Development and research of encryption algorithms based on different approaches

by

Kunbolat Tileukhanuly Algazy

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy (Ph.D.) in the specialty "6D100200 - Information Security Systems"

ABSTRACT

The relevance of the research topic is determent by the modern development of information and communication technologies and the need to improve models for protecting electronic information in order to ensure information security. The processes of handling, storing, transferring, and using information have become a priority in modern society and largely depend on the level of development and use of communication means and methods of transferring information. In the current situation, the necessity to protect information is needed not only by the public sector but also by ordinary users and non-governmental organizations. One of the topical issues of ensuring the security of information is to ensure the required level of its protection by creating modern means of information protection.

Information and communication technologies play an important role in a sovereign state. Kazakhstan, in 2017, adopted the Cybersecurity Concept ("Cyber Shield of Kazakhstan"). The goal of the concept is to achieve and maintain the level of protection of electronic information resources, information systems, and information and communication infrastructure from external and internal threats to ensure the sustainable development of the Republic of Kazakhstan in the context of global competition. In this regard, the creation of domestic information security systems that meet modern information security requirements is urgent.

The Information Security Laboratory of the Institute of Information and Computational Technologies of the RK MES CS carries out research work on the creation of domestic cryptographic information protection facilities, namely, on the development of symmetric block encryption systems for electronic data, including those based on non-positional polynomial notations.

Currently, block encryption algorithms are the main means of cryptographic protection of information stored in computers or transmitted through public infocommunication networks. The demand for encryption algorithms of this type is due to the advantages of their practical application. Driven by their efficient implementation based on modern hardware and software devices, a high encryption speed and level of security are guaranteed. Symmetric block ciphers are used not only as stand-alone cryptographic algorithms, but also as important cryptographic mechanisms that are part of other cryptographic algorithms and protocols. They are often used in practice as a key component of pseudo-random sequence generators and cryptographic hashing algorithms.

Another advantage of block ciphers is the use of short keys. It is possible to encrypt several large files or other data with one short key, the length of which is generally in the range of 128 to 256 bits. This is a major advantage over stream ciphers, for which it is not recommended to use the key more than once. Storing long keys and exchanging them between users requires additional security. Given the above, block ciphers are the most efficient and suitable ciphers to use. Therefore, symmetric block cipher algorithms are currently the main cryptographic means for ensuring the confidentiality of information.

With the development of cryptography, cryptographic attacks and cryptanalysis techniques have evolved. The concepts of cryptography and cryptanalysis have become inextricably linked – they are two constituent parts of cryptology. In order to create a system that is resistant to hacking, it is necessary to take into account all possible ways of attacking it. The importance of cryptography and cryptanalysis will only increase; therefore, the development of cryptographic algorithms is **relevant** both in scientific research and in practical applications.

In Kazakhstan, foreign cryptographic tools and software are mainly used to protect the information, therefore the development of Kazakhstani domestic cryptographic protection means is definitely relevant and necessary.

The purpose of the dissertation work. Development of an iterative block cipher and a function for generating round encryption keys using the capabilities of non-positional polynomial notations (NPNs). Study of the cryptographic strength of the developed algorithms.

Research objectives:

- Analysis of existing symmetric block algorithms for cryptographic information protection;
- Review and analysis of known cryptanalysis and cryptographic attack techniques;
- Development of symmetric block encryption algorithms based on a substitution-permutation network and the function of deriving round encryption keys using non-positional polynomial notations (NPNs);
- Research by methods of cryptanalysis of the strength of the developed encryption algorithms;
- Software implementation of the developed iterative block encryption algorithms.

The object of study. Encryption systems, non-positional polynomial notations, cryptographic attacks, cryptanalysis methods.

The subject of study. Symmetric block cryptographic encryption algorithms, including those based on NPNs.

Research methods. The paper uses methods of the theory of Boolean functions, linear algebra, and probability theory, as well as various cryptographic methods and algorithms, and cryptanalysis techniques.

The scientific novelty of the research:

- A new symmetric block encryption algorithm with a substitution-permutation network architecture was developed that meets the general requirements of encryption algorithms;

- On the basis of an unconventional method (NPNs) a symmetric block encryption algorithm is built. The use of this algorithm makes it possible to increase the cryptographic strength of the algorithm;

- The nodes of nonlinear (S-block) replacement were built, which have increased indicators of strength to differential and linear cryptanalysis.

