Modified Symmetric Block Encryption-Decryption Algorithm Based on Modular Arithmetic

Rustem Biyashev, Saule Nyssanbayeva, Armanbek Haumen and Nursulu Kapalova*
Information Security laboratory, Institute of Information and Computational Technologies CS MES RK, Almaty, Kazakhstan
*Corresponding author

***Abstract*—This paper addresses to a variation (modification) of a symmetric block encryption-decryption algorithm based on nonpositional polynomial notations (NPNs). The proposed encryption model includes two stages. The first stage is that a plaintext is split into bit blocks of a given length. Each plaintext block then undergoes an initial transformation, where a pseudorandom sequence (PRS or key sequence) is added bit by bit to the block through XOR operation. The key sequence is generated with a designed PRS generator. In the second stage, an encryption-decryption algorithm based on NPNs is applied to the transformed bit sequence. A computational model has been developed and implemented to test statistical properties of the sequences enciphered under the proposed modification of the encryption-decryption algorithm.**

Keywords-encryption; nonpositional polynomial notations; encryption model; software implementation

I. Introduction

Algorithms and methods developed on the basis of nonpositional polynomial notations (NPNs) are also known as nonconventional or nonpositional [1-2]. When considering a classical notation in residue number system (RNS), positive integers are chosen as a base system, where a positive integer is represented by its remainders (residues) of dividing by the base system. RNS construction relies on the Chinese remainder theorem. According to the theorem, a representation of a number as a sequence of remainders is unique providing that bases are pairwise relatively prime. As distinct from classical RNSs, irreducible polynomials over $GF(2)$ that is binary polynomials serve as bases in NPNs. Based on NPNs, nonconventional algorithms for encryption, digital signatures and cryptographic key exchange have been developed by now [2-4]. A research is also performing to evaluate their strength against cryptanalysis.

In order to enhance the strength of a nonconventional encryption-decryption algorithm, it has been proposed a modification of the algorithm with an additional procedure, where a key sequence is added modulo 2 to a plaintext. Using this procedure as a component of the modified encryption-decryption algorithm based on NPNs stems from the following characteristics thereof.

The information subject to encryption can have a structure with certain regularities, for instance, long series of consecutive zeroes or ones. To exclude presence of similar regularities in a ciphertext, a model involving additive pseudorandom sequence procedure (key sequence) has been considered. To produce a key sequence, a developed algorithm of pseudorandom bit generation (PRBG) is used [5]. The strength of this procedure is based on the premise that using statistically secure key bit streams guarantees a secure ciphertext for any plaintext. Claude Shannon proved that under certain conditions of a bit stream such encryption method is completely unbreakable [6]. Put it differently, such ciphertext does not contain any information from the respective plaintext.

II. Encryption-decryption algorithm modeling

The proposed modification (hereinafter referred to as the encryption algorithm) differs from the original encryption-decryption algorithm based on NPNs by its structure and cryptographic properties. The encryption algorithm can be used for blocks and keys of various length defined by a user (or a customer). The encryption algorithm scheme under consideration is comprised of two stages.

Stage 1. A plaintext is split into bit blocks of a given length. Each plaintext block then is subject to addition bit by bit of a key sequence through XOR operation.

Stage 2. The nonconventional encryption-decryption algorithm is applied to the block transformed at Stage 1 to get a block of ciphertext.

Let us consider the stages above in detail.

The core of a developed algorithm in use to generate a PRS is as follows. Two arbitrary numbers A and B, are multiplied together. A fixed quantity of any consecutive bits is extracted from the result $A_1 = A \cdot B$. The first extract is reserved as the first element g_1 of the generated bit sequence. Then A_1 multiplies by B, and similarly $B_1 = A_1 \cdot B$ serves as a basis for the second element g_2 of the key sequence. This completes the first step of building a part of key bit sequence in the form $\{g_1, g_2\}$. The second step of the above process is performed in the same way: A_1 multiplies by $B_1$and element g_3 is extracted from $A_2 = A_1 \cdot B_1$ in the manner mentioned above. Further, A_2 multiplies by $B_1$with g_4 extracted from $B_2 = A_2 \cdot B_1$, etc. Eventually, a key bit sequence $G = \{g_1, g_2, g_3, g_4, \dots\}$ of needed length is produced, i.e. the length of the key sequence is equal to the length of the enciphering block.

A key sequence is generated separately for each block, where two elements of the key sequence of a preceding block (intermediate results A_i and B_i) serve as a seed of PRS generator for a subsequent block, etc. Thus, a new key sequence is generated for each enciphering block. The advantage of the generator is that there is no need to necessarily hold the key sequences obtained, since it suffices to know an initial seed of small size.

Let us depict the encryption algorithm [2-4].

1. First of all an NPN is formed with its working bases consisting of chosen irreducible polynomials $p_1(x), p_2(x), \dots, p_S(x)$ over $GF(2)$ of degrees $m_1, m_2, \dots, m_S$ respectively. These polynomials subject to their arrangement constitute a certain base system. All bases should be different including the case when they have the same degree. The working range of the NPN is specified by polynomial (modulus) $P(x) = (\,p_1(x)p_2(x) \cdots p_S(x))$ of degree $m = \sum_{i=1}^{s} m_i$. The process of selection of a set of working bases is equivalent to finding all possible solutions of algebraic equation

$$k_1 m_1 + k_2 m_2 + \cdots + k_s m_s = N, \qquad (1)$$

where $0 \le k_i \le n_i$ are unknown coefficients, one particular set of which is a solution of (1) that defines a set of working bases; n_i is the number of all irreducible polynomials of degree m_i; $1 \le m_i \le N$; k_i is the number of selected irreducible polynomials of degree m_i; and $S = k_1 + k_2 + \cdots + k_S$ is the number of selected bases.

