Universal Quantum Gate as a Tool for Modeling Quantum Cryptanalysis Algorithms on a Quantum Circuit

Aleksei Petrenko [1], Sergei Petrenko [1] and Viktoriya Taran [2]

[1] *Saint Petersburg Electrotechnical University "LETI", 5, Professor Popov Street, St. Petersburg, 197376, Russia*
[2] *V.I.Vernadsky Crimean Federal University, Prospekt Vernadskogo, 4, Simferopol, 295007, Crimea*

Abstract

The article discusses the features of modeling quantum cryptanalysis algorithms on a quantum scheme. Some engineering problems of the implementation of quantum cryptanalysis algorithms are shown and an analysis of possible ways of their solution is carried out. The uniqueness of quantum computation is shown due to the ability to carry out some non-trivial quantum computation using superposition, that is, it is possible to perform a series of mathematical operations, each of which operates with all stored data at the same time. The article discusses an algorithm for a quantum computer, which must initialize this vector in some specified form (depending on the model of the quantum computer). At each step of the algorithm, this vector is modified by a unitary matrix, which is determined by the physics of the device. It is proposed to consider the universal quantum gate as the quantum equivalent of the classical Boolean function from the universal set, which is a gate, and, acting on a qubit or their various combinations, can imitate the action of any other quantum gate. In the study of quantum algorithms, polynomial-time algorithms are found in problems for which no classical polynomial algorithms are known for their solution. For the required protection of quantum systems from decoherence errors and other quantum noise, methods of quantum error correction (QEC) have become widespread.

Keywords

The national quantum program, a roadmap for the development of quantum technologies, quantum computing and computers, quantum and post-quantum cryptography, quantum cryptanalysis algorithms

1. Introduction

Distinguish between symmetric and asymmetric (public key) encryption algorithms. Symmetric encryption algorithms, for example, AES or RC6, are considered sufficiently strong if they are not known to crack them faster than brute force. The brute-force complexity (for an attack with a known ciphertext) can be estimated as O (2k), where k is the key length in bits. Considering that back in 2002, using the amateur network of distributed computing distributed.net, the possibility of cracking a 64-bit key by brute force was demonstrated, now the key length is considered to be 128 bits, and the maximum key length supported by the most symmetric crypto algorithms is 256 bits.

For asymmetric crypto algorithms, cryptanalysis methods are known that work much faster than full search. Because of this, asymmetric crypto algorithms have a key length much longer than symmetric ones. The most commonly used algorithm is RSA, based on the computational complexity of the problem of factorizing integers, and El-Gamal's algorithm, based on the computational complexity of the discrete logarithm problem. In this case, versions of the El-Gamal algorithm are used for various

AISMA-2021: International Workshop on Advanced in Information Security Management and Applications, October 1, 2021, Stavropol, Krasnoyarsk, Russia
EMAIL: a.petrenko1999@rambler.ru (Aleksei Petrenko); s.petrenko@rambler.ru (Sergei Petrenko); victoriya_yalta@ukr.net (Viktoriya Taran)
ORCID: 0000-0002-9954-4643 (Aleksei Petrenko); 0000-0003-0644-1731 (Sergei Petrenko); 0000-0002-9124-0178 (Viktoriya Taran)

fields, for example, over a group of points of an elliptic curve. Consider possible quantum cryptanalysis algorithms for symmetric and asymmetric encryption schemes.

Consider the features of modeling quantum cryptanalysis algorithms on a quantum scheme. Let us show the differences between the mentioned algorithms and classical algorithms (the essence of the transformation of the well-known Church-Turing thesis into the Church-Turing-Deutsch thesis). Then we will point out some engineering problems in the implementation of quantum cryptanalysis algorithms and then analyze possible ways to solve them.

2. Analysis of Publications

The authors of [1] proposed an assessment procedure based on integral estimates of unconditional and conditional criteria, found the absence of a universal post-quantum cryptographic algorithm, proposed to separate three options for using post-quantum algorithms: for lightweight cryptography, for use in standard automated systems and use in a cloud environment, received estimates of post-quantum algorithms depending on the conditions of their application.

The research [2] is dedicated to finding quantum computing algorithms other than Shor's algorithm to explore quantum computing cryptographic attack and various existing algorithms for integer factorization algorithms of quantum computing are studied and show optimistic potentials of quantum annealing algorithm and D-Wave quantum computer for deciphering the RSA cryptosystem.

The article [3] discussed modern encryption algorithms and the possibility of integrating them into different spheres and using cryptanalysis method has chosen algorithm for integration with quantum technologies.

