Abstract

The last two decades have witnessed an exciting advanced research field that stems from non-classical atomic theory, the quantum mechanics. This research promises an interesting applicability in computation known as quantum computation, and also in secure data communications, known as quantum cryptography. Quantum cryptography capitalizes on the inherent random polarization state of single photons, which are associated with binary logic values. Because the polarization state of a photon is not reproducible by an eavesdropper between the source and the destination, polarized photons are used with an intelligent algorithm to disseminate the cryptographic key with high security from the source to the destination, a
To Discover Vulnerabilities of Quantum Cryptography in Secure Optical Data Transport

process known as quantum key distribution. However, although the polarization state of a photon remains intact in free-space propagation, it does not remain so in dielectric medium and thus quantum cryptography is not problem-free. In this paper we review quantum cryptography and we identify the various steps in the quantum key identification process. We then analyze and discuss issues related to quantum key distribution that rise in pragmatic fiber-optic transmission and in communication network topologies. In addition, we identify a major weakness of the method that is prone to attacking and which incapacitates quantum cryptography in fiber communications.

References

- X. Li, &quot;A quantum key distribution protocol without classical communication&quot;, quant-ph/020950, September 6, 2002.
- Q-Y. Cai, &quot;Deterministic Secure Direct Communication Using Ping-pong Protocol

**Index Terms**

Computer Science  
Security

**Keywords**