SELECTION OF MASTER STATION AND SYNCHRONIZATION OF TRANSMISSION IN QUANTUM CRYPTOGRAPHY: A NOVEL APPROACH

MOLOY DHAR, SANDIP TIGGA, SOURISH MITRA & SAYANI CHANDRA

Guru Nanak Institute of Technology, Panihati, Kolkata, West Bengal, India

ABSTRACT

Two parties can communicate in secret if they already share a sufficient quantity of secret information. The problem then is how to distribute this secret information or key. Quantum cryptography provides the potential to ensure the security of the process of key distribution and hence to guarantee the covert nature of the communication. Quantum key distribution (QKD) uses quantum mechanics to guarantee secure communication. It enables two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages. Classical Cryptographic communication system is a secret communication that can only take place after a key is communicated in secret over a totally secure communication channel. Most widely used is the BB84 Protocol which was developed by IBM. In this paper takes advantage of Heisenberg's principle in which measuring a quantum system disturbs it and yields incomplete information i.e. quantum key distribution which takes advantage of certain phenomena that occur at the subatomic level, so that any attempt by an enemy to obtain the bits in a key not only fails, but gets detected as well. In this paper, the intention was to propose the idea of an algorithm that can realize a quantum transmission between two computers. This algorithm, based on the result of the Secret Key conciliation process proposed by Bennett and Brassard on 1984 (BB84), can assure a high security communication between two users. The master station selection and its synchronized transmission oriented approach intend to be a quantum network algorithm that can realize a quantum connection between two computers.

KEYWORDS: Quantum Key Distribution, Quantum Cryptography, Quantum Connection, Secret Key Reconciliation, Synchronized Transmission