Abstract of the Dissertation
The Development and Study of an Information Protection Algorithm Using Non-Positional Notations
by Ardabek Khompysh
in Candidacy for the Degree of Doctor of Philosophy (Ph.D.)
in the specialty 6D100200 – Information security systems

The relevance of the research topic. Currently, Kazakhstan is faced with the historical need to move from an industrial society to a fundamentally new level of social and economic development, determined by the stringent requirements of the modern scientific and technological revolution. Given the high level of development of the information society and information economy in many developed countries, issues of further development in Kazakhstan are becoming one of the priorities. Since the material base of the information society is the information economy, the information resources acquire special significance. At the same time, information resources are considered as strategic resources of the country that require constant protection from unauthorized access by other users.

A high degree of automation, the widespread introduction of computer systems in various spheres of human activity make automated data processing systems very vulnerable to cyber threats, and society becomes dependent on the level of security of the information technologies used. Therefore, the security of circulating and transmitted information becomes an important characteristic of any computer system, regardless of its complexity and purpose.

One of the priorities of the development strategy of any state is national security, and one of its most important elements is information security. Therefore, the urgent tasks are the creation of new technologies for protecting information, limiting access to it, ensuring the required level of information protection, and creating information security means that meet modern requirements.

The Cybersecurity Concept "Cyber Shield of Kazakhstan" (dated June 30, 2017) states that it is necessary to "Giving priority to research and our own school of applied mathematics in the development of **cryptographic information protection facilities, cryptology**, developments in programmable logic integrated circuits, quantum cryptography and the development of the protection of transmission systems, processing and storage of information, as well as information security systems" and "Overcoming the problem of low demand for domestic developments since cybersecurity ultimately depends on the level of development of the domestic IT industry and the electronic industry."

In this regard, R&D aimed at the development of domestic information security systems are relevant to our country.

This is primarily due to the constantly growing pace of scientific and technological progress, which leads to the improvement of computer technology. Their appearance not only raises new security issues, but also offers new solutions to problems, and the complexity of solving information security problems is influenced by:

- An increase in the volume of information collected, stored, and transmitted using computer technology;
- Expanding the circle of users with access to the resources of the computer system;
- The complication of the operating modes of the hardware part of a computer system;
- An increase in the number of technical means and communications in automated data processing systems;
- Widespread use of new infocommunication technologies.

To minimize the consequences of unauthorized access, one needs to create a security system. The purpose of creating such a system is to prevent the consequences of intentional or accidental destructive influence, as a result of which information can be destroyed, modified, or stolen. At the same time, an effective security system should ensure:

- Confidentiality of all information or an important part of it;
- Reliability of information (completeness, accuracy, reliability, integrity, authenticity), the operability of system components at any time;
- Timely access of users to the necessary information and system resources;
- Differentiation of responsibility for violation of the established rules of information relations;
- Operational control of information management, processing, and exchange processes.

It should be noted that among the described properties of a security system, depending on the object of protection, there may be different prioritization. In the context of protecting state secrets, special attention is paid to the confidentiality of information. This determines counter risks, the purpose of which is to reduce the likelihood of a threat or to minimize the consequences of a threat. These measures together form the security policy. Studies of many foreign and domestic scientists show that among organizational, methodological, and technical measures, methods of cryptographic information protection occupy an important place.

Modern cryptographic techniques, including iterative block ciphers, are one of the most popular tools for the secure exchange of information over high-speed data networks. The widespread use of information technology and the rapid growth of computing power pose a cryptanalysis threat to the known ciphers.

Research on the creation of cryptographic data protection means is often aimed at protecting state secrets, so the use of ready-made foreign solutions is insecure. Research on the development of domestic cryptographic information protection, including the development of encryption algorithms, is relevant and necessary.

The purpose of the dissertation is to create an information encryption algorithm using the capabilities of non-positional notations (NPNs), analysis of the cryptographic strength of the created algorithm, and software implementation of the algorithm.

To achieve the research goals the following tasks were set:

- Overview and analysis of cryptographic information security methods;

- Analysis of performance requirements and criteria for cryptographic information security systems;
- Creating a symmetric block encryption algorithm based on a non-positional polynomial notation;
- Software implementation of the created symmetric block encryption algorithm;
- The study of the cryptographic strength of the developed symmetric block encryption algorithm.

The object of research is cryptographic security algorithms and methods of their analysis.

