Cryptographic System in Polynomial Residue Classes for Channels with Noise and Simulating Attacker

O. Finko[1], D. Samoylenko[2]

Kuban State University of Technology.
Moscow street, 2, Krasnodar 350072, Russia
[1]ofinko@member.ams.org, [2]19sam@mail.ru

Abstract: ***Noise-resistant modular cryptographic system that functions in polynomial residue classes is considered in this article. An algorithm for bases expansion of the cryptographic system is suggested. An estimation of interference-stability of proposed cryptographic system in relation to the traditional system is presented.***

Keywords: Chinese Remainder Theorem, cryptanalyst, cryptography, cryptosystem, modular arithmetic, polynomial residue classes, Galois fields, interference coding**.**

1. Introduction

The main goal of any cryptographic system (CS) is to protect data from uncontrolled changes during their transmitting via public communication channels or other usage. Ability of CS to provide this protection makes it sensitive to the distortion influence of different origin (random noise, cryptanalyst's simulating actions) while transmitting via communication channels. Change of one bit of encrypted data (cryptograms) may lead to partial or complete loss of decrypted data, which in turn will lead to loss of management and control while carrying out different tasks, that's why it's necessary to use CS adapted to work in such conditions to transmit cryptograms accurately.

At the same time, there already exist approaches to creating such CS [1, 2]. In works [3-5], a block CS functioning in the $\mathbb{Z}_p$ ring of non-negative integers modulo p was considered. However, it is known that systems functioning in the Galois field with characteristic 2 possess a number of advantages, such as high performance, ease of implementation and effectiveness.

Purpose of this article is to develop interference -stable modular CS in the polynomial ring $\mathrm{GF}(2)$, able to resist destructive influences, both intentional and unintentional.

2. System architecture

CS that is able to resist the destructive effects of different origin was suggested in [3-6]. Encryption and decryption rules are defined in a general form:

$$C \to E_{k_1}: M, \tag{1}$$

$$M \to D_{k_2}: C, \tag{2}$$

where C – cryptogram, M – plaintext, k_1 and k_2 – encryption and decryption keys. When $k_1 \neq k_2$ CS is called asymmetric, and when $k_1 = k_2$ – symmetric [7, 8].

Plaintext M is divided into blocks $M_1, M_2, \ldots, M_n$, where M_i – m-bit block of plaintext. Accordingly, n encryption operations and n decryption operations will be required to obtain cryptograms sequence $C_1, C_2, \ldots, C_n$. Therefore, the transformations (1) and (2) can be rewritten as

$$\begin{cases} C_1 \to E_{k_{1,1}}: M_1, \\ C_2 \to E_{k_{1,2}}: M_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ C_n \to E_{k_{1,n}}: M_n; \end{cases} \tag{3}$$

$$\begin{cases} M_1 \to D_{k_{1,1}}: C_1, \\ M_2 \to D_{k_{1,2}}: C_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ M_n \to D_{k_{1,n}}: C_n; \end{cases} \tag{4}$$

where $k_{1,i} \neq k_{2,i}$ or $k_{1,i} \neq k_{2,i}$ $(i = 1, 2, \ldots, n)$ in corresponding cases.

Let's consider the cryptograms blocks system (3) in a form of binary vectors system:

$$\begin{cases} \mathbf{C}_1 = \left[c_{m-1}^{(1)} \quad c_{m-2}^{(1)} \quad \cdots \quad c_0^{(1)}\right], \\ \mathbf{C}_2 = \left[c_{m-1}^{(2)} \quad c_{m-2}^{(2)} \quad \cdots \quad c_0^{(2)}\right], \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \mathbf{C}_n = \left[c_{m-1}^{(n)} \quad c_{m-2}^{(n)} \quad \cdots \quad c_0^{(n)}\right]; \end{cases} \tag{5}$$

where $c_j^{(i)} \in \{0, 1\}$; $i = 1, 2, \ldots, n$; $j = m-1, m-2, \ldots, 0$.

