Development of an Encryption Algorithm Based on Nonpositional Polynomial Notations

Rustem Biyashev, Saule Nyssanbayeva, Maksat Kalimoldayev and Miras Magzom*
Information Security laboratory, Institute of information and computational technologies CS MES RK, Almaty, Kazakhstan
*Corresponding author

***Abstract*—Cryptographic systems, developed on the basis of nonpositional polynomial notations, are called nonconventional or modular. In this paper modelling of the encryption algorithm based on nonpositional polynomial notations is described. The development of the model of block cipher system comprises the construction of the modified nonpositional block cipher algorithm, using an analog of the Feistel scheme and a mode of application for this modified algorithm.**

Keywords-cryptosystems; encryption; block cipher; nonpositional polynomial notation; cryptostrength; cipher mode

I. INTRODUCTION

The model of the encryption algorithm described in this paper applies nonconventional algebraic method. This method is based on the theory of nonpositional polynomial notation systems (NPNs) in residue classes, which is also called polynomial notations in residue numeral system (polynomial RNS).

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. In contrast, in polynomial RNS moduli are represented by irreducible polynomials with coefficients over $GF(2)$ [1,2]. The application of NPNs allows improving durability and efficiency of nonpositional cryptographic algorithms without increasing the length of secret key [3].

Improved efficiency is provided by the rules of NPNs in which all arithmetic operations can be performed in parallel to the base module NPNs. In nonpositional cryptosystems the cryptostrength is characterized by a complete secret key. Cryptostrength in this case depends not only on the length of a key sequence, but also on choice of a system of polynomial bases. With the growth of the order of irreducible polynomials with binary coefficients, their number also grows rapidly. The greater the length of the input block, the more choices of working systems bases are possible. Therefore, the cryptostrength of the proposed encryption algorithm against bruteforce attack significantly increases with the length of the electronic message.

In [3] the arithmetic of nonpositional number systems with polynomial bases and its application to problems of improving reliability are developed. As it is shown, the algebra of polynomials over a field in modulus of the irreducible polynomial over this field is a field and the representation of the polynomial in the nonpositional form is the only (analogous to the Chinese remainder theorem for polynomials). According to the Chinese remainder theorem, all working base numbers should be different.

II. DESIGN OF THE NONPOSITIONAL ENCRYPTION ALGORITHM

A. Nonpositional Polynomial System

Encryption of the data block of the given length N is done in the following way. From the set of all irreducible polynomials of degree not exceeding N form a system of working bases:

$$p_1(x),p_2(x),...,p_S(x). \quad (1)$$

A data block of length of N bits is represented as a sequence of remainders of division of some polynomial (let us denote it as $F(x)$) by working base (Eq. 1)

$$F(x) = (\alpha_1(x), \alpha_2(x),...,\alpha_S(x)), \quad (2)$$

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

Remainders $\alpha_1(x)$, $\alpha_2(x),...,\alpha_S(x)$ are selected in the way where binary coefficients of reminder $\alpha_1(x)$ correspond to the first l_1 bits of the message, the next binary coefficients of reminder $\alpha_2(x)$ correspond to the next l_2 bits, etc., and binary coefficients of reminder $\alpha_S(x)$ correspond to the last l_S bits.

Then the secret key of length of N bits is also interpreted as a system of residues $\beta_1(x),\beta_2(x),\ldots,\beta_S(x)$, but from division of other polynomial $G(x)$ by the same moduli system:

$$G(x) = (\beta_1(x), \beta_2(x),...,\beta_S(x)), \quad (3)$$

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

After encrypting the message $F(x)$ using the key $G(x)$ a ciphertext is obtained. This ciphertext is considered as a function $H(x)$:

$$H(x) = (\omega_1(x), \omega_2(x),...,\omega_S(x)). \quad (4)$$

Encrypted text (Eq. 4) for a message of the length N bit is obtained by multiplying polynomials (Eq. 2) and (Eq. 3):

$$F(x)G(x) = H(x)(\text{mod } P(x)). \quad (5)$$

For deciphering $H(x)$ by the known key $G(x)$ for each value $\beta_i(x)$ an inverse polynomial $\beta_i^{-1}(x)$ is calculated:

$$\beta_i(x)\beta_i^{-1}(x) \equiv 1(\text{mod } p_i(x)),\ i = 1...S. \quad (6)$$

The result is the polynomial

$$G^{-1}(x) = (\beta_1^{-1}(x),\beta_2^{-1}(x),...,\beta_S^{-1}(x)), \quad (7)$$

which is inverse to the polynomial $G(x)$. Then the plain message is restored in accordance with (Eq. 5) and (Eq. 6):

$$F(x) = G^{-1}(x)\ H(x)(\text{mod } P(x)). \quad (8)$$

Thus, the complete key consists of the chosen system of polynomial working bases $P(x)$ and the secret key $G(x)$.

