Chapter 15
Vulnerability of the Synchronization Process in the Quantum Key Distribution System

A. P. Pljonkin
Southern Federal University, Taganrog, Russia

ABSTRACT

A typical structure of an auto-compensation system for quantum key distribution is given. The principle of operation of a fiber-optic system for the distribution of quantum keys with phase coding of photon states is described. The operation of the system in the synchronization mode and the formation of quantum keys was investigated. The process of detecting a time interval with an optical synchronization pulse is analyzed. The structural scheme of the experimental stand of the quantum-cryptographic network is given. Data are obtained that attest to the presence of a multiphoton signal during the transmission of sync pulses from the transceiver station to the coding and backward direction. The results of experimental studies are presented, which prove the existence of a vulnerability in the process of synchronization of the quantum key distribution system. It is shown that the use of a multiphoton optical pulse as a sync signal makes it possible for an attacker to unauthorized access to a quantum communication channel. The experimental results show that tapping a portion of the optical power from the quantum communication channel during the synchronization process allows an attacker to remain unnoticed while the quantum protocol is operating. Experimentally proved the possibility of introducing malfunctions into the operation of the quantum communication system at the stage of key formation, while remaining invisible for control means.

DOI: 10.4018/978-1-7998-8593-1.ch015

1. INTRODUCTION

Modern cryptographic protocols that ensure the security of transmitted messages have a high resistance to burglary. The stability of ciphers is based on mathematical formulations and the limited computing resources of the attacker. It is believed that until now the most reliable security in the transmission of messages provides the use of one-time pads. The development of symmetric methods of encryption is limited to the main problem in the transmission of confidential information, which is formulated as the problem of distributing a secret key between legitimate users.

The well-known Shannon rule, which interprets the use of a secret key for a secure transmission, is updated with the development of new technologies for the formation of secret keys. Thus, the achievement of absolute secrecy in the transmission of messages is possible only by solving the problem of key distribution.

The development of methods of quantum cryptography to ensure security in telecommunications systems of information transmission theoretically allows to achieve absolute secrecy of ciphers (Gisin et al., 2002). Quantum cryptography is based on the laws of quantum physics and is based on the coding of the quantum state of a single particle. The essence of quantum cryptography lies in the reliable distribution of the secret key between legitimate users. Another component in the quantum distribution is the creation of a random secret key (Bennet et al., 1992; Stucki et al., 2002; Broadbent & Schaffner, 2007).

Practical implementation of quantum cryptography is based on quantum key distribution systems (QKDS). If the existing encryption algorithms can be distorted by mathematical improvements, then quantum cryptography is the only way to solve the problem of key distribution. Recall that the basis of quantum cryptography lies in the following statements: it is impossible to clone an unknown quantum state and it is impossible to obtain information on non-orthogonal quantum states without perturbation. Consequently, any unauthorized measurement will lead to a change in the quantum state.

In quantum cryptography, symmetric cryptosystems are common (Makarov, 2007). In such systems, one key is used for both encryption and decryption. Messages sent along the lines of quantum communication, theoretically can't be intercepted or copied. Quantum key distribution is a technology based on the laws of quantum physics to create a sequence of random bits in two remote users. This sequence is used as a cryptographic key, and the key array itself is called a "one-time pad.

2. QUANTUM KEY DISTRIBUTION SYSTEMS

In 2007, the methods of quantum cryptography were first applied in a large-scale project. Quantum security system, developed by the Swiss company idQuantique, was used to transmit voting data at the parliamentary elections in Geneva. To date, really functioning quantum communication systems have been created. The efforts of developers are now aimed at increasing the communication range, increasing the speed of forming a quantum key, improving the characteristics of fiber-optic components.

As noted earlier, a symmetric cryptosystem generates a shared secret key and distributes it among legitimate users to encrypt and decrypt messages (Rumyantsev & Pijokin, 2015) . An attacker attempting to investigate transmitted data can't measure photons without distorting the original message. The system on the open channel compares and discusses signals transmitted on the quantum channel, thereby verifying them for the possibility of interception. If the system does not contain errors, then the transmit-