We will represent the coefficients $c_j^{(i)}$ of system (5) as a coefficients of algebraic polynomials of Galois fields $\mathrm{GF}(p)$ with characteristic $p = 2$. Then (5) takes the form:

$$\begin{cases} C_1(x) = c_{m-1}^{(1)} x^{m-1} + c_{m-2}^{(1)} x^{m-2} + \cdots + c_0^{(1)}, \\ C_2(x) = c_{m-1}^{(2)} x^{m-1} + c_{m-2}^{(2)} x^{m-2} + \cdots + c_0^{(2)}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ C_n(x) = c_{m-1}^{(n)} x^{m-1} + c_{m-2}^{(n)} x^{m-2} + \cdots + c_0^{(n)}; \end{cases}$$

While transmitting the cryptograms sequence $C_1(x), C_2(x), \dots, C_n(x)$, distortion influence manifests itself as that instead of sent cryptograms other $C_1^*(x), C_2^*(x), \dots, C_n^*(x)$ are accepted. Accordingly, as a result of accepted cryptograms decryption the recipient receives the plaintext blocks $M_1^*(x), M_2^*(x), \dots, M_n^*(x)$ that differ from the original.

We will represent $C_i(x)$ as the least non-negative polynomial residues on the polynomial grounds $m_i(x)$, such as $\gcd\left(m_i(x), m_j(x)\right) = 1$, where $i \neq j$; $i, j = 1, 2, \dots, n$, and $0 \leq \deg C_i(x) < \deg m_i(x)$, where $\deg C_i(x)$ is the power of polynom $(i = 1, 2, \dots, n)$. Then we can consider cryptogram set $\{C_1(x), C_2(x), \dots, C_n(x)\}$ as a single information unit of the modular polynomial code (MPC) on the polynomial bases system $m_1(x), m_2(x), \dots, m_n(x)$. According to the Chinese Remainder Theorem for polynomials [9, 10] for a given set of pairwise relatively prime polynomials $m_1(x), m_2(x), \dots, m_n(x)$ and a set of polynomials $C_1(x), C_2(x), \dots, C_n(x)$, such that $\deg C_i(x) < \deg m_i(x)$ the simultaneous congruences

$$\begin{cases} C(x) = C_1(x) \bmod m_1(x), \\ C(x) = C_2(x) \bmod m_2(x), \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ C(x) = C_n(x) \bmod m_n(x) \end{cases} \quad (6)$$

has got the unambiguous solution $C(x)$.

MPC expansion operation $\{C_1(x), C_2(x), \dots, C_n(x)\}$ is executed by introducing r redundant polynomial grounds $m_{n+1}(x), m_{n+2}(x), \dots, m_{n+r}(x)$ and receiving r redundant residues $C_{n+1}(x), C_{n+2}(x), \dots, C_{n+r}(x)$:

$$\begin{cases} C_{n+1}(x) = C(x) \bmod m_{n+1}(x), \\ C_{n+2}(x) = C(x) \bmod m_{n+2}(x), \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ C_{n+r}(x) = C(x) \bmod m_{n+r}(x). \end{cases}$$

And $\gcd\left(m_i(x), m_j(x)\right) = 1$, where $i \neq j$; $i, j = 1, 2, \dots, n + r$ and $\deg m_1(x), \dots, \deg m_n(x) < \deg m_{n+1}(x) < \dots \dots < \deg m_{n+r}(x)$.

Together, information block elements $\{C_1(x), C_2(x), \dots, C_n(x)\}$ and obtained redundant cryptogram sequence $\{C_{n+1}(x), C_{n+2}(x), \dots, C_{n+r}(x)\}$ form extended MPC in the polynomial ring $F[x]$ over GF(2).

Let's introduce MPC and linear binary code (LBC) metric.

MPC metric: *code vector weight* $\{C(x)\}$ in MPC is a number of non-nil cryptograms (deductions) and it is designated as $w(\{C(x)\})$.

Code distance between $\{C(x)\}$ and $\{D(x)\}$ is estimated as their difference weight $w(\{C(x) - D(x)\})$.

Minimum code distance of MPC is the shortest distance between any of two code vectors according to Hamming taking into account the given weight definition.

We understand arbitrary distortion of one of the MPC code word cryptograms under a single mistake in the MPC code word. Accordingly, multiple q error is defined as arbitrary distortion of q cryptograms of the MPC code word.

