Research Article

Open Access

N.Kapalova* and A. Haumen

The model of encryption algorithm based on non-positional polynomial notations and constructed on an SP-network

<https://doi.org/10.1515/eng-2018-0013>

Received June 30, 2017; accepted January 3, 2018

Abstract: This paper addresses to structures and properties of the cryptographic information protection algorithm model based on NPNs and constructed on an SP-network. The main task of the research is to increase the cryptostrength of the algorithm. In the paper, the transformation resulting in the improvement of the cryptographic strength of the algorithm is described in detail. The proposed model is based on an SP-network. The reasons for using the SP-network in this model are the conversion properties used in these networks. In the encryption process, transformations based on S-boxes and P-boxes are used. It is known that these transformations can withstand cryptanalysis. In addition, in the proposed model, transformations that satisfy the requirements of the "avalanche effect" are used. As a result of this work, a computer program that implements an encryption algorithm model based on the SP-network has been developed.

Keywords: cryptography, encryption algorithms, SP-network, non-positional polynomial notations, avalanche effect.

1 Introduction

In the Institute of the Information and Computational Technologies, under the authority of R.G. Biyashev there were developed nonconventional algorithms for encryption (including a symmetric block data encryption algorithm), digital signature, and cryptographic key exchange on the basis of non-positional polynomial notations (NPNs) with the benefit of properties of algebraic methods [1–4]. Besides, the developed methods are exam-

ined with respect to their reliability or rather their strength against cryptanalysis.

This paper presents the results of work on modification of the encryption algorithm aimed at improving the cryptostrength of the algorithm. The properties of a model developed on an SP-network basis are studied.

An SP-network (Substitution-Permutation network) is a block cipher variation put forward by Horst Feistel in 1971 [5]. A cipher developed on an SP-network consists of an S-box and a P-box.

An S-box (substitution box) substitutes a block of input bits with another block of output bits. This substitution should be one-to-one to ensure its invertibility. Since an S-box implements a nonlinear conversion, this enables the cipher to withstand the linear cryptanalysis.

A P-box (permutation box) is a permutation of all the bits of a block.

2 Encryption algorithm based on non-positional polynomial notations and constructed on an SP-network

While developing the encryption algorithm, we used an encryption method based on NPNs, transformations of substitution (S), permutation (P), and so-termed LT-conversion. All the four transformations are described below. A software implementation model of the algorithm was developed. A flow diagram of the model is shown in Figure 1.

Before encryption, any input data are split into 16-byte or 128-bit blocks. The last block is completed up to the length of 16 bytes, when required, according to a rule specified in advance (e.g. with zeroes). The encryption begins with the addition of the first block of plaintext bits to the respective key bits. Further transformations are as follows.

*Corresponding Author: N.Kapalova: Institute Information and Computational Technologies Almaty, Kazakhstan,
E-mail: Kapalova@ipic.kz
A. Haumen: E-mail: haumen.armanbek@gmail.com

Figure 1: The scheme of the algorithm based on SP-network

2.1 Conversion S

An S-box is used as a nonlinear bijective conversion (substitution table). The S-box is a one-dimensional array consisting of 256 elements. As a rule, S-boxes are included in the transformation function, and they are essential for the encryption algorithm strength. It is important that any changes in the input data of an S-box would change the output data in a random-looking way. The relationship between an input and the respective output should not be linear or easily approximated by linear functions (this very property is used in the linear cryptanalysis) [6, 7].

Transformation S substitutes each input byte by another byte through the S-box (Figure 2).

From the scheme of conversion S it is easily seen that encrypting two identical 16-byte blocks of a plaintext results in two identical blocks of ciphertext. This is a weakness that can be used by a cryptanalyst. In order to eliminate the weakness, an LT-conversion was developed.

2.2 Conversion LT

Developing an encryption algorithm, presumes that the algorithm must be analyzed with regard to its strength against various types of cryptographic attacks. Among the most common standard methods now in use are attacks on

the basis of linear and differential analyses [6]. Essentially, the latter traces the differences between output bits (in the ciphertext) as a function of differences between input bits (in the plaintext) at different rounds of the base transformation. The precondition to ensure that an encryption algorithm is strong against the differential analysis is the "avalanche effect" in the base transformation.