The theoretical and practical significance of the work. The research and the results obtained are of high practical importance and can be used to protect confidential information during its storage and transmission in infocommunication systems and networks. Besides, these results on the creation and development of domestic information security facilities expand the theory of creating effective information encryption algorithms. Developed an iterative block encryption algorithm for software implementation and received a copyright certificate for "Qamal v 1.0.1", No. 5200 dated September 6, 2019, issued by the National Institute of Intellectual Property of the MJ RK.

The main conclusion of the defense. A new symmetric block encryption algorithm was built that meets the general requirements for encryption algorithms. A second version of the encryption algorithm using non-positional polynomial notations is also proposed. The cryptographic strength of the developed encryption algorithms by methods of linear, differential, and algebraic cryptanalysis was studied.

Confidence level and results of approbation. The reliability of the research and the results of the dissertation are shown in the third section.

The results of the dissertation were reported and discussed at the following scientific and practical conferences:

1) III International Scientific and Practical Conference "Informatics and Applied Mathematics" (Almaty, September 26-29, 2018).

2) International Conference on Wireless Communication, Network, and Multimedia Engineering, WCNME-2019 (Guilin, China, 2019).

3) IV International Scientific and Practical Conference "Informatics and Applied Mathematics" (Almaty, September 25-29, 2019).

4) International Conference on Security of Information and Networks (Sochi, Russia, September 2019).

5) International Scientific and Practical Conference "Actual problems of information security in Kazakhstan APISK-2020" (Almaty, January 15, 2020).

6) V International Scientific and Practical Conference "Informatics and Applied Mathematics" (Almaty, September 29 - October 1, 2020).

Connection of the topic of the dissertation with the plans of research works. The dissertation work was carried out in accordance with the plan of the Ph.D. doctoral dissertation, approved by the Institute of Information and Computational Technologies of the RK MES CS and with the plan of research work of the program-targeted financing project "Development of software and hardware-software for cryptographic protection of information during its transmission and storage in infocommunication systems and general-purpose networks" (2018-2020, State registration number: BR05236757). The results of the research on this dissertation work are included in the reports of this PTF project for 2018-2020.

The volume and structure of the work. The dissertation consists of an introduction, four sections, a conclusion, and a list of references. The total volume of the dissertation is 118 pages of written text including 23 figures, 42 tables, a bibliography from 94 sources, and 4 appendices.

Publication of results. The number of published scientific articles during research work is 21 including 3 articles in journals indexed in the Scopus and Thomson Reuters databases ("Cogent Engineering" and "International Journal of Electronics and Telecommunications"), 8 articles in publications recommended by the Committee on Control in the Field of Education and Science of the Ministry of Education and Science of the Republic of Kazakhstan, 10 articles were published in the collections of international scientific conferences.

The introduction substantiates the relevance of the dissertation work. The purpose of the work, the object, and the subject of the research work are formulated. The scientific novelty and practical significance are determined. The results of the conducted research are described. Information on the approbation of the research results and publication is provided.

The first section describes the classification and main directions of research in information security algorithms. The terms used in cryptography and the dissertation work are given. Cryptoalgorithms divided by the degree of security, requirements for symmetric block ciphers, and encryption modes used in encryption are described. The main types of cryptanalysis applied to modern encryption algorithms are considered.

The second section describes the new symmetric block encryption algorithm Qamal, developed on the basis of an SP network, and the proposed second version of this algorithm Qamal NPNS due to the peculiarities of using the key. All used transformations in these algorithms are described in detail. The length of the encryption block and the algorithm key can take on three different values according to different security levels. The structure of the created S-box for the developed encryption algorithm is given. Since Qamal NPNS is an algorithm developed on the basis of the NPNs, information is provided on the construction of non-positional polynomial notations and their use in encryption and decryption. An example of data encryption using the developed algorithm is given.

The third section presents the results obtained in the study of the reliability of the developed encryption algorithm. The analysis begins by checking the statistical security of the ciphertext obtained using the encryption algorithm. Then, the properties of the avalanche effect of the cipher are checked, which is one of the prerequisites in cryptography. The cryptographic strength of the algorithm was verified by algebraic, differential, linear, and other cryptanalysis methods. The theoretical results of crypto attacks, tested on specific examples, are presented. Also, the influence of the encryption algorithm using NPNs on the cryptographic strength was investigated and established.

The fourth section describes the created software that implements the developed symmetric block encryption algorithm, as well as the programming language, system requirements, the description of the software operation, etc. To assess the computational speed of the program, three different ways of implementing

the Mixer2 transformation used in the developed algorithm are considered. encryption. The results obtained are compared.

In the conclusion, the main results obtained in the dissertation are formulated.