Quantum Cryptography

Saturday, 16 April 2022 2:08 PM

Quantum Computers:
- A computer that can perform very fast calculations;
- It can perform calculations that are based on probability rather than simple 0 and 1 bit values.
- This gives a quatum computer the potential to process considerably more data than existing computers in very less time.

Quantum Cryptography:
- It exploits the laws of quantum mechanics to improve on the security of data.
- It is based on the use of light particles; photons. and their physical quantum properties to produce a virtually unbreakable encryption system for data transmitted over fibre optic lines.
- This technology is based on laws of physics, rather than mathematics.

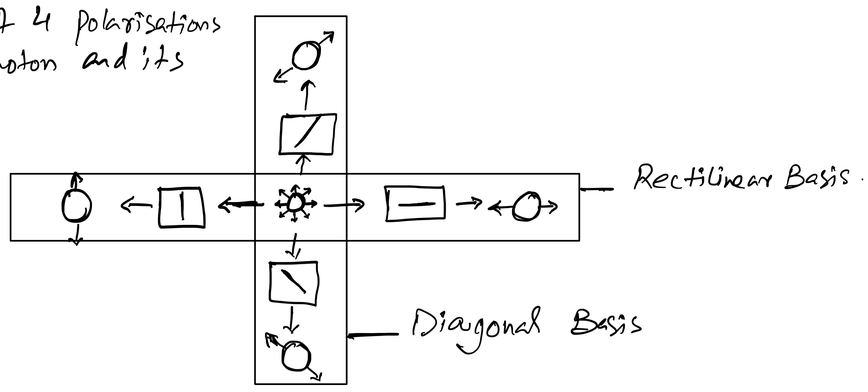
One of the uses of quatum cryptography is when sending encryption keys across a network. This uses Quantum Key Distribution (QKD) protocol. We will study with reference to most common BB84 algo.

QKD uses quantum mechanics to ensure a secure transmission of encryption keys. They use a Qubit (Quantum Bit), which is basic unit of quantum data. Unlike normal binary, the state of Qubit is both 0 and 1 until the photon is measured using basis.

A photon spins (vibrates/oscillates) in all directions. We use polarisation to restrict these vibrations to particular directions.

Photon oscillating in its various directions.

Effects of 4 polarisations on a photon and its results.



★ HOW DO WE USE QUANTUM CRYTOGRAPHY TO SEND AN ENCRYPTION KEY:

- Photons can be polarised in one of two bases - rectilinear or diagonal
- In rectilinear basis, 1 can be represented by ↕ and 0 by ↔. In diagonal basis 1 is ↗ and 0 is ↖.
- A photon that is polarised in rectilinear basis will always give the same result when measured in rectilinear basis and same is true for diagonal basis.
- However if a photon is polarised in rectilinear basis but measured in diagonal basis then information the original polarisation is changed/lost.
- The result of the measurement has a 50-50 chance of being correct.
- This state of photon having both 1 and 0 states at the same time tells receiver nothing about original polarisation.
- So,
  1. The sender polarises each photon using randomly selected basis
  2. The receiver measures each phon using randomly selected basis.
  3. The receiver shares his basis with sender publically.
- Only when the sender and receiver use the same basis for measurement can they be sure that are both reading as 0 or 1. When they used the same basis the receiver knows they have measured Qubits correct.