КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ имени АЛЬ-ФАРАБИ

ИНСТИТУТ ВЫЧИСЛИТЕЛЬНЫХ ТЕХНОЛОГИЙ
СИБИРСКОГО ОТДЕЛЕНИЯ РАН

ISSN 1560-7534
ISSN 1563-0285

СОВМЕСТНЫЙ ВЫПУСК

по материалам международной научной конференции
"Вычислительные и информационные технологии в науке, технике и образовании"
(CITech-2015)
(24-27 сентября 2015 года)

ВЫЧИСЛИТЕЛЬНЫЕ ТЕХНОЛОГИИ

Том 20

ВЕСТНИК КАЗНУ им. АЛЬ-ФАРАБИ

Серия математика, механика и информатика № 3 (86)

ЧАСТЬ I

АЛМАТЫ – НОВОСИБИРСК, 2015

Computational Technologies

2015

Vol 20

The BULLETIN of KAZNU 2015

Mathematics, Mechanics and Informatics Issue № 3 (86)

Modification of the Encryption Algorithm, Developed on The Basis of Nonpositional Polynomial Notations

Saule Nyssanbayeva and Miras Magzom

Institute of Information and Computational Technologies of MES RK,
125 Pushkin str., Almaty, 050010, Republic of Kazakhstan {snyssanbayeva,magzomxzn}@gmail.com
http://ipic.kz

Abstract. A model of the encryption algorithm, developed on the basis of nonpositional polynomial notation, is proposed. The possibility of modifying the model, using a Feistel network and encryption modes, is considered. The proposed model of the cryptographic algorithm will considerably improve statistical characteristics of resulting ciphertexts.

Keywords: cryptographic system, encryption algorithm, modular arithmetic, Feistel network, encryption mode.

1 Introduction

For symmetric block ciphers one of the criteria of cryptographic strength is the length of the secret key. In the encryption system under consideration as a criterion of cryptographic strength the cryptostrength of algorithm itself is used, which is characterized by a complete secret key. Its structure, apart from the standard secret key, also includes secret parameters of the cryptographic algorithm based on nonpositional polynomial notations (NPNs). Synonyms of NPNs - classical notations in residue number system (RNS), polynomial notations systems in RNS, modular arithmetic.

Classical modular arithmetic, or residue number system (RNS), is based on the Chinese remainder theorem, which states that any number can be represented by their remainders (residues) from its division by the base numbers systems, which are formed by pairwise coprime numbers [1,2]. In contrast to the classical RNS, proposed cryptographic procedures are considered in polynomial number system in residue classes, where bases are not prime numbers but are irreducible polynomials in [3,4]. Cryptographic algorithms and methods, based on NPNs are called nonconventional, modular or nonpositional. Nonconventional cryptographic methods and algorithms, developed on the basis of nonpositional polynomial notations (NPNs), allow increasing the reliability of the encryption algorithm and reduce the length of the key. Cryptostrength in this case is defined by full key, which depends not only on the length of a key sequence, but also on choice of a system of polynomial bases and the number of permutations of these bases in the system. If the length of the full encryption key in NPNs is larger, then there are more choices of systems of working bases. Therefore, the cryptostrength of the proposed encryption algorithm based on NPNs significantly increases with the length of the electronic message [3].

2 Nonconventional encryption algorithm

The encryption algorithm based on NPNs includes the following steps. For an electronic message of the length N bits from the set of all irreducible polynomials of degree not exceeding N a system of working base numbers is selected

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

According to the Chinese remainder theorem, all the base numbers must be different even if their degrees are equal. The main working range in this system is defined by the polynomial $P(x) = p_1(x), p_2(x), ..., p_S(x)$ of the degree m:

$$m = \sum_{i=1}^{S} m_i, \tag{2}$$

where $S-$ is a number of selected working base numbers. In this system any polynomial, which degree is less than m, has a unique representation in the form of sequence of residues of its division by the working base numbers (1). Therefore, the message of the length N bits could be represented in the form of sequence of residues $\alpha_1(x), \alpha_2(x), ..., \alpha_S(x)$ from division of some polynomial *F(x)* by the working base numbers $p_1(x), p_2(x), ..., p_S(x)$:

$$F(x) = (\alpha_1(x), \alpha_2(x), ..., \alpha_S(x)), \tag{3}$$

where $F(x) \equiv \alpha_i(x)(mod\ p_i(x)), i = \overline{1, \mathrm{S}}$.

In the same way the key of the length N bit is also interpreted as a system of residues $\beta_1(x), \beta_2(x), ..., \beta_S(x)$ from the division of another polynomial *G(x)* by the same working base numbers:

$$G(x) = (\beta_1(x), \beta_2(x), ..., \beta_S(x)), \tag{4}$$

where $G(x) \equiv \beta_i(x)(mod\ p_i(x)), i = \overline{1, \mathrm{S}}$.

Then the cryptogram $\omega_1(x), \omega_2(x), ..., \omega_S(x)$ is considered as some function *H(F(x),G(x))*:

$$H(x) = (\omega_1(x), \omega_2(x), ..., \omega_S(x)), \tag{5}$$

where $H(x) \equiv \omega_i(x)(mod\ p_i(x)), i = \overline{1, \mathrm{S}}$.

According to operations of nonpositional notation system, operations in functions *F(x)*, *G(x)*, *H(x)* are executed in parallel on the modules of polynomials $p_1(x), p_2(x), ..., p_S(x)$, which are selected as the base numbers of NPNs.