The subject of the research is algorithms for the encryption and generation of round keys based on non-positional polynomial notations.

Research methods: modular arithmetic, non-positional polynomial number systems, statistical tests, bit-scattering tests, cryptanalysis methods.

The scientific novelty of the research. The problem of ensuring information security remains unresolved today. In this regard, a study was carried out, some successes were achieved, and scientific results were published in highly rated journals. The novelty of these scientific results forms the basis of the dissertation. In particular:

- A new symmetric block encryption algorithm has been created using the EM conversion method;
- An S-box substitution table has been created that meets the requirements of protection against cryptanalysis;
- An algorithm for creating round keys has been created;
- To improve encryption speed, an index table of the selected working bases has been created.

The theoretical and practical significance of the work. The results of the dissertation research can be used to protect the information in telecommunication and information systems and networks, electronic document management systems, as well as software products of domestic information and communication technologies, to protect the confidential information of the state and individuals from unauthorized access and theft. Also, they can be used in the educational process in higher education, as well as in the development of new cryptographic protection systems.

The main conclusion of the defense. A new symmetric block encryption algorithm was developed to protect information based on the EM conversion method, which meets the basic requirements of modern symmetric block encryption algorithms.

Besides, the S-box substitution tables used in the algorithm were investigated by linear and differential cryptanalysis of the proposed S-box, and the results were compared with known algorithms. To increase the encryption speed of the algorithm, a non-positional polynomial number system and an index table of the selected working bases were used.

Recommended results for protection. A new block encryption algorithm has been developed. The cryptographic strength of the algorithm was verified

using various cryptanalysis methods and the presentation of the results. The research was carried out jointly with the scientific advisor and foreign scientific advisor.

Implementation of research results. The results of the dissertation research were approved at the Institute of Information and Computational Technologies, the Information Security Laboratory, and implemented within the framework of the BR05236757 project - Development of software and firmware means for cryptographic protection of information during its transfer and storage in infocommunication systems and general-purpose networks."

Testing the results of the dissertation. The main results of the study were presented and discussed at the following conferences and seminars:

- XLI International Scientific and Practical Conference KazATC named after M. Tynyshpaeva on the topic: "Innovative technologies in transport: education, science, practice" (3-4 April 2017, Almaty, Kazakhstan);
- Scientific conference "Modern Problems of Informatics and Computer Technology" of the Institute of Information and Computational Technologies (June 29-30, 2017, Almaty, Kazakhstan);
- II International Scientific and Practical Conference "Informatics and Applied Mathematics" (September 27-30, 2017, Almaty, Kazakhstan);
- III International Scientific and Practical Conference "Informatics and Applied Mathematics" (September 26-29, 2018, Almaty, Kazakhstan);
- "Science of the XXI century: a new approach": Materials of the XXIII international youth scientific and practical conference of students, graduate students, and young scientists. (May 22-23, 2019, St. Petersburg, Russia);
- IV International Scientific and Practical Conference "Informatics and Applied Mathematics" (September 25-29, 2019, Almaty, Kazakhstan);
- Materials of the international scientific and practical conference "Actual problems of information security in Kazakhstan APISK-2020" (January 15, 2020, Almaty, Kazakhstan);
- Scientific and practical seminars on the topic "Actual problems of computer science, mathematics, and management" of the Institute of Information and Computational Technologies (2017-2020, Almaty, Kazakhstan);
- Scientific seminars of the faculty "Information Technology" Kazakh National University. Al-Farabi (2017-2020, Almaty, Kazakhstan).

On the topic of the dissertation, 14 articles were published and 1 copyright certificate was obtained:

1. Khompysh A. Application of non-positional notations, materials of the XLI International scientific-practical conference "Innovative technologies in transport: education, science, practice." Almaty, 2017, P. 64-66.

2. Kapalova N.A., Khompysh A. Development of a modification of the El-Gamal encryption algorithm using a non-positional notation, Bulletin of the Satbayev Kazakh National Technical Research University, Almaty, 2017. No. 4 (122). P. 506-510.

3. Khompysh A. Development of a mobile application of El-Gamal encryption algorithm, materials of the scientific conference "Modern problems of computer technology and computer science." Almaty, 2017, P. 281-284.

4. Khompysh A. Use of El-Gamal encryption algorithm in the data exchange network, based on the non-positional number system, Proceedings of the II International Scientific Conference "Computer Science and Applied Mathematics". Almaty, 2017, P. 157-161.

