Analysis of information protection methods in the system telecommunications based on quantum cryptography

Bayram Ibrahimov[1], Mirfatma Javadova[2]
[1]Azerbaijan Technical University, Baku, Azerbaijan
[2]Azerbaijan Architecture and Construction University, Baku, Azerbaijan
[1]*i.bayram@mail.ru*

Abstract — **In this paper, the methods, algorithms and principles operation of quantum cryptography to protect information from unauthorized access to a telecommunications system using fiber-optic communication lines are partially analyzed. The system key distribution and protocols in the system quantum cryptography are considered.**

Keywords — quantum key, quantum cryptography, protocol, encryption, telecommunication network, fiber-optic communication line.

I. INTRODUCTION

It is known [1, 2] that in order to provides multimedia services in a telecommunications systems using fiber-optic communication lines, it is necessary to ensure the possibility continuous operation of a public multiservice network and the security transmitting non-uniform traffic. Considering the distributed architecture of the NGN (Next Generation Network, NGN), in which attacks can occur at various points at the network boundaries, technical difficulties arise in ensuring the security such systems.

It should be noted that, according to estimates of domestic and foreign experts, a significant part of the lines used via the publicly available telecommunication channel is fiber-optic communication lines (FOCL). The tasks of protecting a multiservice network using FOCL in a telecommunication system occupy one of the leading places in solving the general problem of information security.

However, various methods communication are currently widely used in the telecommunications system: wired communication lines, cellular communication, satellite communications, fiber-optic communication lines, etc. Subscriber and network users in a wide range are used daily by communication services, which are necessary to ensure the threat to the security of transmitted information.

Modern NGN-based telecommunications systems use various encryption methods, mathematical algorithms, and efficient network coding to preserve and protect the transmitted heterogeneous traffic.

Based on an analysis of the work on Internet security threats for 2015 [3, 4], it was established that the number of targeted attacks on personal data increased by 91% last year, and more than 550 million people became their victims. Therefore, in recent years, new and effective methods and algorithms for protecting information from unauthorized access to subscriber and network communication lines have been developed.

In telecommunication systems, cryptographic systems from unauthorized access are widely used [2, 3]. The latter are based on the use cryptographic keys and are of two types - symmetric and asymmetric. In symmetric cryptosystems, the sender and the recipient - the recipient of the message use the same secret key, in asymmetric two cryptosystems use two keys: one - open, for encryption - the sender uses, the second - closed, for decryption - uses recipient.

In work [1, 2, 3] cryptographic methods and algorithms of information protection from unauthorized access are considered and their cryptographic strength is revealed. In [2, 4] it is determined that at this stage of development and the use cryptographic methods for protecting information do not fully ensure the protection of transmitted information.

Based on the study [4, 5], it was established that one of the important and promising methods and algorithms cryptography is the principles of quantum cryptography, and the network itself is called a quantum network.

Considering the above, this paper discusses the methods and algorithms quantum cryptography, which is based on the principles operation of a quantum computer, using the parallelism of quantum computing.

DOI: 10.25045/NCInfoSec.2018.10

II. FORMULATION OF THE PROBLEM

The problem of ensuring security in the transmission of information is formulated as the problem of the distribution of the secret key between two remote users [1]. Users form the same bit set, which is used as a cryptographic key. To realize absolute secrecy, it is necessary to observe certain conditions: the key can be used only once, the key must be random, its length must be greater than or equal to the length of the message being encoded [2].

It is known [3, 5] that the security of classical cryptographic methods is based on mathematical laws and is theoretically limited to the computational capabilities of an attacker. The physical solution to the problem of ensuring secrecy in key distribution is to use the principles of quantum cryptography [3, 4].

Quantum cryptography is based on quantum networks, a quantum network is an information and telecommunication network that protects the transmitted information of heterogeneous traffic using the fundamental laws of quantum mechanics. The latter is a practical implementation of the so-called quantum cryptography.

Quantum cryptography is a method and algorithm for protecting information in next-generation multiservice telecommunication networks based on the principles quantum physics.

Unlike traditional methods and algorithms of cryptography, which uses mathematical methods to ensure the secrecy of information transmitted, quantum cryptography focuses on physics, considering cases where information is transferred using objects of quantum mechanics.

The process of sending and receiving messages of non-uniform traffic is always carried out by physical means, for example, using electrons in an electrical signal and photons in fiber-optic communication lines. In this case, eavesdropping can be considered as a change in certain parameters of physical objects - in this case, carriers of information.

