IRSTI 81.93.29 https://doi.org/10.26577/JMMCS.2020.v105.i1.16

[1]R.G. Biyashev, [2]A. Smolarz, [3]K.T. Algazy, [4]A.Khompysh

[1]Doctor of Technical Sciences, Institute of Information and Computational Technologies of the RK MES CS, Almaty, Kazakhstan, E-mail: brg@ipic.kz
[2]Doctor of Technical Sciences, Lublin University of Technology, Lublin, Poland, E-mail: a.smolarz@pollub.pl
[3]PhD student, Al-Farabi Kazakh National University, Almaty, Kazakhstan, E-mail: kunbolat@mail.ru
[4]PhD student, Institute of Information and Computational Technologies of the RK MES CS, Almaty, Kazakhstan, E-mail: ardabek@mail.ru

ENCRYPTION ALGORITHM "QAMAL NPNS"BASED ON A NONPOSITIONAL POLYNOMIAL NOTATION

Processing, storage, and transmission of information are important processes in modern society. The practical application of cryptography has become an integral part of the life of modern society. In Kazakhstani, for the protection of the electronic information are mainly used foreign software and hardware-software tools . Therefore, the development of Kazakhstan cryptographic protection tools is certainly necessary. This article describes the new Qamal NPNS encryption algorithm, which is a modification of the previously developed Qamal encryption algorithm. The modification lies in the use of a transformation based on a non-positional polynomial notation (NPN). To build a new encryption algorithm, an SP-network is also used. The theoretical justification of the appropriateness of applying the NPN and the results of the analysis of the encryption algorithm are given. Algebraic cryptanalysis for multiplication in non-positional polynomial notations was considered separately. The study of the algorithm strength for separate procedures showed good results, which suggest the cryptographic strength of the developed algorithm.

Key words: cryptography, encryption, S-box, non-positional polynomial notation, SP-network.

[1]Р.Г. Бияшев, [2]А. Смоларш, [3]К.Т. Алгазы, [4]А. Хомпыш

[1]т.ғ.д., ҚР БжҒМ ҒК, Ақпараттық және есептеуіш технологиялар институты, Алматы қ., Қазақстан, E-mail: brg@ipic.kz
[2]т.ғ.д., Люблин Техникалық университеті, Люблин қ., Польша, E-mail: a.smolarz@pollub.pl
[3]докторант, әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қ., Қазақстан, E-mail: kunbolat@mail.ru
[4]докторант, ҚР БжҒМ ҒК, Ақпараттық және есептеуіш технологиялар институты, Алматы қ., Қазақстан, E-mail: ardabek@mail.ru

«QAMAL NPNS» шифрлеу алгоритмінің позициялы емес полиномдық санау жүйесін пайдаланған модификациясы

Ақпаратты өңдеу, сақтау және алмасу қазіргі қоғамдағы маңызды процесс болып табылады. Криптографияны іс жүзінде қолдану қазіргі қоғам өмірінің ажырамас бөлігіне айналды. Қазақстанда электронды ақпаратты қорғау үшін негізінен шетелдіік бағдарламалық және аппараттық-бағдарламалық құралдар қолданылады. Сондықтан да қазақстандық криптографиялық қорғаудың құралдарын әзірлеу қажет. Бұл мақалада бұрын әзірленген Qamal шифрлеу алгоритмінің жаңа модификациясы сипатталады. Модификация позициялы емес полиномдық санау жүйелеріне (ПЕПСЖ) негізделген шифрлеу алгоритмін құру үшін SP желісі қолданылған. Сонымен қатар шифрлеуде ПЕПСЖ пайдалану мақсатының дұрыстығына теориялық түсініктеме берілді және шифрлеу алгоритмін талдау нәтижелері келтірілді. Позициялық емес полиномдық санау жүйелеріндегі көбейтуге арналған алгебралық криптоталдау нәтижелері бөлек көрсетілген. Сонымен қатар, алгоритмде пайдаланылған басқа да процедураларға арналған беріктілігін зерттеу жұмыстары жақсы нәтижелер көрсетті. Бұл өз кезегінде әзірленген алгоритмнің криптографиялық берік болатындығына болжам жасауға негіз болып табылады.

