Analysis of the Robustness of Quatum Key Disnribution Protocols to Noise, Losses and Adversarial Attacks

Kaskarauov Adilet
Kazakh-British Technical University, Almaty, Kazakhstan

Abstract

The development of quantum systems leads to new challenges regarding information security mechanisms. In this regard, specialists are required to create alternative methods of information protection, especially in quantum cryptography. An important role is played by the study of the resilience of quantum key distribution (QKD) protocols. Objective: to conduct a comprehensive study of the resilience of quantum cryptographic key distribution protocols in the face of various types of attacks, noise, communication channel losses, and in the process of assessing their reliability. Methods used in the course of the research activities: theoretical analysis, modeling, simulation of attack scenarios, and experimental verification on specialized quantum simulators. The research activities were aimed at evaluating the efficiency of protocols, the error rate (QBER), the level of key secrecy, and their resilience to external influences. The research results demonstrated the impact of different types of attacks on protocol performance. It was found that the efficiency of the BB84 and CV-QKD protocols decreases with increasing noise and losses, while E91 showed higher stability. At the same time, the mechanisms of decoy states protection, privacy amplification, and error correction play an important role in enhancing resilience. The obtained results can be applied in scientific and practical research, as well as in work on the effective implementation of quantum communication systems in real-world conditions.

Keywords

BB84, noise and losses in the channel, quantum key distribution, quantum attacks.