Authors [4] describe ciphers and classical encryption and decryption algorithms and specify the basic methods and evolution vectors for cryptography and cryptanalysis. During this research, we have conducted a review of the requirements for the stability of the developed quantum key integration algorithm.

The authors [5] evaluate the computational power of some existing quantum computers to illustrate research in post-quantum security and analyze the post-quantum security of well-known messaging specification Signal, the core of Signal specification is the Double Ratchet protocol, and suggest some possible ways to improve the security features of Signal specification.

The work [6] is devoted to the study of quantum versions of the differential cryptanalysis based on using a combination of the quantum minimum/maximum search algorithm and the quantum counting algorithm. The author has estimated the complexity and the required resources for applying the quantum differential and quantum linear cryptanalysis to searching round keys of block ciphers. It is shown that the implementation of the quantum linear method requires fewer logical qubits than for the implementation of the quantum differential method.

The authors [7] are investigated biometric cryptographic systems, which are designed to generate secure pseudorandom sequences that can be used as cryptographic keys, passwords, etc. This work presents a new key generation scheme that uses fuzzy extractors from the biometric data of the iris. The proposed method is based on the code-based public-key cryptosystems which are considered to be resistant to quantum cryptanalysis.

In [8] paper, authors describe a new implementation of MST3 cryptosystems based on the group of automorphisms of the field of the Pu function. The main difference of the presented implementation is the extension of the logarithmic signature and, as a consequence, the presence of multi-stage recovery of message parts from the ciphertext.

In [9] paper, the author devised a concretely efficient polynomial method-based algorithm for solving multivariate equation systems over F2 and analyze this algorithm's performance for solving random equation systems, and bound its complexity, and apply the algorithm in cryptanalysis of recently proposed instances of the Picnic signature scheme (an alternate third-round candidate in NIST's post-quantum standardization project) that are based on the security of the LowMC block cipher.

3. The Quantum Algorithm

A quantum analog of a bit (quantum bit, or *qubit*) has quantum mechanical features of behavior. Almost any quantum system (with at least two states) can act as a *qubit*. Its state space is the *Hilbert space* the linear hull spanned by two (or more) basis vectors (in Dirac's notation, quantum states are written as $|0\rangle$ and $|1\rangle$).

The general state of a quantum system with two states can be represented by a superposition of basis states $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, wherein $|\alpha|^2+|\beta|^2 = 1$ (Fig. 1).