The LT-conversion serves to comply with the requirement of avalanche effect.

The avalanche effect is an important cryptographic property for encryption, where a small change in the input plaintext bits or the key results in a drastic change in the output ciphertext bits. In other words, all output bits depend on each input bit. It is known that such encryption algorithms as AES, RC4, Kuznyechik and others use transformations that meet the requirements of "avalanche effect" to increase their cryptostrength [8–11].

Before conversion LT, the bytes of a block are placed in a 4x4 two-dimensional array, as is shown in Figure 3.

At the first step, the bytes of the first row in the array are added to each other modulo 256. The new byte obtained in such a way is stored in the place of the leftmost byte, while the rest bytes are rotated right shift of one position.

$$L(c_{ij}) = \sum_{i=0}^3 a_{ij} \bmod 256, j = \overline{0, 3}. \quad (1)$$

Figure 2: The scheme of conversion S

Conversion LT

a_0	a_1	a_2	a_3
a_4	a_5	a_6	a_7
a_8	a_9	a_{10}	a_{11}
a_{12}	a_{13}	a_{14}	a_{15}

Figure 3: The location of the bytes in LT conversions

The procedure is performed four times for the row. As a result, we will get four new bytes in the first row. We then repeat the operation for each row in the array.

At the next step, the operation above is implemented for the columns of the array. The obtained new bytes are placed here from up to down. After the LT-conversion, the bytes in the array will receive new values.

2.3 Conversion P

For this transformation, the bytes in a block are considered as bits, which are permuted with a specially designed P-box (a permutation table).

As a result of the bit permutation, the bytes receive new values. After the conversion, the obtained bit sequences are sent to the encryption module. The module encrypts the block of bytes on the basis of NPNs.

Examples that meet the requirements of the avalanche effect are shown below.

2.4 Description of a nonpositional encryption scheme

As distinct from a classical residue number system, irreducible polynomials over $GF(2)$ serve as bases in an NPN.

First of all, an NPN is formed for an N -bit block of electronic message [12, 13]. For this purpose, we choose its working bases, i.e. irreducible polynomials

$$p_1(x), p_2(x), \dots, p_S(x) \quad (2)$$

over $GF(2)$ of degrees $m_1, m_2, \dots, m_S$ respectively [2]. Polynomials (1) subject to their arrangement constitute a certain base system. All bases (1) are to be different includ-

Figure 4: The scheme of conversion LT

Figure 5: The scheme of conversion P

Table 1: Examples of the avalanche effect

Conversion	aaaaaaaaaaaaaa	aaaaaaaaaaaaaab
LT	d1 25 4f e4 25 09 7b b4 4f 7b 91 9c e4 b4 9c 10	e1 2d 53 e8 2d 0d 7d b6 53 7d 92 9d e8 b6 9d 11
S+LT	8b d6 db 3c 55 af a7 ef 2b c8 9a 4c 32 57 dd a8	6b 46 93 f4 c5 67 83 cb e3 a4 88 3a ea 33 cb 96
S+P+LT	c6 b0 14 2b 22 65 9c 66 b2 8e 48 81 40 f8 d3 e9	9a 20 cc 87 8c 9d f8 14 4e de 70 95 0e e0 07 83

ing the case when they have the same degree. The working range of the NPN is specified by polynomial (modulus)

$$P(x) = p_1(x) \cdot p_2(x) \cdot \dots \cdot p_S(x)$$

of degree $m = \sum_{i=1}^S m_i$. Therefore, a message of N -bit length could be interpreted as a sequence of remainders $\alpha_1(x), \alpha_2(x), \dots, \alpha_S(x)$ of dividing a polynomial $F(x)$ by working bases $p_1(x) \cdot p_2(x) \cdot \dots \cdot p_S(x)$:

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

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

In expression (2) remainders $\alpha_1(x), \alpha_2(x), \dots, \alpha_S(x)$ are chosen so that the first l_1 bits of a message associate to binary coefficients of remainder $\alpha_1(x)$, the next l_2 bits associate to binary coefficients of remainder $\alpha_2(x)$, etc., and the last l_S bits associate to binary coefficients of $\alpha_S(x)$.

