Abstract

Quantum Cryptography allows us to do secure communication by exploiting the properties of quantum mechanics. The basic idea behind the security of quantum cryptography comes from no-cloning theorem. Whenever an eavesdropper tries to gain information by attacking the quantum channel, one would end up disturbing the state. The communicating parties can easily detect this error by introducing some check bits.

There are various applications of Quantum Cryptography, such as, Quantum Key Distribution (QKD), Quantum Coin Flipping, Quantum Private Comparison (QPC), Quantum Voting, etc. Here, we analyze the security of specifically QKD and QPC.

To render the security of our Quantum Cryptographic protocols, high fidelity of shared quantum states is required. But in real world, quantum channels can be noisy (in addition to the noise caused due to eavesdropping). Quantum Error-Correction allows us to overcome the effects of noise and achieve very high fidelities, given the error rate is below a certain threshold.

We first develop the formalism of error-correction, starting from classical linear codes; the properties of which are exploited in several Quantum Error-Correcting codes. We look at a particular class of such codes, known as CSS Codes; which we then use to prove the security of BB84 QKD Protocol. Some QPC protocols under noiseless, as well as, noisy conditions, are discussed. We then propose a three-party entangled state QPC Protocol which uses CSS Codes to encode our state, and is unconditionally secure.