Chapter 15

Modeling of Quantum Key Distribution System for Secure Information Transfer

K. E. Rumyantsev
Taganrog Institute of Technology, Russia

D. M. Golubchikov
Southern Federal University, Russia

ABSTRACT

This chapter is an analysis of commercial quantum key distribution systems. Upon analysis, the generalized structure of QKDS with phase coding of a photon state is presented. The structure includes modules that immediately participate in the task of distribution and processing of quantum states. Phases of key sequence productions are studied. Expressions that allow the estimation of physical characteristics of optoelectronic components, as well as information processing algorithms impact to rate of key sequence production, are formed. Information security infrastructure can be utilized, for instance, to formulate requirements to maximize tolerable error level in quantum channel with a given rate of key sequence production.

1. QUANTUM KEY DISTRIBUTION

Quantum Cryptography (QC) is a part of quantum computing that examines the methods of information security by using a quantum carrier (Kilin, Nizovtsev, & Horoshko, 2007; Scarani, 2006; Bouwmeester, Ekert, & Zeilinger, 2000; Gisin, Ribordy, Tittel, & Zbinden, 2002; Rumyantsev, 2010). QC proposes a new method of generating random private keys for quantum communication line users. Its privacy and eavesdropping protection is based upon quantum principles instead of Classical Cryptography (CC) methods (Kotenko, & Rumiantsev, 2009; Mao, 2003; Smart, 2004; Singh, 2000; Brassard, 2007) used now and based upon mathematical law, which can be cracked.

Quantum key distribution (QKD) is a technology based upon quantum principles for generation random bit strings, which could be used as privacy keys, between two remote users.

The hardware is the realization of the process of sending and receiving data, for example, a single photon used in a fiber link. An eavesdropping changes the influential parameters of the physical objects, which used as data carrier.

DOI: 10.4018/978-1-4666-2208-1.ch015

QC is permitted to generate random keys for two users, which has no shared confidential data initially, and that key will be unknown for eavesdroppers.

The quantum physics law starts influence when data transmission uses signals containing average photon number less than 0.1 instead of the signals containing many thousands of photon. The nature of QC privacy is based on this law in conjunction with CC procedures. One of these laws is Heisenberg's uncertainty principle, and in accordance with it, a trial measurement of a quantum state changes to an initial state

The main gain of QC is that eavesdropping will be known to legal users, besides of absolute privacy.

Indivisible quantum and entanglement are very specific features of quantum physics (Kilin, Nizovtsev, & Horoshko, 2007; Scarani, 2006; Bouwmeester, Ekert, & Zeilinger, 2000; Gisin, Ribordy, Tittel, & Zbinden, 2002). QC uses both of these features.

The necessity in symmetric encryption systems arises in process of data transmission for reducing economic and social risks.

1.1. Symmetric Ciphers Require a Single Key to Encrypt and Decrypt

The quantum channel and open data link for checking of eavesdropping are the main components of QKD. The quantum channel and open data link connect legal users. The term of quantum channel mean that data carrier is a quantum in it.

QKD starts from transmission quantum between legal users. A matching of keys is realized through open data link. The eavesdropper has access to open data link, but it could not change information in it.

The sender encode the message into bit string (a_m is binary number) by using a random key a_k in symmetric encryption systems. Each bit of message add to same bit of key to make ciphertext as $a_t = a_m \oplus a_k$. Here $\oplus$ is congruence addition by 2 without carry (XOR). A receiver decode ciphertext by subtract key from it as $a_t\text{-}a_k = a_m \oplus a_k - a_k = a_m$. The bits of the ciphertext are random as the bits of the keys, so they are not contain any information. That cryptosystems are secure in accordance with information theory.

The system is secure absolutely on condition that the sender Alice and receiver Bob have shared private key, which has the same length as the message, and the key is used only once for encode.

The eavesdropper Eva can record all ciphertexts in order to create an image of plaintexts and the key if the key is used more than once.

If Eva has two ciphertexts a_{t1} and a_{t2} which encoded by single key a_k then she could add both ciphertexts and get a sum of plaintexts:

$$\begin{aligned} a_{t1} \oplus a_{t2} &= a_{m1} \oplus a_k \oplus a_{m2} \oplus a_k \\ &= a_{m1} \oplus a_{m2} \oplus a_k \oplus a_k = a_{m1} \oplus a_{m2}. \end{aligned}$$

The symmetric encryption systems *require for all users shared private key which* has the same length as the message and can be used only once.

The main idea of QC is trusted key distribution between users never met each other.

QC proposes a perspective way based on physical principles to solve the key distribution problem.

Statement 1: An unknown quantum state could not be cloned.

Statement 2: Information from the nonorthogonal quantum states could not be obtained without distortion it.

Statement 3: Any measurement performed by an eavesdropper leads to changes quantum state of data carrier.

Hardware-software solution for confidential data transmission with QKD system and synchronizing system is shown of Figure 1.