Abstract

Is the newly born quantum cryptography the ultimate solution for information security? A technique needs to be both theoretically strong and practically viable. But quantum cryptography comes to naught in the latter. Unlike many of the classical cryptosystems in use today, whose security often draws on unproven assumptions about the computational complexity of mathematical problems, the security of quantum cryptography is based on—and employs—the laws of physics. The term “unconditional security” is used to emphasize the fact that it does not rely on the presumed, yet unproven hardness of somemathematical problem. In this Paper, we present the proof of the unconditional security of the BB84 protocol, as devised by Peter Shor and John Preskill [1].

Reference

- H. Lo and H. Chau. Unconditional security of quantum key distribution over
Key words

Qubit
Quantum Key Distribution
Security