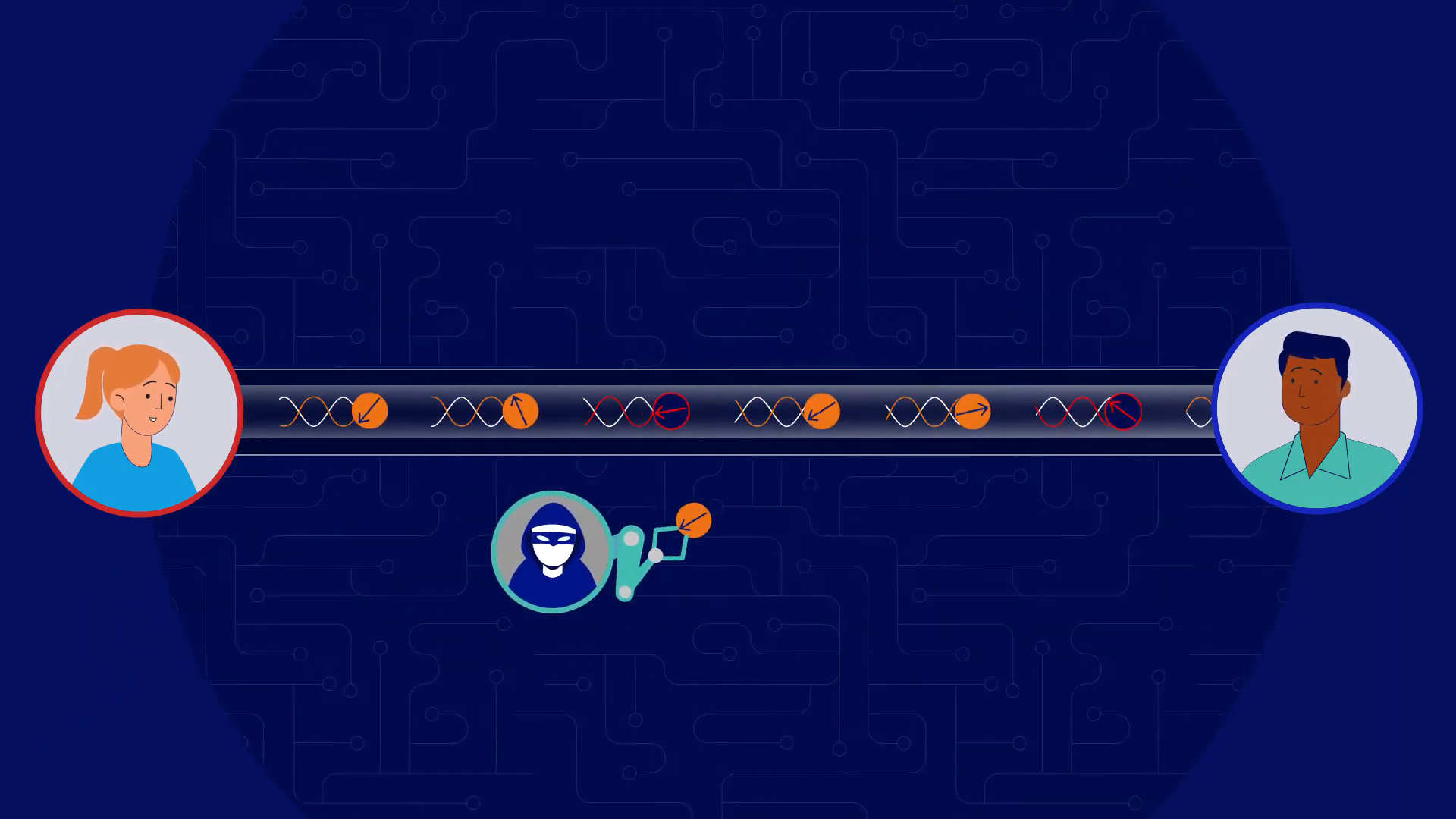
1. Vertical
2. Horizontal
3. Diagonal right
4. Diagonal left

The Vertical and Diagonal right specify the bit 1.

The Horizontal and Diagonal left specify the bit 0.

When Alice sends a stream of photons to Bob, Alice uses the 4 filters interchangeably letting the photon pass through the filter and change its direction, vertical, horizontal, etc. this switching between filters is random and it is according to the Alice mindset.

Eve a hacker if want to know the key, the only way eve can measure the photon’s spin is by passing it through the filter. But Eve don’t know which filter is used by Alice to send the photon, Alice can use either of the 4 filters, if Eve places a wrong filter Eve may receive a wrong bit.



As per the principles of quantum mechanics, when the hacker retrieves the information encoded into a photon, he or she irreversibly change their properties because quantum states cannot be cloned or copied.

Now there will be a major problem “how come Bob receives the key?”, the researchers think a lot about the problem and finally found a solution.

Bob has the beam splitter and receives all the beam of photons passing by it. Bob has to communicate with Alice and they both want to compare the filters they use. if both the filters of Alice and Bob matches it is marked and unmatched one are discarded. The marked ones are the key.

If Eve sits in the middle of the comparison she can’t find the key, say Alice and Bob uses a Vertical filter for first photon and Eve uses the Horizontal filter it is wrong for Eve, Alice and Bob keeps the digit, if Alice and Eve uses a Horizontal filter for second photon and Bob uses the Diagonal filter, Alice and Bob discards the digits and again Eve is mistaken.