Түйін сөздер: криптография, шифрлеу, S блок, позициялы емес полиномдық санау жүйесі, SP жүйесі.

[1]Р.Г. Бияшев, [2]А. Смоларш, [3]К.Т. Алгазы, [4]А. Хомпыш
[1]д.т.н., Институт информационных и вычислительных технологий КН МОН РК,
г. Алматы, Казахстан, E-mail: brg@ipic.kz
[2]д.т.н., Люблинский Технический университет, г. Люблин, Польша, E-mail: a.smolarz@pollub.pl
[3]докторант, Казахский национальный университет имени аль-Фараби,
г. Алматы, Казахстан, E-mail: kunbolat@mail.ru
[4]докторант, Институт информационных и вычислительных технологий КН МОН РК,
г. Алматы, Казахстан, E-mail: ardabek@mail.ru

Алгоритм шифрования "QAMAL NPNS"с использованием непозиционной полиномиальной системы счисления

Обработка, хранение и передача информации являются важными процессами в современном обществе. Практическое применение криптографии стало неотъемлемой частью жизни современного общества. В Казахстане для защиты электронной информации применяются в основном зарубежные программные и аппаратно-программные средства. Поэтому разработка казахстанских средств криптографической защиты безусловно является необходимой. В данной статье описывается новый алгоритма шифрования «Qamal NPNS», который является модификацией ранее разработанного алгоритма шифрования «Qamal». Модификация заключается в использовании преобразования, основанного на непозиционной полиномиальной системе счисления (НПСС). Для построения нового алгоритма шифрования также применяется SP-сеть. Приводятся теоретическое обоснование целесообразности применения НПСС и результаты анализа алгоритма шифрования. Отдельно приведены результаты алгебраического криптоанализ для умножения в непозиционных полиномиальных системах счислениях. Исследование стойкости алгоритма для отдельных процедур показало хорошие результаты, что предполагает криптостойкость разрабатываемого алгоритма.

Ключевые слова: криптография, шифрование, S-блок, непозиционная полиномиальная система счисления, SP-сеть.

1 Introduction

The science of secret transmission of information arose in ancient times. The development of writing and communications has greatly advanced its formation. The advent of affordable internet has taken cryptography to a new level. Due to the increasing dependence of society on information technology and the need to ensure information security, the use of cryptographic methods has become relevant for almost everyone. However, secrecy can be inferior in importance to ensuring integrity, authenticity and other aspects of security. The invention of new principles of cryptography and the emergence of the so-called public key cryptography gave a powerful impetus to the widespread use of this science for the needs of civil society, business, banking and other fields of activity [1].

Cryptographic information protection is one of the main subsystems of any information protection system. The processes of handling, storage, transmission and use of information become dominant in the life of modern society [1-3]. All specific tasks of cryptography substantially depend on the level of development of engineering and technology, on the means of communication used, and the methods of transmitting information [4, 5].

2 Literature review

The security of sensitive information has begun to be governed primarily by the key. The encryption algorithm itself is considered to be known to the enemy and available for study, but the algorithm provides for the use of an unknown to the adversary key, on which the applied information transformations substantially depend [3-6].

Claude Shannon was the first who with mathematical rigor formulated questions about the absolute and theoretical strength of ciphers. Namely, to what extent a cryptosystem is resistant to an attacker with unlimited resources [7]. Requirements for perfect secrecy: 1) the key is truly random (equally probable); 2) the key is exactly as long as the message that is encrypted; 3) the key is used one time only. In case of violation of at least one of these conditions, the cipher ceases to be completely unbreakable, and there appear possibilities in principle to break it. But these conditions make a completely unbreakable cipher very expensive and impractical. Before using such a cipher, it is necessary to provide all subscribers with a sufficient supply of random keys and exclude the possibility of their repeated use. And this is extremely difficult and expensive to do [5, 6]. Therefore, completely unbreakable ciphers are used only in communication networks with a small amount of transmitted information, and these are usually networks for transmitting sensitive or critical information.