To achieve the objective, the methods, algorithms and principles of operation of quantum cryptography are analyzed to protect information from unauthorized access to the telecommunications system using FOCL.

III. THE ESSENCE OF THE CRYPTOKEY IN THE SYSTEM OF QUANTUM CRYPTOGRAPHY

In the system of quantum cryptography, almost all the collisions in the keys. In quantum cryptography, crypto-keys are distributed in two ways [3, 4]: either with the participation of a key distribution center or a direct exchange between users. Crypto keys should be distributed or they can be exchanged over a communication channel in a secure way.

In the system, a by-product of developing a quantum computer using quantum computing parallelism is quantum cryptography, which could bring to light a new encryption algorithm by generating a secret key. At the same time, the algorithm is the basic construction unit of quantum cryptography qubit (qubit, Quantum Bit).

The classic bit has, as is known, only two states — 0 and 1, while the set of qubit states is much larger. This means that the qubit in one unit time is equal to 0 and 1, and the classical bit in the same unit of time is either 0 or 1. For example, if quantum memory consists of two qubits, then in parallel work with all its possible states: 00, 01, 10, 11.

Due to the possibility of parallel work with a large number options, a quantum computer needs much less time to solve problems of a certain class. Such problems, for example, include problems decomposing numbers into prime factors, searching a large database, etc.

The considered algorithm for generating the secret key is based on quantum cryptography technology, where it is expedient to use telecommunications systems using FOCL.

Consequently, the rapid development of quantum technology to create an effective secret key and fiber-optic communication lines led to the emergence of quantum cryptographic systems. They are an extreme case protected FOCL. Using quantum mechanics to protect information allows you to receive results that are unattainable with both FOCL technical protection methods and traditional methods of mathematical cryptography.

Protection this class information is used in limited quantities mainly to protect the most critical from the point view security in the FOCL-based telecommunications system.

IV. KEY DISTRIBUTION SYSTEM AND PROTOCOLS IN A QUANTUM CRYPTOGRAPHY SYSTEM

The analysis showed [3] that in quantum cryptography two main directions for the development key distribution systems have emerged. The first direction is based on the coding of the quantum state of a single particle and is based on the principle of the impossibility to distinguish absolutely reliably two no orthogonal quantum states. An arbitrary state any two-level quantum-mechanical system can be represented as a linear superposition [1, 5]:

$$\left|\chi_{kk}\right\rangle = \alpha \left|0\right\rangle + \beta \left|1\right\rangle \qquad (1)$$

her own states $\left|0\right\rangle$ and $\left|1\right\rangle$ with complex coefficients α and β, where

$$\left|\alpha^2\right| + \left|\beta^2\right| = 1 \qquad (2)$$

From (1) and (2) it follows that the basic principles these two areas formed the basis for the development of all protocols for the quantum distribution keys.

There are many quantum cryptography protocols based on the transmission of a message by encoding in the states of single photons, both BB84, B92 and BB84 with six states, Goldenberg-Weidman, Koashi-Imoto,

as well as their modifications [4]. The only protocol developed for coding information in tangled states is E91 [5].

Various quantum cryptography protocols require the construction complex signal processing circuits, which is also convenient to implement on the basis of a single integrated circuit. Solving the problem of key distribution systems and protocols in the system of quantum cryptography on the element base of modern fiber optics is still a challenge.

CONCLUSIONS

The results of the research and analysis show that the progress information security in quantum cryptographic directions is progressing rapidly. In the near future, quantum cryptographic methods for protecting information other than a telecommunications system using FOCL will use top-secret military and commercial applications.

REFERENCES

[1] K.E.Rumyantsev. Sistemy kvantovogo raspredeleniya klyucha: Monografiya. Taganrog: Izdatelstvo TTI YuFU, 2011. - 264 p.

[2] B.G. Ibrahimov, R.T.Humbatov, R.F. Ibrahimov. Cryptographic methods and means protection transmitted information in telecommunication systems // International Journal of Electronics & Communication.Vol.6., Issue 4. 2018. – pp.16 –20.

[3] L.Lydersen, C.Wiechers, C.Wittmann, D.Elser, J.Skaar, V.Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination // Nat. Phot.,Vol.4, no. 686. 2010.p.

[4] N.Gisin, G.Ribordy, W.Tittel, H Zbinden. Quantum cryptography. Rev.Mod. Phys., vol. 74, №1. 2002. - pp. 145-195.

[5] Makarov V. Quantum cryptography and quantum cryptanalysis, doktor ingenior thesis, Norwegian University of Science and Technology. 2007.-158 p.