

Research Article

Open Access

Saule Nyssanbayeva, Maksat Kalimoldayev, and Miras Magzom*

Model of nonconventional encryption algorithm based on nested Feistel network

DOI 10.1515/eng-2016-0030

Received May 04, 2016; accepted Jun 24, 2016

Abstract: The purpose of research - studying the possibilities of practical application of the encryption algorithm based on nonpositional polynomial notations using nested Feistel network. In this paper, a mathematical model of non-conventional encryption algorithm with recursive Feistel network and the encryption mode is described.

Keywords: encryption algorithm; residue arithmetic; nonpositional polynomial notation; Feistel network; cipher mode

1 Introduction

The increase of the scale of modern information systems increases the need for persistent and effective means of ensuring information security during storage and transmission of data. Today such areas of theoretical and applied research, as creation and analysis of reliability of cryptographic algorithms and protocols, arouse great interest. The encryption system described in this paper applies nonconventional algebraic method, which is based on the theory of nonpositional polynomial notation systems (NPNs) in residue classes. Synonyms of NPNs are polynomial residue number system (RNS), modular arithmetic. Classical modular arithmetic 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]. The difference of the pro-

posed method from classical residue notation systems is that in polynomial number system in residue classes bases are not prime numbers but are irreducible polynomials in $GF(2)$. Nonconventional approach, based on the application of nonpositional polynomial notations, allows to increase reliability and speed of the encryption algorithm as in NPNs all arithmetic operations can be performed in parallel on the base moduli of NPNs.

2 Nonconventional encryption algorithm based on NPNs

For an electronic message of the length N bits NPNs are formed: bits from the set of all irreducible polynomials of degree not exceeding N working base numbers (moduli) are selected

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

Selected polynomials (1) forms a bases (moduli) system, in which their order is also important. The working range of the system is defined by the polynomial $P(x) = p_1(x)p_2(x) \cdots p_S(x)$ of a degree m :

$$m = \sum_{i=1}^S m_i \quad (2)$$

where S is a number of selected working base numbers, and m_i is a degree of the corresponding $p_i(x)$.

All selected base numbers (1) must differ from each other, i.e. must be unique for this system. Then, according to the terms of the Chinese remainder theorem, in this system, any polynomial of degree less than m has a unique representation as a sequence of remainders (residues) of dividing it by the bases (1).

After forming bases system, a plaintext block of length N bits can be represented as a sequence of residues $\alpha_1(x), \alpha_2(x), \dots, \alpha_S(x)$ from the division of a polynomial $F(x)$ by the working bases $p_1(x), p_2(x), \dots, p_S(x)$:


$$F(x) = (\alpha_1(x), \alpha_2(x), \dots, \alpha_S(x)), \quad (3)$$

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

Saule Nyssanbayeva: Institute of Informational and Computational Technologies of MES RK, Almaty, Kazakhstan, E-mail: snyssanbayeva@gmail.com

Maksat Kalimoldayev: Institute of Informational and Computational Technologies of MES RK, Almaty, Kazakhstan, E-mail: mnk@ipic.kz

***Corresponding Author: Miras Magzom:** Institute of Informational and Computational Technologies of MES RK, Almaty, Kazakhstan, E-mail: magzomxzn@gmail.com

 © 2016 S.E. Nyssanbayeva et al., published by De Gruyter Open. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 License.

In the same way a secret key of the length N is interpreted in the formed NPNs. It is defined as a residue system $\beta_1(x), \beta_2(x), \dots, \beta_S(x)$, but from the division of the other polynomial $G(x)$ by the same base numbers of the system:

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

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

Nonconventional encryption procedure is considered as a function $H(F(x), G(x))$ of the representation (3) of the plaintext and (4) of the secret key. Obtained ciphertext is also recorded in nonpositional representation as a sequence of residues $\omega_1(x), \omega_2(x), \dots, \omega_S(x)$:

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

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

The cryptostrength of the encryption algorithm is defined by a full key, which consists of the base numbers system (3) and the secret key (4).

3 Modelling of the nonconventional encryption algorithm

To build a model of the nonconventional block cipher the Feistel scheme is used. This scheme has gained wide popularity in the development of symmetric block ciphers. Feistel scheme is a method of mixing the sub-blocks of the input text in the cipher through repetitive application of round-key-dependent nonlinear functions and performing permutation of subblocks [3, 4]. 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. Feistel networks have been extensively studied because of their widespread use in the development of encryption algorithms.

Encryption is performed in the developed model in the following way, as shown in Figure 1.

The input block is divided into two halves L_0 and R_0 . The right side R_0 passes through the conversion function G , which is a nested Feistel network. The resulting transformed sub-block R_0 is XORed with the left sub-block L_0 and becomes the right part R_1 of the input block for the next round, while unmodified sub-block R_0 rearranged to the left L_1 sub-block in the next iteration.

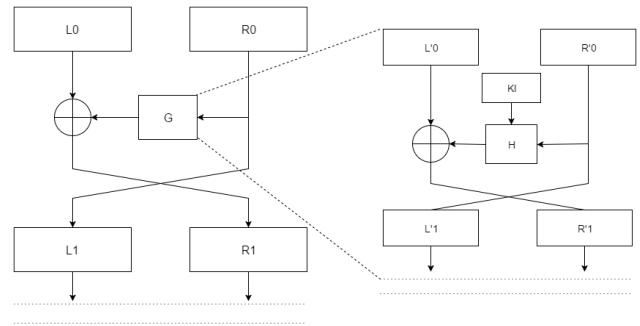


Figure 1: The scheme of the application of the nested Feistel network

The conversion function G is also a Feistel network. The input data block, received from the upper layer network node, is divided into two equal parts L'_0 and R'_0 .