Most typically, legitimate users are forced to use not completely unbreakable ciphers to protect their information. Symmetric block encryption algorithms have gained wide use, and now they are the main cryptographic means to ensure confidentiality in the processing of information in modern information and telecommunication systems [5-7].

The main types of block ciphers are a Feistel network and a substitution-permutation network (SP-network). An SP-network is a block cipher in which the transformation of each round is a combination of substitutions (S-boxes) and permutations. Two fundamental principles for constructing cryptographic transformations, confusion and diffusion, proposed by Claude Shannon in 1949, can clearly be implemented in the structure of SP-network[7-9]. Recall that confusion means complicating all kinds of connections between the plaintext and the ciphertext. Examples of SP-networks are the ciphers IDEA, AES (Rijndael), Serpent, Kuznyechik [10-13]. Every day there are more and more such examples. It is the new practical applications of cryptography that are one of the sources of its development.

For Kazakhstan, information and communication technologies play a big part in the development of the young state. In 2017, the Cybersecurity Concept was adopted. The objectives of the Concept are to achieve and maintain the level of security of electronic information resources, information systems, and the information and communication infrastructure from external and internal threats, ensuring sustainable development of the Republic of Kazakhstan in the context of global competition [14].

In recent years, the Institute of Information and Computational Technologies of the Science Committee of the Ministry of Education and Science of the Republic of Kazakhstan has carried out research on the study of symmetrical block encryption algorithms for electronic messages and has developed various modifications, including those based on non-positional polynomial notations (NPNs) [15-21]. These works, in turn, will contribute to the creation of domestic cryptographic information protection facilities.

3 Materials and methods

The paper [19] introduced the new symmetric block encryption algorithm Qamal. The Qamal algorithm scheme is shown in Figure 1 (a). The encryption algorithm includes pairing a plaintext with a key using the bitwise addition (XOR) operation, a substitution S-box, and mixing procedures Mixer1 and Mixer2.

The considered algorithm is a modification of the above one, where a non-positional polynomial notation is used (Figure - 1 (b)). Instead of the operation of pairing (addition) a key modulo 2 (XOR operation) to a plaintext block, multiplication by the NPN is performed. For this reason, the algorithm was named Qamal NPNS. The developed algorithm supports a fixed block and a key length of 128 bits. This is yet another difference from the basic algorithm.

Building an NPN is the selection of its bases designated as working bases. Let some irreducible polynomials be chosen as such bases:

$$p_1(x), p_2(x), ..., p_S(x) \tag{1}$$

Let us denote their degrees by $m_1, m_2, ..., m_S$ respectively. The polynomials (1), considering their arrangement, form a single system of bases. The main working range of the NPN is the polynomial $P^m(x) = p_1(x)p_2(x)...p_S(x)$ of degree $m = \Sigma_{i=1}^{S} m_i$. In the NPN, any polynomial $F(x)$ whose degree is fewer than m has a unique non-positional representation in the form of a sequence of residues of its division by the bases(1):

$$F(x) = (\alpha_1(x), \alpha_2(x), ..., \alpha_S(x)), \tag{2}$$

where $\alpha_i \equiv F(x)(mod p_i(x)), i = 1, ..., S$. The positional notation of $F(x)$ is restored by its nonpositional form (2) [22-25]:

$$F(x) = \Sigma_{i=1}^{S} \alpha_i(x) B_i(x)$$

where

$$B_i(x) = \frac{p^m(x)}{p^i(x)} M_i(x) \equiv 1(mod p_i(x)). \tag{3}$$

The polynomials $M_i(x)$ are selected in such a way as to satisfy the congruence in (3). In the case of only the transmission and storage of information, the positional form of the polynomial $F(x)$ according to the formula:

$$F(x) = \Sigma_{i=1}^{S} \alpha_i(x) P_i(x)$$

where

$$P_i(x) = \frac{p^m(x)}{p^i(x)}. \tag{4}$$

Each working base must have a degree not higher than the value of L (in our case, 128). The bases (1) are selected from among all irreducible polynomials of degree $m_1 to m_S$ with the condition that equation (4) holds:

$$k_1 m_1 + k_2 m_2 + ... + k_S m_S = L. \tag{5}$$

In the equation (5), $0 < k_i < n_i, i = 1, ..., S$ are unknown coefficients and the number of selected irreducible polynomials of degree m_i. One specific set of these coefficients is a solution of (5) and defines one system of working bases, n_i is the number of all irreducible polynomials of degree $m_i, 1 \leq m_i \leq L, S = k_1 + k_2 + ... + k_S$ is the number of selected working