5. Kapalova N.A., Khompysh A., Algazy K.T. Modification of the algorithm for cryptographic protection of information on the basis of modular reduction. Bulletin of the M. Tynyshbayev Kazakh Academy of Transport and Communications, Almaty, 2018, No. 4 (107), P. 247-253.

6. Khompysh A. Software implementation of the algorithm of cryptographic protection of information on the basis of the modular reduction operation. Proceedings of the III International Scientific Conference "Computer Science and Applied Mathematics", Almaty, 2018, P. 167-171.

7. Khompysh A. Cryptostrength of S-boxes in an encryption algorithm based on EM, "Science of the XXI century: a new approach": Proceedings of the XXIII international youth scientific-practical conference of students, graduate students and young scientists, St. Petersburg, 2019, P. 15-19.

8. Dyusenbaev D.S., Sakan K.S., Khompysh A., Algazy K. Cryptographic analysis of the encryption algorithm "MODNPSS14". Bulletin of the M. Tynyshbayev Kazakh Academy of Transport and Communications, Almaty, 2019, No. 3 (110), P. 235-243.

9. Biyashev R.G., Kapalova N.A., Algazy K.T., Dyusenbaev D.S., Khompysh A. Cryptanalysis of a pseudo-random sequence generator and its modification. Bulletin of the Satbayev Kazakh National Research Technical University, Almaty, 2019, No. 3 (133), P. 179-185.

10. Khompysh A., Kapalova N.A., Algazy K. Evaluation tests on a block encryption algorithm based on the method of EM conversion. IV International Scientific Conference "Computer Science and Applied Mathematics", Kazakhstan, Almaty, 2019, 2, P. 580-587.

11. Biyashev R.G., Algazy K., Khompysh A. The study of the developed algorithms by the criterion of "avalanche effect". Proceedings of the international scientific-practical conference "Actual problems of information security in Kazakhstan APIBK-2020", Almaty, 2020, P. 107-119.

12. Biyashev R.G., Smolarz A., Algazy K.T., Khompysh A. The encryption algorithm Qamal NPNS' based on a nonpositional polynomial notation. Journal of Mathematics, Mechanics and Computer Science, KazNU Bulletin, Almaty, 2020, No. 1 (105), P. 198-207.

13. Kapalova N.A., Khompysh A., Müslüm A., Algazy K. A block encryption algorithm based on exponentiation transform, Cogent Engineering (2020), 7:1788292, ISSN 2331-1916, V. 7, P. 1-12

14. Khompysh A., Kapalova N.A., Algazy K. The study of the developed algorithm on the basis of the EM conversion under the criterion of "avalanche

effect". Bulletin of the M. Tynyshbayev Kazakh Academy of Transport and Communications, Almaty, 2020, No. 3 (114), P. 284-292.

15. Khompysh A., Kapalova N.A. CryptoEM v1.0.1 file encryption program, copyright certificate for computer software, No. 5450, September 24, 2019.

The structure and scope of the thesis. The structure of the dissertation consists of an introduction, 3 chapters, a conclusion, a list of references, and 4 annexes.

The introduction substantiates the relevance of the problem of constructing algorithms for cryptographic protection of information that meets the requirements for modern block algorithms by current users, formulates the purpose of the work, defines the general scientific problem and its division into specific scientific problems, defines the object and topic of research, presents the main provisions, reflects the novelty dissertation work submitted for defense, and its results

The first section, taking into account the fact that one of the most effective ways to solve the problems mentioned in the dissertation is cryptographic methods, considers the basic concepts of cryptographic methods, terms and basic classes of cryptographic transformations, the main stages of symmetric block cipher algorithms, and requirements for block cipher algorithms.

The second section describes the developed symmetric block encryption algorithm based on non-positional polynomial number systems, as well as approaches to creating polynomials, the main parameters of the algorithm, the encryption and decryption scheme, as well as the EM transformation method, the S-block replacement table, the order of operation and fast construction in degree, and algorithm for generating round keys.

The third section describes the created software package for the new block encryption algorithm presented in the thesis. To test the cryptographic security of the algorithm, the results of testing the statistical security of the ciphertext using evaluation and graphical tests were presented. Also, the results of the study of the algorithm using the bit scattering criterion, linear and differential cryptanalysis of the S-box, differential analysis for all modifications of the algorithm are described.

The conclusion formulates the main of the work.