QUANTUM CRYPTOGRAPHY

Cryptography is the process of encrypting and protecting data so that only the person who has the right secret key can decrypt it. Quantum cryptography is different from traditional cryptographic systems in that it relies on physics, rather than mathematics, as the key aspect of its security model.

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.

HISTORY

FROM THE BEGINNING : -

At the early stage of Quantum Cryptography , when quantum signal was used to encode the transmitter's confidential message in such a way that the receiver could decode it, if there is no eavesdropper. But in the presence of an eavesdropper, if the eavesdropper attempted to intercept the messages , then the message was spoiled and no information was leaked.

DISADVANTAGE :

(i) At the early stage of Quantum Cryptography it may look like that it is safe , but in reality there are many disadvantages like delay of time increases . If the message was spoiled then the sender have to send the message again and that may take a long time.

(ii) The process was unidirectional and it required legitimate parties to share a secret key, much as in a one time pad encryption.

(iii) The One time pad encryption can be used over and over again if no eavesdropping are detected but if eavesdropping are detected then it will be no longer used for.

To avoid the disadvantages , another theory was arrived. It would be easier to use the quantum channel to transmit an arbitrarily long random secret key. If eavesdropping were detected on the quantum channel, due to unavoidable disturbance, the key would be thrown away ; otherwise it could be used safely to transmit a sensitive message by use of the classical one-time pad scheme. (BB84 PROTOCOL)

DISADVANTAGES : -

(i) Quantum channels are susceptible to various types of noise and errors. Quantum states can be lost or corrupted during transmission.

(ii) Quantum channel has finite range due to phenomena like quantum decoherence and absorption. If the distance between sender and receiver increases , the probability of successfully transmitting quantum states decreases.

(iii) The rate at which secure bits can be generated over a Quantum channel is limited.

The previous two theory was rejected because of their major disadvantages . But in the early time of 1990's , Quantum key was discovered . After that some theory was revealed and became more feasible because entanglement-based cryptography provided a form of Quantum Key Distribution that would remain secure not only against eavesdropping , but also against burglary.

SECRET KEY : - In classical cryptography a secret key is a random string of bits used to encrypt and decrypt messages using classical encryption algorithms.

QUANTUM KEY : - In quantum cryptography a quantum key is a sequence of quantum states (usually photons) prepared in specific quantum states, like polarized photons or qubits.

EVOLUTION OF QUANTUM COMPUTING

Before we proceed towards deep in Quantum Cryptography , we have to know about Quantum Computing a little bit. Quantum Computing is at the initial stage of technology evolution but has a high potential of generating innovations in quantum communications, quantum cryptography, quantum optics etc. to support competitive advantage of firms and nations. As we all know that the evolution of technologies is driven by science, increases based on the interaction between technologies and scientific fields that generate co-evolutionary pathways of new technological trajectories.

THEORETICAL FRAMEWORK

The theoretical framework of quantum computing is based on principles from quantum mechanics and information theory. There are some key elements which are mentioned by the scientists and developers to understand Quantum Computing.

Quantum Bits (Qubits): Quantum bits, or qubits, are the fundamental units of quantum information. Unlike classical bits, which can represent either a 0 or a 1, qubits can exist in a superposition of states. This means that a qubit can represent both 0 and 1 simultaneously, with varying probabilities. Superposition is a crucial property that enables quantum computers to perform certain computations much faster than classical computers.

Entanglement: Entanglement is another unique property of quantum systems. When two qubits become entangled, the state of one qubit becomes dependent on the state of the other, regardless of the distance between them. This phenomenon allows for the creation of quantum gates that can perform operations on multiple qubits simultaneously, leading to the potential for massively parallel computation.

Quantum Gates: Quantum gates are the quantum analogs of classical logic gates. They are used to manipulate qubits, change their states, and perform computations. Common quantum gates include the Hadamard gate, CNOT gate (controlled-NOT), and Toffoli gate, among others. These gates are responsible for creating quantum circuits to execute quantum algorithms.

Quantum Algorithms: Quantum computing is best known for its potential to solve certain problems exponentially faster than classical computers. Shor's algorithm, for example, can factor large numbers efficiently, threatening current encryption methods, while Grover's algorithm can perform database search tasks faster. Other algorithms, like those for quantum simulations and optimization, also show promise in various fields.

Quantum Superposition: Superposition allows qubits to be in multiple states at the same time. This property is exploited in quantum algorithms to explore multiple possibilities simultaneously. Quantum algorithms often use superposition to speed up certain types of calculations, like factoring large numbers or searching unsorted databases.

Quantum Measurement: Measurement in quantum computing collapses the superposition of qubit states into a definite classical state. The outcome of a measurement is probabilistic, and the probability of a specific measurement result is determined by the coefficients in the superposition.