Therefore, a message (or its block) of length N bits 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 $p_1(x), p_2(x), \dots, p_S(x)$ respectively:

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

2. Encryption of a message of length N bits is performed with a key sequence of the same length, which is interpreted as a sequence of remainders $\beta_1(x), \beta_2(x), \dots, \beta_S(x)$ of dividing some other polynomial $G(x)$ by the same working bases of the system:

$$G(x) = (\,\beta_1(x), \beta_2(x), \dots, \beta_S(x)), \qquad (3)$$

where $G(x) \equiv \beta_i(x)\big(mod\; p_i(x)\big), i = \overline{1, s}$.

3. Cryptogram $H(x) = (\,\omega_1(x), \omega_2(x), \dots, \omega_S(x))$ is the result of multiplying polynomials (2) and (3). Members of residue sequence $\omega_1(x), \omega_2(x), \dots, \omega_S(x)$ are then remainders on dividing products $\alpha_i(x)\,\beta_i(x)$ by respective bases $p_i(x)$:

$$\alpha_i(x)\,\beta_i(x) \equiv \omega_i(x)\big(mod\; p_i(x)\big), i = 1,2, \dots, s. \qquad (4)$$

4. Decryption of cryptogram $H(x)$ with a known key $G(x)$ for each $\beta_i(x)$ represents evaluation of a reciprocal (inverse) polynomial ${\beta_i}^{-1}(x)$ under the following condition:

$$\beta_i(x) \times {\beta_i}^{-1}(x) = 1\big(mod\; p_i(x)\big), i = \overline{1, s} \qquad (5)$$

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 (4) and (5) through remainders of the following congruence:

$$\alpha_i(x) = {\beta_i}^{-1}(x)\omega_i(x)\big(mod\; p_i(x)\big), i = \overline{1, s} \qquad (6)$$

Hence, the complete key in the above model of encryption-decryption algorithm of a message of length N bits in NPNs is comprised of the chosen system of polynomial bases $p_1(x), p_2(x), \dots, p_S(x)$, key $G(x) = (\,\beta_1(x), \beta_2(x), \dots, \beta_S(x))$ obtained while generating a pseudo-random sequence, and inverse key $G^{-1}(x) = ({\beta_1}^{-1}(x), {\beta_2}^{-1}(x), \dots, {\beta_s}^{-1}(x))$ calculated according to expression (5).

For the purposes of implementation of the encryption-decryption algorithm based on NPNs and modifications thereof, software application KorganCryptv1.1 has been developed. The aim of the application is exploration of properties of encryption-decryption algorithm models. Encryption and decryption keys are kept in a specific file. To examine cryptograms subject to statistical security, graphical and assessment tests were used [7]. To check statistical properties of the encrypted files, software suite "Computer-aided system to choose statistical tests by L. Knuth and graphical tests" was used. This model has been also investigated subject to statistical properties of resulting ciphertexts. The testing performed has shown that ciphertexts of the modification have better statistical characteristics as compared to the original encryption-decryption algorithm based on NPNs. However, the rate of encryption is significantly reduced due to the fact that the key sequence is generated separately for each block.

III. Summary

Analysis of the proposed model of the original encryption-decryption algorithm based on NPNs has demonstrated a possibility of building the model, which can be recommended for implementation. In this context, further developments will be performed to build and investigate modifications of the encryption-decryption algorithm based on NPNs with the aim to improve statistical characteristics thereof. It is also planned to conduct works focused on enhancing effectiveness of software implementations of the models, and also studying effects of file formats on statistical properties of the models.

Acknowledgement

The research is funded by the Ministry of Education and Science of the Republic of Kazakhstan.

References

[1] 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).

[2] Bijashev, R.G., Kalimoldayev M.N.,Nyssanbayeva S.E., Kapalova N.A., Khakimov R.A.: Program Modeling of the Cryptography Algorithms on Basis of Polynomial Modular Arithmetic / The 5th International Conference on Society and Information Technologies (ICSIT 2014, March 4-7, 2014- Orlando, Florida, USE) – IIIS. pp. 49-54

[3] Biyashev R.G., Nyssanbayeva S.E., Begimbayeva Ye.Ye., Magzom M.M. Modification of the cryptographic algorithms, developed on the basis of nonpositional polynomial notations // Proceedings of the International Conference on Circuits, Systems, Signal Processing, Communications and Computers (CSSCC 2015), - Vienna, Austria., 2015, pp. 170-176.

[4] 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. – P.16.

[5] Kapalova N.A., Nyssanbayeva S.E.: Encrypting sequence generator for stream encryption. Proceedings of the IX International Research and Practice Conference // Information Security. P. 2. – Taganrog: TTI SFU Press, 2007. - 135-137 pp.

[6] Shannon C.E. Communication Theory of Secrecy Systems // BellSyst. Tech. Journal. - 1949. – Vol.2

[7] Ivanov, M.A., Chugunkov, I.V.: The theory, application and evaluation of the quality of pseudo-random sequence generator. CUDYC-OBRAZ, Moscow, 2003, P. 240.

[8] Kapalova N.A., Nyssanbayeva S.E. Investigation of algorithm of generation of pseudorandom sequences // Information Technologies and Security. Information Security Management: Proceedings, Kiev, 2007. No. 10. - pp. 32-39.

[9] Kapalova N.A., Nyssanbayeva S.E.: Analysis of statistical properties of algorithm of generation of pseudorandom sequences, Proceedings of the X International Research and Practice Conference Information security, P. 2., Taganrog: TTI SFU Press, 2008, pp. 169-172.