The obtained code detects all single errors, if the amount of redundant cryptograms $r \geq 1$, and corrects q or less errors if $2q \leq r$.

Detection of errors in the accepted cryptogram sequence $C_1^*(x), \dots, C_n^*(x), \dots, C_{n+r}^*(x)$ is executed by comparing $C^*(x)$ with $M(x) = \prod_{i=1}^{n} m_i(x)$, where simultaneous congruences solution (6) for accepted cryptogram sequence $C_i^*(x)$ $(i = 1, 2, \dots, n + r)$; $*$ - indicates possible distortions.

If $0 \leq C^*(x) < M(x)$, then it is decided that the accepted cryptogram sequence $C_1^*(x), \dots, C_n^*(x), \dots, C_{n+r}^*(x)$ doesn't contain detectable errors. If not, the error with the maximum multipleness determined by the code detecting abilities is detected [11, 12].

LBC metric corresponds to the Hamming metric. Code word *norm (or weight)* $x = (x_1, x_2, \dots, x_n)$ is a number of non-nil symbols.

Code distance between words $x = (x_1, x_2, \dots, x_n)$ and $y = (y_1, y_2, \dots, y_n)$ of linear binary code over GF(2) is equal to the weight of their difference.

Minimum LBC code distance is the minimum distance of all possible pairwise distances between the code words and it is equal to $d_{\min}$.

We understand one bit cryptogram distortion under a single error in the LBC metric $C_i(x)$. Accordingly, multiple t error is defined as an arbitrary distortion t of bit cryptogram $C_i(x)$.

Example of *n*-channel CS with one redundant channel is shown in Fig. 1.

Thus, the redundancy introduced in the form of redundant cryptograms secures CS's properties to control MPC code word errors (number of distorted cryptograms) and correct errors in a certain cryptogram (number of distorted bits).

3. Algorithm of expansion of system of the bases MPC

MPC expansion is one of the main operations executed in the given CS. An extension algorithm of modular code that operates in the $\mathbb{Z}_p$ ring is suggested in [6].

Let us consider this algorithm with regard to our CS. It consists in solving simultaneous congruences (6). According to the Chinese Remainder Theorem for polynomials [9, 10], the solution of simultaneous congruences (6) corresponds to the expression

$$C(x) = \sum_{i=1}^{n} C_i(x) B_i(x) - r_C(x) M(x), \quad (7)$$

where $B_i(x) = k_i(x) M_i(x)$ – polynomial orthogonal bases, $M_i(x) = \frac{M(x)}{m_i(x)}$, $M(x) = \prod_{i=1}^{n} m_i(x)$, $r_C(x)$ – rank $C(x)$, $k_i(x) = M_i^{-1}(x) \bmod m_i(x)$ for $i = 1, 2, \dots, n$.

It is natural to assume that the definition of $r_C(x)$ will be made directly during the expansion operation execution.