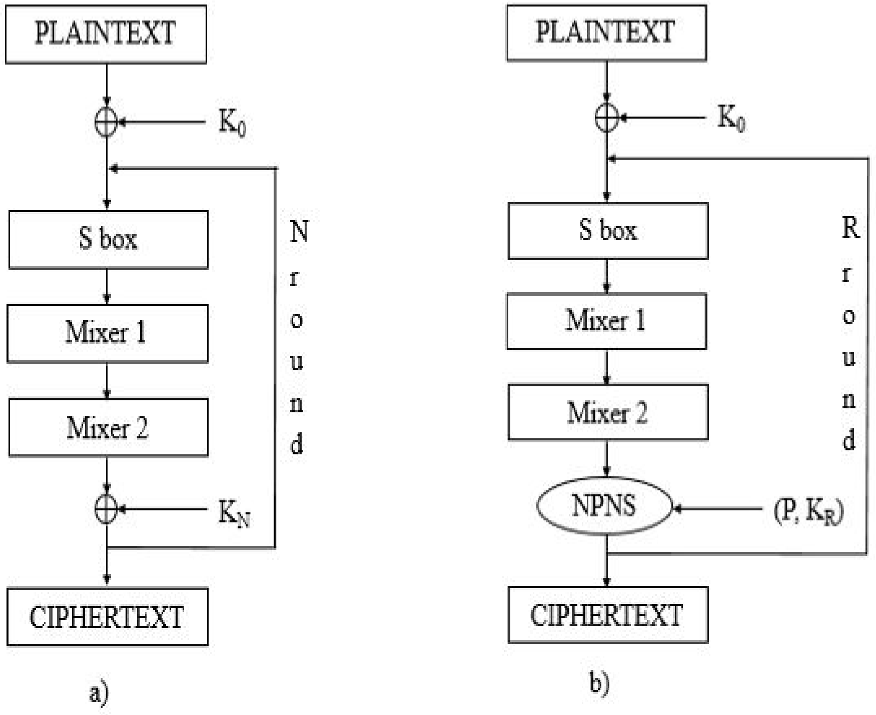

Figure 1: Qamal encryption algorithm scheme, b) Qamal NPNS encryption algorithm scheme

bases. Complete residue systems modulo polynomials of degree m_i include all polynomials of degree at most m_{i-1}, for the notation of which m_i bits are required.

Encryption. The used key sequence of L bits long is also interpreted as the sequence of remainders $k_1(x), k_2(x), ..., k_S(x)$, but from dividing some other polynomial K(x) by the same working bases of the system:

$$K(x) = k_1(x), k_2(x), ..., k_S(x). \tag{6}$$

where $K(x) \equiv k(x)(modp_i(x)), i = 1, ..., S$. Then, as a cryptogram $\omega_1(x), \omega_2(x), ..., \omega_S(x)$, some encryption function $H(F(x), K(x))$ can be considered:

$$H(x) = \omega_1(x), \omega_2(x), ..., \omega_S(x). \tag{7}$$

where $H(x) \equiv \omega_i(x)(modp_i(x)), i = 1, ..., S.$

In accordance with the operations in the NPN, the operations in the functions F(x), K(x), H(x) are performed in parallel modulo the polynomials (1) selected as the working bases of the NPN.