To encrypt a message, it is used a secret key of N bits, which is also interpreted as a sequence of remainders resulting from dividing some other polynomial $G(x)$ by the same working bases of the system:

$$G(x) = (\beta_1(x), \beta_2(x), \dots, \beta_S(x)), \quad (4)$$

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

Hence, some function $H(F(x), G(x))$ is considered as a cryptogram:

$$H(x) = (\omega_1(x), \omega_2(x), \dots, \omega_S(x)), \quad (5)$$

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

In NPNs, a cryptogram is the result of multiplying polynomial $F(x)$ by $G(x)$. The members of residue sequence $\omega_1(x), \omega_2(x), \dots, \omega_S(x)$ are the least remainders on dividing products $\alpha_i(x)\beta_i(x)$ by respective bases $p_i(x)$:

$$\alpha_i(x) \cdot \beta_i(x) \equiv \omega_i(x)(\text{mod } p_i(x)), \quad i = \overline{1, S}. \quad (6)$$

The binary form of cryptogram $H(x)$ is as follows. The binary coefficients of residue $\omega_1(x)$ associate to first consecutive l_1 bits of $H(x)$. The binary coefficients of residue $\omega_2(x)$ associate to further consecutive l_2 bits of $H(x)$, etc. The binary coefficients of the last residue $\omega_S(x)$ associate the last consecutive l_S binary bits of the cryptogram.

When decrypting cryptogram $H(x)$ with a known key $G(x)$, for each $\beta_i(x)$ it is calculated, as follows from (5), a reciprocal (inverse) polynomial $\beta_i^{-1}(x)$ under the following condition:

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

The result is polynomial

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

inverse to polynomial $G(x)$. The original message then could be calculated according to (5) and (6) through remainders of the following congruence:

$$\alpha_i(x) \equiv \beta_i^{-1}(x)\omega_i(x)(\text{mod } p_i(x)), \quad i = \overline{1, S}. \quad (8)$$

3 The encryption algorithm analysis

Computer-based experiments to test statistical properties of the algorithm ciphertext have been conducted. The developed software package implementing a quality assessment system based on graphical and assessment tests was used to test the output ciphertexts. The results of the statistical analysis of the ciphertexts are detailed in [14].

The results for each test are represented in the form of histogram per key and per the number of files under study are shown in Figure 6.

To evaluate if the developed algorithm is secure, mathematical models of cryptanalysis involving algebraic, linear and differential methods have been designed.

The cryptanalysis is as follows. A system of nonlinear equations is obtained from a function transforming plaintext into ciphertext with a key. Next, a possibility of transition of the nonlinear system to a linear one is considered. The cryptanalysis of the algorithm under investigation was conducted for the cases with known: 1) ciphertext; 2) plaintext and the related ciphertext; 3) plaintext file format; and 4) ASCII-encoded plaintext [5, 6]. When performing the cryptanalysis, it is believed that an encryption scheme has been known in advance. The cryptanalyst needs to derive:

- Plaintext and a key from a ciphertext;
- Secret key from a plaintext-ciphertext pair.

To conduct algebraic and linear analyses of a nonpositional encryption algorithm, a set of equations is built subject to regularities of ring multiplication.

The results of the linear and differential analyses were compared against each other with respect to uniformity. Table 2 shows the results for the linear and differential cryptanalyses of S-boxes for certain known and developed algorithms.

The study results (Table 2) suggest as follows. To ensure the strength of S-box against the linear cryptanalysis, the elements of the table obtained during the linear cryptanalysis should take the values close to half the quantity of all possible combinations of input vectors in the binary notation. To ensure the strength of an S-box against the differential analysis, the elements of the table (difference matrix) obtained during the differential analysis should take the values close to 1.