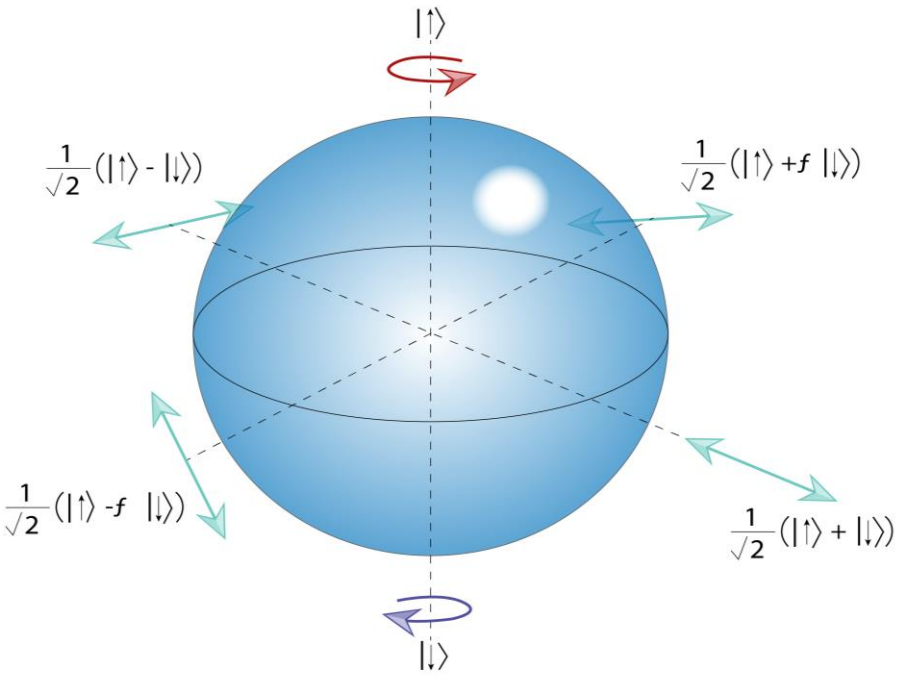

Figure 1: States of a qubit in the form of a Bloch sphere

Note that a register composed of L two-level qubits can simultaneously store up to 2^L numbers in a quantum superposition. Therefore, if the register is replenished with additional qubits, then the amount of stored information in the register will increase exponentially. For example, a 250-qubit register with atomic dimensions will be able to store more numbers than there are atoms in the known universe (10^{78}). Moreover, this is an understated estimate of the amount of quantum information contained in a quantum register, since the superposition vectors are in a continuously variable proportion - each with its own phase. Even so, if we measure the state of the register, we get only one of those numbers. However, the uniqueness of quantum computation lies in the fact that it is possible to carry out some non-trivial quantum computation using superposition - you can perform a series of mathematical operations, each of which operates on all the stored data at the same time.The state of the L-qubit register can be represented by a 2^L-dimensional complex vector. An algorithm for a quantum computer must initialize this vector in some specified form (depending on the model of the quantum computer). At each step of the algorithm, this vector is modified by a unitary matrix, which is determined by the physics of the device. The unitarity of the matrix guarantees its reversibility (thus, each step is reversible). After the completion of the algorithm, the 2^L-dimensional complex vector stored in the register must be read from the qubit register by quantum measurement. According to the laws of quantum mechanics, the result of this measurement will be a random string of L bits (and the measurement will destroy the final state). This random string can be used in calculating the function value because (according to the model) the probability distribution of the measured bit string is skewed towards the correct function value. By repeated runs of the quantum computer and then measuring the yield, the correct value can be determined with high probability (Fig. 2).

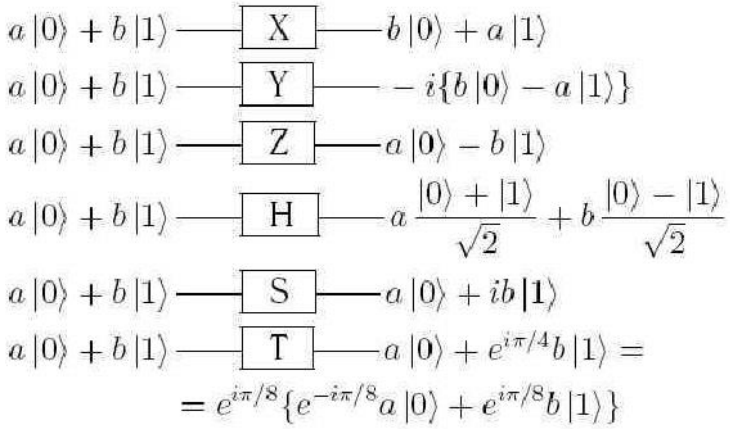

Figure 2: An example of basic 1-qubit gates

The quantum algorithm is performed by implementing a series of sequential unitary operations. Note that for a given algorithm, operations will always be performed in the same order. There is no "IF, THEN" logical condition to varying the sequence since there is no way to read the state of the qubit before the final measurement. But there are conditional operations implemented by the CNOT gate (Figure 3).

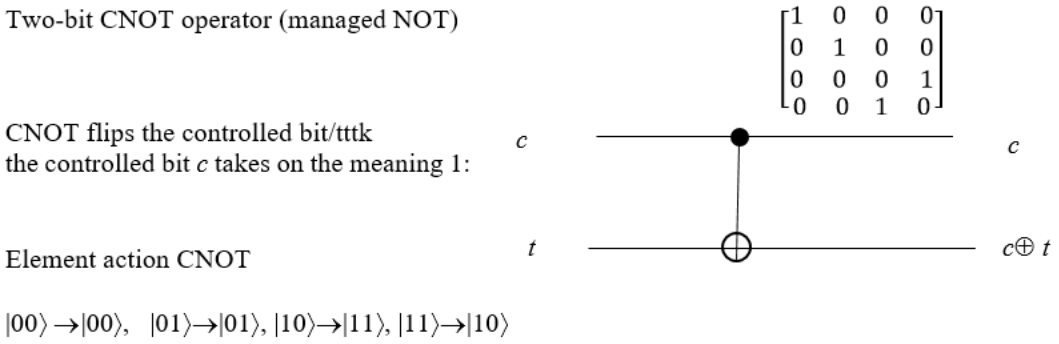

Figure 3: Application of gate (operator) CNOT

According to D. Deutsch, the following requirements are imposed on a quantum computer. A quantum computer is a set of n qubits, for which the following operations are practically defined:

1) Each qubit can be initialized in a known state (for example, the state $|0\rangle$.