For encryption, elements of the residue sequence $\omega_1(x), \omega_2(x), ..., \omega_S(x)$ in the cryptogram are used, which are the least remainders on dividing the products $\alpha_i(x)k_i(x)$ by the corresponding bases $p_i(x)$, if the multiplication operation is used as the function $H(F(x), K(x))$ [22-25]:

$$\alpha_i(x)k_i(x) \equiv \omega_i(x)(modp_i(x)), i = 1, ...S. \tag{8}$$

Decryption. When decrypting the cryptogram H(x) using the known key $K(x)$, for each value $k_i(x)$, we calculate, as follows from (8), the reciprocal (inverse) polynomial $k_i^{(-1)}(x)$ from the following congruence:

$$k(x)k_i^{(-1)}(x) = 1(modp_i(x)), i = 1, ..., S \tag{9}$$

The result is the polynomial

$$K^{(-1)}(x) = (k_1^{(-1)}(x), k_2^{(-1)}(x), ..., k_S^{(-1)}(x))$$

which is inverse to the polynomial K(x). Then the elements of the residue sequence (2) in accordance with (8) and (9) are restored by the congruence:

$$\alpha_i(x) = k_i^{(-1)}(x)\omega_i(x)(modp_i(x)), i = 1, ..., S$$

Thus, in the considered model of the encryption algorithm for an electronic message of a given length L bits in the NPN, the complete key is the selected system of the polynomial working bases $p_1(x), p_2(x), ..., p_S(x)$ and the inverse key $K^{(-1)}(x) = (k(x), k_2^{(-1)}(x), ..., k_S^{(-1)}(x))$ to decrypt the message.

Round keys. The round-key generation algorithm remains the same as in the basic algorithm [19]. The round keys K_i are generated from the cipher key K_0 using the key extension procedure. As a result, an array of round keys is formed, from which the required round key is then directly selected.

The complete key in the developed encryption algorithm modification is comprised of the chosen system of polynomial bases $p_1(x), p_2(x), ..., p_S(x)$, the key $K(x) = (k_1(x), k_2(x), ..., k_S(x))$ obtained while generating a pseudo-random sequence, and the inverse key $K^{(-1)}(x) = (k_1^{(-1)}(x), k_2^{(-1)}(x), ..., k_S^{(-1)}(x))$ calculated according to expression (9).

4 Results and discussions

4.1 Encryption algorithm analysis

The main methods for analyzing the strength of such algorithms include brute force attacks, statistical and algebraic methods. Brute force attacks are to check all possible keys by using them to decrypt the ciphertext and then to verify whether the result obtained represents a plaintext.

Statistical methods for purposes of analysis use some statistical dependence of the algorithm, which is performed for the correct key with a greater frequency than for a false key.

The basis of algebraic methods is the building of a system of linear equations in which the elements of plaintext and key are selected as variables. When solving the system of equations using the linearization method, the possibility of finding key elements in parts is considered.

Keyspace calculation. In the algorithm, the key consists of two parts that are generated independently of each other. The length of each key is 128 bits. One part of the key is a pseudo-random sequence generated for the bitwise addition operation and for the non-positional encryption system. In an NPN, the second part of the key is the selected set of polynomial bases $p_1(x), p_2(x), ..., p_S(x)$. It is known that the number of operations to enumerate all candidate keys with a length of 128 bits is equal to 2^{128}. The cryptographic strength of the encryption algorithm based on an NPN is determined by the number of all possible and different options for choosing complete keys. The cryptostrength of encryption of a message of a given length L is calculated by the formula [26]:

$$Q_k = 2^L \cdot \Sigma_{k_1,k_2,...,k_S}(k_1 + ... + k_S)!C_{n_1}^{k_1}...C_{n_S}^{k_S} \tag{10}$$

To find the exact value of Q_k for each L, it is necessary to calculate the number of irreducible polynomials of degrees up to L and the compositions of L.

The number of irreducible binary polynomials of degree L is calculated by the following formula [26]:

$$I_L = \frac{1}{L}\sum_{d\backslash L}\mu(d)2^{L/d} = \frac{1}{n}\sum_{d\backslash L}\mu(L/d)2^d$$

where d are divisors of L, $\mu(x)$ is the Mobius function defined as follows:

$$\begin{cases} 0, & \text{if } x \text{ has a squared prime factor} \\ (-1)^k, & \text{if } x \text{ is the product of } k \text{ different numbers} \\ +1, & \text{if x=1} \end{cases}$$

Table 1 shows the values of I_L from 1 to 32. If $L = 128$, then $I_L \approx 2^{122}$.

