SIMULATION OF SOME SECURITY TASKS FOR SECURE TELECOMMUNICATIONS USING A QUANTUM-COMPUTING SIMULATOR IN ONE OF THE QUANTUM PROGRAMMING LANGUAGES

A. A. Kryuchkov, A. V. Korolkov
RTU MIREA, Moscow, Russian Federation

andrai12@mail.ru

I. INTRODUCTION

In Russia, as part of the implementation of the national program "Digital Economy of the Russian Federation", a roadmap for the development of the high-tech area "Quantum Communications" is being implemented since 2020. One of the most important elements that ensure the effective use of quantum communications are quantum key distribution protocols. These protocols must be resistant to known attacks on quantum communication channels, as well as to the possible appearance of quantum computers that implement threats to decrypt information.

The main issue of symmetric cryptography is how to securely distribute the secret key among legitimate users. Quantum cryptography provides the ability to securely generate a secret sequence between

participants in information exchange, ensuring that the key cannot be intercepted by an intruder. Quantum protocols are based on the fundamental laws of quantum physics combined with a provable mathematical apparatus.

The BB84 protocol is widely used to implement quantum key distribution. Modeling this protocol using remote quantum programming on a quantum computer is the main subject of this article.

In the submitted article:

1. Quantum programming methods are applied to simulate quantum key distribution according to the BB84 protocol. The process of quantum key distribution was simulated using a quantum computer model and also by means of a real 5-qubit quantum computer provided by IBM.

2. An attempt to intercept a private key by an intruder with an attack "man-in-the-middle" was simulated.

3. The results of modeling the BB84 protocol are presented. The security of the mathematical model for generating a secret key between users has been confirmed.

4. The analysis of practical implementations of quantum key distribution to date is given.

II. MAIN DIAGRAMS AND FORMULAS

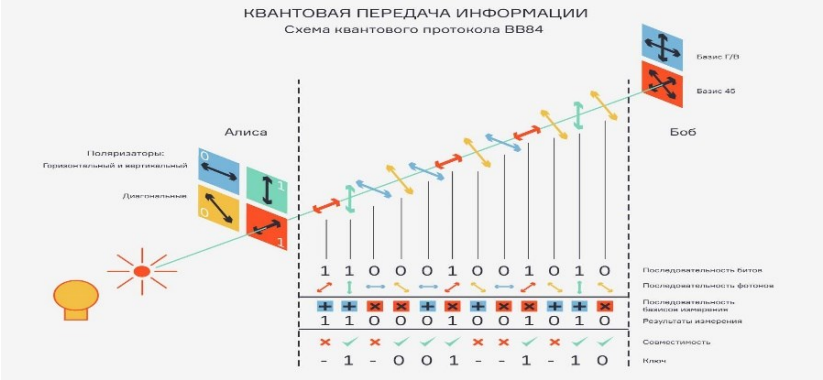

Figure 1. The scheme of the quantum protocol BB84

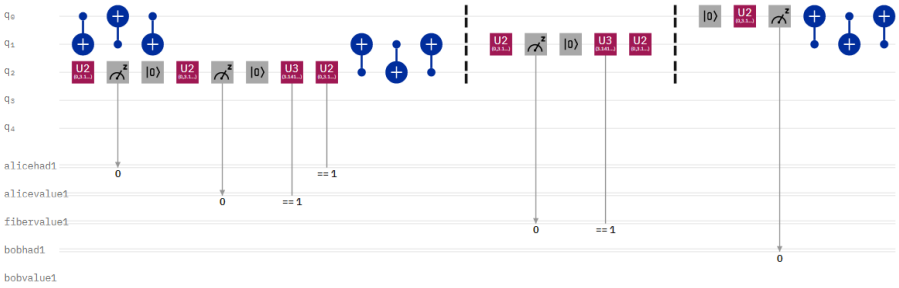

Figure 2. The scheme of the quantum protocol BB84 on an IBM quantum simulator

A two-level quantum mechanical system is defined by a linear superposition of its own states $|0\rangle$ and $|1\rangle$ (1)

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1}$$

where α and β are complex coefficients satisfying equality:

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2}$$

The description of the quantum states of the system is given by the following expressions:

$$|0_\times\rangle = \frac{1}{\sqrt{2}}(|0_+\rangle + |1_+\rangle) \tag{3.1}$$

$$|1_\times\rangle = \frac{1}{\sqrt{2}}(|0_+\rangle - |1_+\rangle) \tag{3.2}$$

REFERENCES

[1] C. H. Bennett and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing". In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York, 1984.

[2] I. Chang M. Nilsen, "Quantum computation and quantum information", Mir, pp. 711-714, 2006.