2) Each qubit can be measured in the basis $\{|0\rangle, |1\rangle\}$.

3) A universal quantum gate (or set of gates) can act on any limited subset of qubits.

4) The state of the qubits does not change except through the above transformations.

This description does not touch on certain technological aspects but contains the basic ideas for constructing a quantum computer.

Note that the theoretical model of quantum computing is networked and implies a sequential effect of logical gates on a set of qubits. Logic gates of a classical electronic computer are located on a circuit board separately from each other; in a quantum computer, logical gates are considered as interactions of several qubits that occur at a certain time. In this case, qubits form a certain configuration, in which there are fundamentally more options for interaction between elements than in a classical computer. It is also possible to develop other models of quantum computing, for example, the cellular automaton model [10].

The universal quantum gate is the quantum equivalent of the classical Boolean function from the universal set and is a gate that, acting on a qubit or their various combinations, can simulate the action of any other quantum gate. In 1985, D. Deutsch showed that fairly simple quantum gates can constitute

a universal set that will be sufficient to build a quantum computer. For example, a pair of one-qubit gate *V(θ, φ)* and two-qubit gate "CNOT", where *V(θ, φ)* is a gate of arbitrary rotation of one qubit:

$$V(\theta,\varphi)=\begin{pmatrix}\cos\left(\frac{\theta}{2}\right) & -ie^{-i\varphi}\sin\left(\frac{\theta}{2}\right)\\ -ie^{i\varphi}\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right)\end{pmatrix},$$

CNOT can be represented by a matrix

$$CNOT=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$$

and can be considered a universal set. Any unitary $n \times n$ matrix can be formed by combining two-qubit CNOT gates and rotation gates of one qubit. A description of such universal gates can be found in D. Deutsch, S. Lloyd, D.P. di Vincenzo, and A. Barenzo

A quantum algorithm is an algorithm that uses the quantum properties of an object to process a computation. You can formalize the description of quantum computing in terms of the classical computing model. For example, logical operations on bits of computer memory according to Turing of classical computation are replaced by unitary transformations acting on a fixed finite number of qubits.

In the study of quantum algorithms, it turns out to be interesting to find polynomial-time algorithms in problems for which no classical polynomial algorithms for their solution are known. According to researchers [6-10], quantum computers will be able to solve cryptanalysis problems much more efficiently than classical ones.

Thus, quantum computers are based on quantum registers, which are made up of quantum bits (qubits). When measuring a quantum system, a quantum bit can have such a state that the measurement can show |0⟩ with some probability, and show |1⟩ with some other probability.

A quantum register consisting of n quantum bits has dedicated states corresponding to n bit binary numbers from |00K0⟩ to |11K1⟩. The state of a quantum register is written as a linear combination of all these highlighted states:

$$\sum_{x=0}^{2^n-1} a_x\,|x\rangle.$$

In this case, the normalization condition is satisfied:

$$\sum_{i=0}^{2^n-1}|a_i|^2=1.$$

The a_x coefficients are complex numbers. They are called the amplitudes of the corresponding states |x⟩.

The state of a system consisting of n quantum bits is described by a vector of unit length in a 2^n-dimensional complex unitary space (the scalar product of states $|a\rangle = |a_1\mathrm{K}a_n\rangle$ and $|b\rangle = |b_1\mathrm{K}b_n\rangle$ denoted as $\langle a|b\rangle$ and is introduced in the usual way: $\langle a|b\rangle = \sum a_i\, b_i$. Quantum register of length n, can represent different values of an n-bit word at the same time.

To extract information from a quantum register, a measurement must be made. Any set of quantum bits can be measured. In addition, since quantum states form Euclidean space, measurements can be made on different bases. However, the measurement leads to the transition of the system to the basic state corresponding to the measurement results.

A quantum computer can perform transformations on a quantum register. A quantum transformation is a mapping of a unitary space formed by a quantum system into itself. With quantum systems, only linear unitary transformations can be performed, and any linear unitary transformation is admissible. Due to linearity, quantum transformations are completely determined by their action based on vectors. Table 1 lists the main quantum gates.

The engineering problems of the implementation of quantum cryptanalysis algorithms include keeping the computer elements in a relatively stable (coherent) state, as well as protecting against decoherence errors. The first problem is related to the fact that, in practice, the interaction of a quantum

system with the outside world leads to a loss of coherence (otherwise, its decoherence), and, consequently, to an emergency shutdown of the computer. This effect leads to a violation of the unitary nature (or, more precisely, reversibility) of the quantum steps of the computation, which will soon be after the launch of the algorithm, as a result of which it will be impossible to solve complex problems of cryptanalysis.