Table 1: Values of I_L from 1 to 32

I	I_L	I	I_L	I	I_L	I	I_L
1	2	9	56	17	7,710	25	1,342,176
2	1	10	99	18	14,532	26	2,580,795
3	2	11	186	19	27,594	27	4,971,008
4	3	12	335	20	52,377	28	5,586,395
5	6	13	630	21	99,858	29	18,512,790
6	9	14	1,161	22	190,557	30	35,790,267
7	18	15	2,182	23	364,722	31	69,273,666
8	30	16	4,080	24	698,870	32	134,215,680

It is known from the theory of numbers that in the general case for the number L there are 2^{L-1} compositions, of which exactly C_{L-1}^{k-1} ones have the length of k.

Based on this fact, the total number of complete keys was calculated for different values of L. For L equal to 16, 32, and 64, the number of enumeration operations is 2^{34}, 2^{69}, and 2^{138}, respectively. Taking into account these calculations, it is suggested that when L takes the value of 128, the number of enumeration operations is close to 2^{276}.

4.2 Algebraic analysis results

Algebraic methods are based on the algebraic properties of an information transformation algorithm. The strength of algorithms against statistical methods depends on the amount of accumulated information about plaintexts and the corresponding converted texts. Algebraic methods usually do not require a lot of statistics when using the same key.

Algebraic cryptanalysis for multiplication in non-positional polynomial notations was considered separately. For multiplication in an NPN, a partial attack was used. Earlier studies had been conducted in this direction [27]. The system of equations binding the key, plaintext, and ciphertext in the encryption scheme based on an NPN for one irreducible polynomial is given below:

$$\begin{cases} c_{n-1}d_{n-1} \bigoplus k_n s_{n-2} = 0 \\ c_{n-1}d_{n-2} \bigoplus c_{n-2}d_{n-1} \bigoplus k_n s_{n-3} \bigoplus k_{n-1}s_{n-2} = 0 \\ ... \\ c_{n-1}d_1 \bigoplus c_{n-2}d_2 \bigoplus ... \bigoplus c_1 d_{n-1} \bigoplus k_n s_0 \bigoplus k_{n-1}s_1 \bigoplus ... \bigoplus k_2 s_{n-2} = 0 \\ c_{n-1}d_0 \bigoplus c_{n-2}d_1 \bigoplus ... \bigoplus c_0 d_{n-1} \bigoplus k_{n-1}s_0 \bigoplus ... \bigoplus k_1 s_{n-2} = a_{n-1} \\ c_{n-2}d_0 \bigoplus c_{n-3}d_1 ... \bigoplus c_0 d_{n-2} \bigoplus k_{n-2}s_0 \bigoplus k_{n-3}s_1 \bigoplus ... \bigoplus k_0 s_{n-2} = a_{n-2} \\ ... \\ c_2 d_0 \bigoplus c_1 d_1 \bigoplus c_0 d_2 \bigoplus k_2 s_0 \bigoplus k_1 s_1 \bigoplus k_0 s_2 = a_2 \\ c_1 d_0 \bigoplus c_0 d_1 \bigoplus k_1 s_0 \bigoplus k_0 s_1 = a_1 \\ c_0 d_0 \bigoplus k_0 s_0 = a_0 \end{cases}$$

Here $c = (c_{n-1}, c_{n-2}, ..., c_2, c_1, c_0)$ is a numerical sequence of the given ciphertext, $a = (a_{n-1}, a_{n-2}, ..., a_2, a_1, a_0)$ is a sequence of characters of the unknown plaintext, $k = (k_n, k_{n-1}, ..., k_2, k_1, k_0)$, $d = (d_{n-1}, d_{n-2}, ..., d_2, d, d_0)$, and $s = (s_{n-2}, s_{n-3}, ..., s_2, s_1, s_0)$ are the sequences of unknown variables.