B. Nonconventional Encryption Algorithm

In proposed model of the nonconventional encryption algorithm the Feistel scheme (network), which has gained wide popularity in the development of symmetric block ciphers, is used. This scheme was first used by Horst Feistel in 1973 in the development of the cipher Lucifer[4], and then used in many developments of block ciphers, including standards DES and AES [5]. 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 round 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 round 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 common exchange scheme is a permutation of $n \geq 2$ sub-blocks in the round.

During the development of the nonpositional encryption algorithm different designs of the Feistel scheme are investigated. In [6] the modification of the unconventional encryption algorithm was described, considering the usage of Feistel scheme as a pre- and postprocessing of data block.

Unlike traditional Feistel network where the input data is a plain text message, the input of the modified postprocessing Feistel scheme is supplied by the bit sequence of ciphertext, obtained from the unconventional encryption algorithm (Eq. 4)

In the model with preprocessing, the input block of plain data first is encrypted by classical Feistel scheme, then is transformed by the unconventional encryption algorithm.

Additionally, the model was developed, which repeats the structure of classical Feistel scheme, but the round function of which encrypts the subblock of data by the unconventional encryption algorithm. The round function might depend not only on round key, but also on selected system of bases. In this case the round function is called heterogeneous. The use of heterogeneous networks can significantly improve the characteristics of the cipher as uneven changes in internal properties of the network makes the study of statistical characteristics of encrypted data rather difficult task.

Currently the possibilities of practical application of the encryption algorithm based on nonpositional polynomial notations using nested Feistel network are being studied. The use of nested, or recursive, Feistel network scheme can significantly complicate a cryptanalysis of the cipher [7].

There is a potential possibility of information leaks about recurring parts of data which encrypted on the one and the same key, in view of the fact that the block ciphers encrypt data by fixed-size blocks [8]. Therefore, for using block cipher algorithms various modes are developed [9]. Encryption modes in the process of cryptographic transformations are used to provide the required conditions for encrypted messages. The main condition is that the encryption result of each block must be unique regardless of the encrypted data.

III. SUMMARY

The research of the possibility of implementing Feistel scheme and encryption modes helps to investigate the practical usability of the developed models. Computer modelling of the nonpositional encryption algorithm allows to develop recommendations for its application.

Proposed models of the unconventional encryption algorithm are the basis for its future application in nonpositional cryptosystems. These models will also be studied further in the future.

ACKNOWLEDGEMENT

Authors express their deep appreciation to the Committee of Science, Ministry of Education and Science of the Republic of Kazakhstan, for the funding of the research. The results of the development of nonpositional cryptographic systems are obtained during these studies.

REFERENCES

[1] M. Pohst and H. Zassenhaus, Eds., Algorithmic algebraic number theory. New York, NY, USA: Cambridge University Press, 1989

[2] Cormen, Thomas H.; Leiserson, Charles E.; Rivest, Ronald L.; Stein, Clifford (2001), Introduction to Algorithms (Second ed.), MIT Press and McGraw-Hill.

[3] R. G. Biyashev, S. E. Nyssanbayeva, "Algorithm for Creation a Digital Signature with Error Detection and Correction," Cybernetics and Systems Analysis, 4, 489-497, 2012.

[4] H. Feistel. Cryptography and Computer Privacy, H. Feistel // Scientific American. – 1973. V. 228, N. 5.P. 15-23.

[5] 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).

[6] R. G. Biyashev, S. E. Nyssanbayeva, Ye. Ye. Begimbayeva, M. M. Magzom, Building modified modular cryptographic systems, International Journal of Applied Mathematics and Informatics, Volume 9 2015, P103-109.

[7] Mitsuru Matsui and Toshio Tokita. MISTY, KASUMI and Camellia Cipher Algorithm Development. Mitsubishi Electric Advance. Vol. 100/December 2002 Mitsubishi Electric.

[8] N. Ferguson, B. Schneier, T. Kohno, "Cryptography Engineering: Design Principles and Practical Applications," Wiley Publishing Inc, 2010.

[9] Recommendation for Block Cipher Modes of Operation. NIST Special Publication 800-38A. Technology Administration U.S. Department of Commerce. 2001 Edition.