The results of the encryption algorithm analysis are detailed in [14].

4 Conclusions

A software application to implement the encryption algorithm model has been developed, and the application is currently under testing. To study the statistical security of the proposed algorithm model, it has been developed a software package embedding statistical and assessment tests.

The work on improving and updating the software applications for the encryption algorithm based on nonpositional polynomial notations will continue. A computational model to keep and transfer key information for the algorithm is the next step of our studies.

It is further planned to use a round mode on the algorithm model, and develop a round key generation scheme.

Figure 6: Test results

Table 2: The interval of results of the linear and differential cryptanalyses

Name		Minimum	Maximum	Arithmetical mean minimum	Arithmetical mean maximum	Chi-square	Degree of freedom
DES	Linear	12	48	15,5	46,25	480	944
	Differential	0	16	0	16	20514	1007
GOST 28147-89	Linear	2	14	2,75	13,75	120	224
	Differential	0	8	0	6,25	480	239
GOST R 34.13-2015	Linear	100	156	-	-	32640	65024
	Differential	0	8	-	-	111297	65279
AES-128	Linear	111	145	-	-	32639	65024
	Differential	0	5	-	-	67125	65279
Encryption algorithm constructed on an SP-network	Linear	92	164	-	-	32640	65024
	Differential	0	12	-	-	130776	65279

Acknowledgement: Ongoing studies are funded by the Ministry of Education and Science of the Republic of Kazakhstan.

References

- [1] I. Ya. Akushskii, D. I. Juditskii, "Machine Arithmetic in Residue Classes," Moscow: Sov. Radio, 1968 (in Russian)
- [2] R. G. Biyashev, "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 (in Russian)
- [3] R. G. Biyashev, S. E. Nyssanbayeva Algorithm for Creation a Digital Signature with Error Detection and Correction, Cybernetics and Systems Analysis. – 2012, Vol. 48, No 4, 489-497
- [4] R. Biyashev, S. Nyssanbayeva, N. Kapalova, 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, pp.16-21
- [5] W. Stallings, Cryptography and Network Security: Principles and Practice, 2nd Edition, Transl. from English, M: Williams, 2001, 672 p.
- [6] L. K. Babenko, E. A. Ischukova, Modern Block Encryption Algorithms and Methods of their Analysis, Moscow, Helios, ARV, 2006, 376
- [7] B. Schneier, Applied Cryptography, 2nd ed.; Transl. from English — Triumph, 2002, 816
- [8] National Standard of the Russian Federation GOST R 34.13, <http://www.tc26.ru/standard/gost/GOSTR34.13-2015.pdf>, 2015, 21 p.
- [9] FIPS 46 3, Data Encryption Standard (DES). — USA, NIST, 1977
- [10] FIPS PUB 197. Advanced Encryption Standard (AES). — USA, NIST, 2002
- [11] Recommendation for Block Cipher Modes of Operation // NIST Special Publication 800-38A. Technology Administration U.S. Department of Commerce. - 2001, 10 p.
- [12] R. Biyashev, N. Kapalova, S. Nyssanbayeva, A. Haumen, Construction and analysis of models of increasing reliability for modular encryption algorithm // Proceedings of the 10th International Conference on Computer Engineering and Applications (CEA '16). – Barcelona, Spain, 2016. – pp. 161-165
- [13] R. Biyashev, S. Nyssanbayeva, N. Kapalova, A. Haumen, Modified symmetric block encryption-decryption algorithm based on modular arithmetic // Proceedings of the International Conference on Wireless Communications, Network Security and Signal Processing (WCNSSP2016). – Chiang Mai, Thailand, 2016. – pp. 263-265.
- [14] R. G. Biyashev, S. E. Nyssanbayeva, N. A. Kapalova, et al., FRPR&D F.0678, Development and study of national encryption algorithm models based on modular arithmetic, State Registration No. 0115RK01304. 175 p.