In this context, the input data are random sequences resulting from other transformations. It was shown in [25] that after one cycle, each bit of the intermediate result depends on each bit of the plaintext and on the key. Minimal changes in the plaintext or in the key lead to changes of about 50% of the bits (an avalanche effect). In view of the above, an attack in parts is impractical.

In the case of an algebraic attack, provided that the ciphertext and plaintext are known, the number of search operations for finding the key lies within the following interval [27]:

$$\sum_{i=1}^{s} I(m_i) \leqslant J(m) < \prod_{i=1}^{s} I(m_i)$$

where $I(m_i)$ is the number of irreducible polynomials of degree fewer than m_i, $J(m)$ is the number of search operations for complete keys of length m.

5 Conclusion

The study of the cryptostrength of the algorithm begins with the cryptanalysis of each transformation separately. Then, depending on the results obtained, an analysis of the entire algorithm, i.e. for the whole round transformation, is conducted.

The basis of algebraic methods is combining a set of equations describing the internal transformations in the cipher system, and solving the simultaneous equations. Typically, these internal transformations include linear and non-linear parts. Developers of modern encryption systems often use S-boxes, which due to their non-linearity significantly increase the level of strength of such encryption systems against algebraic cryptographic attacks. In addition, in order to complicate the use of analytical approaches, iterative (round) schemes are widely used, when the transformation output is again fed to the input a certain number of times.

The study of the algorithm strength for separate procedures showed good results, which suggest the cryptographic strength of the developed algorithm and the possibility to study the algorithm comprehensively, i.e. considering all transformation procedures and rounds. Work in this direction is ongoing. The results will be presented in the following publications.

6 Acknowledgments

This work was supported by a targeted funding program «Development of software and hardware and software for cryptographic protection of information during its transmission and storage in infocommunication systems and general purpose networks» from the Committee of Science of the Ministry of Education and Science of the Republic of Kazakhstan (registration number 0118PK01064).

References

[1] Kamol Lek, Naruemol Rajapakse, "Cryptography: Protocols, Design, and Applications" , *Nova Science Publishers* (2012): 242.

[2] Keith Martin, "Everyday Cryptography: Fundamental Principles and Applications" , *Oxford University Press* (2012): 560.

[3] Gatchenko N.A., Isaev A.S., Yakovlev A.D., "Kriptograficheskaya zashchita informatsii [Cryptographic protection of information]" , *Spb: NIU ITMO* (2012): 142.

[4] Camel Tanougast, "Progress in Data Encryption Research" , *Nova Science Publishers Inc* (2013): 158.

[5] Yaschenko V.V., "Vvedeniye v kriptografiyu [Introduction to Cryptography" , *SPb: Peter* (2001): 348.

[6] Douglas R. Stinson, Maura B. Paterson, "Cryptography: Theory and Practice" , *Boca Raton, CRC Press, Taylor & Francis Group* (2019): 580.

[7] Tokareva N.N., "Symmetric Cryptography [Simmetrichnaya kriptografiya]" , *NSU, Novosibirsk* (2012): 234.

[8] Wenbo Mao, "Modern Cryptography: Theory and Practice" , *Prentice Hall PTR* (2003): 648.

[9] Bruce Shnier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C" , *John Wiley & Sons* (1996): 784.

[10] William Stallings, "Cryptography and Network Security: Principles and Practice" , *Pearson; 6 edition* (2013): 752.

[11] F.L.Bauer, "Decrypted Secrets. Methods and maxims of cryptology" , *Springer-Verlag Berlin, Fourth, Revised and Extended Edition* (2006): 555.

[12] L. K. Babenko, E. A. Ischukova, "Sovremennyye algoritmy blochnogo shifrovaniya i metody ikh analiza [Modern Block Encryption Algorithms and Methods of their Analysis]" , *Moscow, Helios, ARV* (2006): 376.

[13] Alferov A.P., Zubov A.Yu., Kuzmin A.S., Cheremushkin A.V., "Osnovy kriptografii [Fundamentals of cryptography]" , *M.: Helios ARV* (2001): 479.

