Implemetation of BB84 quantum key distribution protocol's with attacks.

ABSTRACT

Quantum cryptography is basically based on a trusted channel in communication between two parties compared to classical channel. Recently, Quantum Key Distribution (QKD has become more secure transmission method used to transmit secret key between two legitimate parties. This paper discusses the implementation of QKD protocol (BB84 protocol), which is widely used today. The implementation simulates the communication of two parties who wish to share a secret key with the existing of eavesdropper. The existing of eavesdropper is simulated with two kinds of attacks, which is use as parameter to measure the length of final key agreed by both authenticated parties at the end of the communication. This paper also discuss about future works to fully implement the shared secret key.

Keyword: Quantum Key Distribution; Protocol implementation; BB84 protocol; Simulate attacks, Final key.