In software implementation of this nonconventional algorithm the encryption method [4] is used. The ciphertext is obtained from multiplication of the polynomials (3) and (4) in accordance with the properties of comparison to the double modulus:

$$F(x)G(x) \equiv H(x)(mod\ P(x)), \tag{6}$$

i.e. represented as remainders of division of products $\alpha_i(x)\beta_i(x)$ to the respective base numbers $p_i(x)$.

In the decryption process of the cryptogram *H(x)* with known key *G(x)* for each $\beta_i(x)$ an inverse polynomial $\beta_i^{-1}(x)$ is calculated, completing the following comparisons

$$\beta_i(x)\beta_i^{-1}(x) \equiv 1(mod\ p_i(x)), i = \overline{1, \mathrm{S}}. \tag{7}$$

The result is a polynomial which inverse to a polynomial *G(x)*. Then, the original message is restored over:

$$F(x) \equiv G^{-1}(x)H(x)(mod\ P(x)). \tag{8}$$

3 Application of the modified Feistel network

In the development of symmetric block cipher the cryptosystem called Feistel scheme has gained wide popularity. It was first used by Horst Feistel in 1973 in the development of the cipher Lucifer[5], and then used in many developments of block ciphers, including standards DES and AES [6].

Feistel scheme is a method of blending the sub-blocks of the input text in the cipher through the repeated use of the key-dependent non-linear functions, called F-functions and performance of permutations of the sub-blocks. Round of a block cipher is a transformation that connects the sub-blocks of the input block by the F-function and permutations of sub-blocks. In the standard Feistel network, the plaintext is divided into two sub-blocks of the same length.

In general case, the Feistel network can split an input block into $n \geq 2$ sub-blocks. Further assumed that all sub-blocks are of the same length, so that each sub-block may be involved in the transposition with any other sub-block. A generalized exchange scheme is a permutation of $n \geq 2$ sub-blocks in the round.

The developed encryption algorithm based on NPNs is the basis for solving the problems of its practical use. In development of the model of unconventional encryption algorithm, it is planned to use the modified Feistel network to develop its application mode. The aim of this works is to improve the statistical characteristics of nonpositional cryptograms. In this regard, it is planned to consider several models of the Feistel scheme.

Unlike traditional Feistel network where the input data is a plain text message, in the developed model the input is a bit sequence of the ciphertexts obtained in (5).

A necessary condition for the strength of the cipher is achievement of complete diffusion. The diffusion process of the cipher is characterized by the distribution of influence of the one of the input bit on many output bits. Cipher is called complete if every output bit depends on all input bits [7]. In the considered model, all F-functions are implied to be complete.

Most ciphers with Feistel network architecture use function F that each round only depends on one of subkeys generated from the main encryption key. A network with such dependence of the function is called heterogeneous and homogeneous otherwise. The use of heterogeneous networks can significantly improve the properties of the cipher, as uneven changes of the internal properties of the network within the permissible limits make study of the characteristics of the cipher rather difficult task.

For example, consider a model in which the input block of 128 bits is divided into two sub-blocks of equal length R and L.

When using a homogeneous network, at each round of encryption a separate key sequence K_i is used:

$$L_i = R_{i-1} \tag{9}$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i) \tag{10}$$

When using a heterogeneous network at each round the encryption function F depends not only on the round key K_i, but also on the chosen system of base numbers (1):

$$L_i = R_{i-1} \tag{11}$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i, P(x)) \tag{12}$$

During computer modeling of developed modified algorithms, the statistical characteristics of the resulting ciphertexts will be analyzed. Verification of the model for satisfying the strict avalanche criterion will be conducted by examining the received bit sequence through statistical tests of uniformity (frequencies) - Frequency (Monobit) Test for cryptographic functions from National Institute of Standards and Technology [8]. "NIST Statistical Test Suite statistical package consisting of 16 tests designed to check the randomness of binary sequences produced both by technical means and by software.

4 Conclusion

The proposed modification of the nonpositional cryptographic algorithm is the basis for its software implementation. On implemented model, the statistical characteristics of obtained ciphertexts will be investigated. The results of computer modeling will allow making recommendations on the use of the described encryption model.

References

1. Akushskii, I.Ya., Juditskii, D.I., *Machine Arithmetic in Residue Classes [in Russian]*, Sov. Radio, Moscow (1968).
2. Bijashev, R.G., *Development and investigation of methods of the overall increase in reliability in data exchange systems of distributed ACSs*, Doctoral Dissertation in Technical Sciences, Moscow (1985).
3. Bijashev, R.G., Nyssanbayeva S.E., *Algorithm for Creation a Digital Signature with Error Detection and Correction*, Cybernetics and Systems Analysis, 4, 489-497 (2012).
4. Nyssanbayev, R.K., *Cryptographical method on the basis of polynomial bases*, Herald of the Ministry of Science and Higher Education and National Academy of Science of the Republic of Kazakhstan, 5, 63-65 (1999).
5. Feistel H., *Cryptography and Computer Privacy*, Feistel H., Scientific American, V. 228, N.5, 15-23(1973).
6. Bassham L., Burr W., Dworkin M., Foti J., Roback E., *Report on the Development of the Advanced Encryption Standard (AES)* , Computer Security Division, Information Technology Laboratory; NIST: Technology Administration; U.S. Department of Commerce, 116 p. (2000).
7. Schneier B., Kelsey J., *Unbalanced Feistel Networks and Block-Cipher Design*, Fast Software Encryption, Third International Workshop Proceedings (February 1996), Springer-Verlag, 121-144 (1996).
8. Rukhin A., Soto J., *[8] A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* , NIST Special Publication 800.-22, 154 p. (2001).