The sub-block R'_0 is encrypted by the nonconventional encryption procedure (5) with the use of a round key K_i . According to (3), the right sub-block R'_0 is interpreted as a sequence of residues $\alpha_1(x), \alpha_2(x), \dots, \alpha_S(x)$, while the round key K_i , according to (4), is represented as a system of remainders $\beta_1(x), \beta_2(x), \dots, \beta_S(x)$. Then, the encrypted sub-block is obtained in the form of operation

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

i.e. represented as remainders of division of products $\alpha_i(x)\beta_i(x)$ to the respective base numbers $p_i(x)$, $i = \overline{1, S}$. The binary sequence of the obtained ciphertext of R'_0 is XORed with the binary sequence of the left sub-block L'_0 and becomes the right side R'_1 . The original sub-block R'_0 becomes the left side L'_1 of the input block for the next round of a nested Feistel network.

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

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

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

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

The use of nested, or recursive, Feistel network scheme can significantly complicate a cryptanalysis of the cipher [5].

During the modelling of the encryption algorithm the number of round keys on each of the levels and methods of their generation may be different. Therefore, it is possible to build different models of the proposed encryption system with application of nonconventional cipher and nested Feistel networks.

In the developed model the nested network includes sixteen rounds, and the top-level Feistel network consists of four rounds. In the proposed algorithm, sixteen round keys are obtained by shifting the bit sequence of the secret key K on a variable number of bits, which is determined by the degree of the i -th polynomial in the bases system. There also may be used other secret parameters that are defined in the full key. The encryption algorithm based on the NPNs the full secret key depends not only on the length of a key sequence, but also on the chosen system of polynomial bases, as well as on the order of the bases in the system. The use of these properties of the algorithm in the generation of round keys leads to uneven changes in the internal properties of the network, which complicates the analysis of the properties of the cipher.

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 based on NPNs significantly increases with the length of the electronic message.

This model uses the input block length of 512 bits. In this case, the length of the block of nested Feistel network, for which NPNs is formed, equals 128 bits. This gives a large choice of irreducible polynomials for the construction of the system of working bases [6, 7].

In this model, to improve the statistical properties of the produced cryptograms an encryption mode is used. Encryption modes are used to modify the encryption process so that the result of the encryption of each block is unique, regardless of the encrypted data and does not allow to draw any conclusions about their structure. This is due primarily to the fact that block ciphers encrypt data blocks of fixed size, therefore there is a potential possibility of information leaks about recurring parts of data which are encrypted by the same key.

In the developed model a Cipher Block Chaining (CBC) mode is applied [7]. The transform is performed in the following way: each block of the plaintext is XORed with the previous block of cryptogram. Thus, results of the encryption of previous blocks affect the encryption of next blocks.

In the beginning of the encryption initialization vector (IV) is used in order to provide that encryption result of any input message is unique. In this regard, the IV has to be a random number. It is not necessary to keep IV in secret; it is possible to pass it along with the message.

To verify the effectiveness and reliability of the proposed model of the nonconventional encryption an algorithm of its computer implementation is developed. Testing of the algorithm is carried out by encryption and decryption of files of various formats. The usage of similar file formats allows to evaluate the effectiveness of the en-

ryption algorithm during processing data with explicit repeating structure. Analysis of the statistical characteristics of the resulting ciphertext is conducted through the use of a set of statistical tests [8].

4 Conclusion

Modelling of the encryption algorithm based on NPNs with the use of recursive Feistel scheme is carried out. This approach allows to hide the structural features of the source text block that during additional use of encryption mode greatly improves the statistical characteristics of all ciphertexts.

Ongoing research is focused on the development of recommendations on the practical application of nonconventional encryption algorithm. The results of this study will be used in work on the construction and investigation of the other models of nonconventional encryption algorithm.

References

- [1] Pohst M., Zassenhaus H., *Algorithmic algebraic number theory*, Cambridge University Press, New York, 1989
- [2] Biyashev R., Nyssanbayeva S., *Algorithm for creation a digital signature with error detection and correction*, *Cybern. Syst. Anal.*, 2012, 4, 489–497
- [3] Feistel H., *Cryptography and Computer Privacy*, *Sci. Am.*, 1973, 228, 5, 15–23
- [4] Bassham L., Burr W., Dworkin M., Foti J., Roback E., *Report on the development of the Advanced Encryption Standard (AES)*, NIST, U.S. Department of Commerce, 2000
- [5] Matsui M., Tokita T., MISTY, KASUMI and Camellia cipher algorithm development. *Mitsubishi Electr. Ad.*, 2002, 100, 1–8
- [6] Kapalova N., Nyssanbayeva S., Khakimov R., *Irreducible polynomials over the field $GF(2^n)$* , *Proceedings of "KAKHAK" scientific-technical society (Almaty, Kazakhstan)*, 2013, 1, 17–28
- [7] Biyashev R., Nyssanbayeva S., Begimbayeva Ye., Magzom M., *Building modified modular cryptographic systems*, *Int. J. AP-MAIN*, 2015, 9, 103–109
- [8] Dworkin M., *Recommendation for block cipher modes of operation: methods and techniques*, *NIST Spec. Publ.*, 2001, 800–38A
- [9] Rukhin A., Soto J., Nechvatal J., Smid M., Barker E., Leigh S., et al., *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, *NIST Spec. Publ.*, 2001, 800–22
- [10] Schneier B., Kelsey J., *Unbalanced Feistel networks and block cipher design*, *Proceedings of the Third International Workshop on Fast Software Encryption (21-23 February 1996, Cambridge, UK)*, Springer-Verlag, 1996, 121–144