Table 1

Basic elementary transformations (or quantum gates)

Name, designation, and a short description of the quantum gate	Baseline action	Matrix
Identity transformation I	$\|0\rangle \to \|0\rangle$ $\|1\rangle \to \|1\rangle$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Negation X	$\|0\rangle \to \|1\rangle$ $\|1\rangle \to \|0\rangle$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Phase Shift Z	$\|0\rangle \to \|0\rangle$ $\|1\rangle \to -\|1\rangle$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Phase shift s negation of Y	$\|0\rangle \to -\|1\rangle$ $\|1\rangle \to \|0\rangle$	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$
Controlled-NOT CNOT Adds the first modulo 2 to the second bit	$\|00\rangle \to \|00\rangle$ $\|01\rangle \to \|01\rangle$ $\|10\rangle \to \|11\rangle$ $\|11\rangle \to \|10\rangle$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$
Controlled-Controlled-NOT Tofolli valve Adds to the third bit the product of the first two modulo 2	$\|000\rangle \to \|000\rangle$ $\|001\rangle \to \|001\rangle$ $\|010\rangle \to \|101\rangle$ $\|011\rangle \to \|010\rangle$ $\|100\rangle \to \|100\rangle$ $\|101\rangle \to \|101\rangle$ $\|110\rangle \to \|111\rangle$ $\|111\rangle \to \|110\rangle$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$
Transformation Hadamard H	$\|0\rangle \to \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$ $\|1\rangle \to \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

The point is that the fourth point of D. Deutsch's requirements to a quantum computer on the invariability of the state of a quantum system is, in principle, physically unrealizable [3, 9, 10]. In reality, there is no perfect quantum gate, nor a completely isolated system. You can strive for the most accurate approximation of a real device to the ideal, but at present, this is not feasible. Gates such as XOR are based on the interaction of two initially separated qubits. But if qubits interact with each other, then they will inevitably interact with something else [2, 5, 6]

In practice, it turned out that designing a quantum system in which the loss of coherence would occur less than once in a million uses of the XOR gate turned out to be a rather difficult engineering task. According to the researchers, it remains to be seen whether the laws of physics allow finding a lower limit on the rate of loss of coherence. This problem was identified in the works of S. Garoche and J.M. Raymond, R. Landauer, C. Miguel and A. Barenzo.

Thus, periodically projecting the state of the computer through carefully selected measurements is not sufficient by itself. Therefore, for the required protection of quantum systems from decoherence errors and other quantum noise, methods of quantum error correction (QEC) have become widespread

[20]. For quantum systems, were first proposed and considered in the works of E. Steen and, independently of him, A.R. Kalderbank and P. Shor [1-7].

Scientists have noted the importance of quantum error correction for error-correcting quantum computing, not only to combat noise are stored quantum information but also to compensate for "noisy" quantum gates, as well as to compensate for imperfections in quantum measurement tools. Initially, it was not clear whether network data should be ideal when using error correction techniques. P. Shor showed how to make error correction networks insensitive to errors within these networks. In other words, it turned out that such "error correction" networks cancel out more interference than they create.

4. Conclusions

The discovery of the method of quantum error correction approximately coincided with the emergence of the associated method of "entanglement enhancement", which also provides interference-free transmission of quantum states over a noisy quantum channel [10]. The basic idea behind this method is that the sender forms many linked pairs of qubits, and then sends one qubit from each pair over the noisy channel to the receiver.

The sender and receiver accumulate qubits and then perform a parity-checked measurement: for example, the receiver XOR the received and subsequent qubits and then measures the resulting qubit. After the sender performs identical operations on their qubits, they compare the results. If the results match, then the states of more than half of the unmeasured qubits coincide with the required one by chance: $|00\rangle + |11\rangle$. If the results do not match, the qubits are discarded.

It is required to have its technical solutions with the maximum degree of localization of production (both end devices and components) to eliminate the risk of introducing destructive hardware and software (undeclared capabilities, NDV) into hardware and software, and, as a consequence, access to protected information [11].

Thus, The study of user awareness as an element of predicting the targets of an attack has also practical application as a study of the dynamics of changes in the landscape of security threats [12-14].

5. Acknowledgments

The article was prepared based on the results of research carried out with the support of the RFBR grant (No. 20-04-60080).