[14] Alferov A.P., Zubov A.Yu., Kuzmin A.S., Cheremushkin A.V., "Kontseptsiya kiberbezopasnosti "Kibershchit Kazakhstana"[Concept of Cybersecurity "Cyber Shield of Kazakhstan"]" , *Approved by Decree of the Government of the Republic of Kazakhstan* (2017): 407.

[15] R. G. Biyashev, S. E. Nyssanbayeva , "Algorithm for Creation a Digital Signature with Error Detection and Correction" , *Cybernetics and Systems Analysis* Vol. 48, No. 4, (2012): 489-497.

[16] Biyashev R., Nyssanbayeva S., Kapalova N., "The Key Exchange Algorithm on Basis of Modular Arithmetic" , *Proceedings of International Conference on Electrical, Control and Automation Engineering (ECAE2013), Hong Kong ? Lancaster, U.S.A.: DEStech Publications,* (2013): 16.

[17] Kapalova N., Haumen A., "The model of encryption algorithm based on non-positional polynomial notations and constructed on an SP-network" , *Open Engineering,* Volume 8, Issue 1, (2018): 140-146.

[18] Amerbayev V.M., Biyashev R.G., Nyssanbaeva S.E., "Use of nonpositional notations in cryptographic protection" , *Izv. Nat Acad. of Sciences Resp. Kazakhstan, Ser. Phys.-Mat,* No 3 (2005): 84-89.

[19] Amerbayev V.M., Biyashev R.G., Nyssanbaeva S.E., "Use of nonpositional notations in cryptographic protection" , *Izv. Nat Acad. of Sciences Resp. Kazakhstan, Ser. Phys.-Mat,* No 3 (2005): 84-89.

[20] Otchet o nauchno-issledovatel'skoy rabote «Razrabotka programmnykh i programmno-apparatnykh sredstv dlya kriptograficheskoy zashchity informatsii pri yeye peredache i sokhranenii v infokommunikatsionnykh sistemakh i po obshchim"[Research report "Development of software and firmware means for cryptographic protection of information during its transfer and storage in information and communications systems and general-purpose networks."], (2018), State reg. No. 0118RK01064.

[21] Kapalova N., Dyusenbayev D., "Security analysis of an encryption scheme based on nonpositional polynomial notations" , *Open Engineering,* No. 6, (2016): 250-258.

[22] Amerbayev V. M., Biyashev R. G., Nyssanbayeva S. E., "Primeneniye nepozitsionnykh sistem schisleniya pri kriptograficheskoy zashchite [Implementation of Non-positional Notations for Cryptographic Security]" , *News of the National Academy of Science of the Republic of Kazakhstan, Physical-mathematical series, Almaty: Gylym,* No. 3, (2005): 84-89.

[23] Biyashev R. G., Nyssanbayeva S. E., "Algoritm formirovaniya elektronnoy tsifrovoy podpisi s vozmozhnost'yu obnaruzheniya i ispravleniya oshibok [Algorithm for creating a digital signature with error detection and correction]" , *Cybernetics and Systems Analysis,* Vol. 48, No, 4, (2012): 14-23.

[24] Biyashev R., Nyssanbayeva S., Kapalova N., Khakimov R., "Modular models of the cryptographic protection of information" , *International Conference on Computer Networks and Information Security (CNIS2015), Changsha, China,* (2015): 393-398.

[25] Biyashev, R.G., Kalimoldayev M.N., Nyssanbayeva, S.E., Kapalova N.A., Dyusenbayev, D.S., Algazy K.T., "Development and analysis of the encryption algorithm in nonpositional polynomial notations" , *Eurasian Journal of Mathematical and Computer Applications,* No. 6(2)(2018): 19-33.

[26] Biyashev R.G., Nyssanbayeva S.E., Kapalova N.A., "Sekretnyye klyuchi dlya nepozitsionnykh kriptosistem. Razrabotka, issledovaniye i primeneniye [Private keys for non-positional cryptosystems. Development, research, and application]" , *LAP LAMBERT Academic Publishing,* (2014): 126.

[27] Kapalova N., Dyusenbayev D., "Security analysis of an encryption scheme based on nonpositional polynomial notations" , *Open Engineering,* No. 6, (2016): 250-258.