6. References

[1] I. Gorbenko, V. Ponomar, Examining a Possibility to Use and the Benefits of Post-Quantum Algorithms Dependent on the Conditions of Their Application. Eastern-European Journal of Enterprise Technologies. 2017. V. 2. No 9 (86). PP. 21-32. DOI: 10.15587/1729-4061.2017.96321

[2] C. Wang, H.-N. Yao, B.-N. Wang, F. Hu, X.-M. Ji, H.-G. Zhang, Progress in Quantum Computing Cryptography Attacks. Jisuanji Xuebao. 2020. V. 43. No 9. PP. 1691-1707. DOI: 10.11897/SP.J.1016.2020.01691

[3] N. Abdinurova, B. Kynabay, Revealing Encryption Algorithm for Integrating with Quantum Technologies by Using Cryptanalysis. In 14th International Conference on Electronics Computer and Computation, ICECCO 2018. 14. 2019. PP. 8634689. DOI: 10.1109/ICECCO.2018.8634689

[4] A. Pljonkin, A. Gorbunov, The General Principles of Quantum Key Integration into Data Network ParT 1. In 2019 2nd International Conference on Intelligent Communication and Computational Techniques, ICCT 2019. 2. 2019. PP. 308-312. DOI: 10.1109/ICCT46177.2019.8969011

[5] Bobrysheva J., Zapechnikov S. Post-Quantum Security of Messaging Protocols: Analysis of Double Ratcheting Algorithm. In Proceedings of the 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, EIConRus 2020. 2020. PP. 2041-2044. DOI: 10.1109/EIConRus49466.2020.9039075

[6] Denisenko D. Quantum Differential Cryptanalysis. Journal of Computer Virology and Hacking Techniques. 2021. DOI: 10.1007/s11416-021-00395-x

[7] M. Lutsenko, A. Kuznetsov, A. Kiian, T. Kuznetsova, O. Smirnov, Biometric Cryptosystems: Overview, State-Of-The-Art and Perspective Directions. Lecture Notes in Networks and Systems. 2021. V. 152. PP. 66-84. DOI: 10.1007/978-3-030-58359-0_5
[8] G. Khalimov S., Khalimova, Y.Kotukh, Encryption Scheme Based on the Automorphism Group of the Ree Function Field. In 2020 7th International Conference on Internet of Things: Systems, Management, and Security, IOTSMS 2020. 7. 2020. C. 9340192. DOI: 10.1109/IOTSMS52051.2020.9340192
[9] I. Dinur, Cryptanalytic Applications of the Polynomial Method for Solving Multivariate Equation Systems over GF(2). Lecture Notes in Computer Science. 2021. T. 12696 LNCS. C. 374-403. DOI: 10.1007/978-3-030-77870-5_14
[10] A.S. Petrenko, A.M. Romanchenko, A promising cryptanalysis method based on Shor's algorithm. Protection of information. Inside No. 2 2020. SPb.: Publishing house. Athena, 2020. PP. 17-23.
[11] A.S. Petrenko, S.A. Petrenko, K.A. Makoveichuk, A.V. Olifirov, H. Krachunov, Security Threat Model Based on Analysis of Foreign National Quantum Programs. Selected Papers of the VI International Scientific and Practical Conference "Distance Learning Technologies" (DLT 2021). 2021. PP. 11-25. http://ceur-ws.org/Vol-3057/paper2.pdf
[12] V.V. Zolotarev, M.A. Lapina, N.Y. Parotkin, E.V. Ulianova, Evaluation of Game Resources as a Purpose of Cyber Attacks for Educational Games. Selected Papers of the VI International Scientific and Practical Conference "Distance Learning Technologies" (DLT 2021). 2021. PP. 290-295. http://ceur-ws.org/Vol-3057/paper35.pdf
[13] N. Proshkin, E. Basan, M. Lapina, Radio Frequency Method for Emulating Multiple UAVs. 17th International Conference on Intelligent Environments, IE 2021 Proceedings, 2021, 9486599, https://doi.org/10.1109/IE51775.2021.9486599
[14] Basan, E., Peskova, O., Lapina, M. Analysis of Communication Channels for the Organization of Control and Interaction of UAVs from the Security Viewpoint. CEUR Workshop Proceedings SibDATA 2021: Short Paper Proceedings of the 2nd Siberian Scientific Workshop on Data Analysis Technologies with Applications, 3047, 2021. PP. 17-23, http://ceur-ws.org/Vol-3047/paper3.pdf