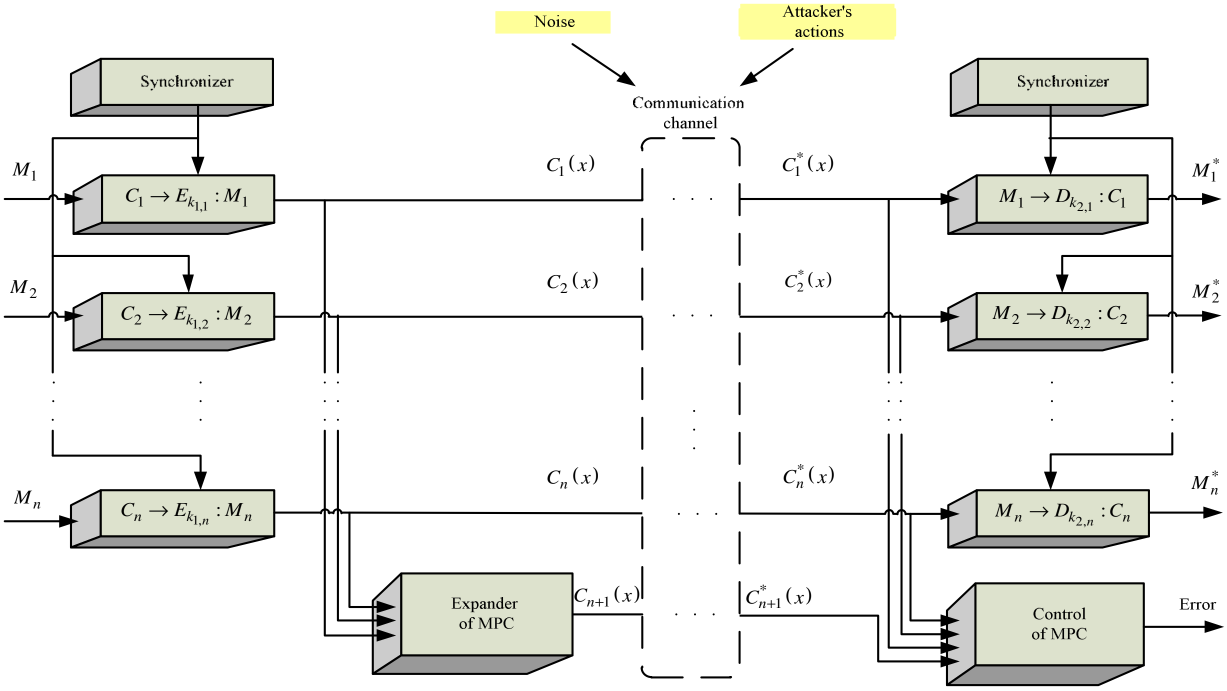

Figure 1. CS with detection of single errors

Then

$$r_C(x) = \text{Quotient}\left(\frac{C_i(x)k_i(x)}{m_i(x)}\right), \qquad (8)$$

where Quotient $\left(\frac{C_i(x)k_i(x)}{m_i(x)}\right)$ – the least integer from the division of $C_i(x)k_i(x)$ on the basis of $m_i(x)$, for $i = 1, 2, \ldots, n$.

To obtain $C_{n+1}(x)$ equation (7) taking into account (8) will look like

$$\begin{aligned} C_{n+1}(x) &= C_1(x)\beta_1(x) \bmod m_{n+1}(x) + \\ &+ C_2(x)\beta_2(x) \bmod m_{n+1}(x) + \cdots \\ &\ldots + C_n(x)\beta_n(x) \bmod m_{n+1}(x) - \\ &- r_C(x)\mu(x) \bmod m_{n+1}(x), \end{aligned}$$

where $\beta_i(x) = B_i(x) \bmod m_{n+1}(x)$, $\mu(x) = M(x) \bmod m_{n+1}(x)$, for $i = 1, 2, \ldots, n$.

Let's perform

$$\begin{aligned} &G_1(x) = C_1(x)\beta_1(x) \bmod m_{n+1}(x) = \\ &= g_{m-1}^{(1)}x^{m-1} + g_{m-2}^{(1)}x^{m-2} + g_{m-3}^{(1)}x^{m-3} + \cdots + g_0^{(1)}, \\ &G_2(x) = C_2(x)\beta_2(x) \bmod m_{n+1}(x) = \\ &= g_{m-1}^{(2)}x^{m-1} + g_{m-2}^{(2)}x^{m-2} + g_{m-3}^{(2)}x^{m-3} + \cdots + g_0^{(2)}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &G_n(x) = C_n(x)\beta_n(x) \bmod m_{n+1}(x) = \\ &= g_{m-1}^{(n)}x^{m-1} + g_{m-2}^{(n)}x^{m-2} + g_{m-3}^{(n)}x^{m-3} + \cdots + g_0^{(n)}, \\ &A(x) = r_C(x)\mu(x) \bmod m_{n+1}(x) = \\ &= a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + a_{m-2}x^{m-2} + \cdots + a_0. \end{aligned}$$

Let's imagine polynomials $G_i(x)$ $(i = 1, 2, \ldots, n)$ and $A(x)$ as a sequence of binary coefficients:

$$\begin{aligned} \mathbf{G}_1(x) &= [g_{m-1}^{(1)} \quad g_{m-2}^{(1)} \quad g_{m-3}^{(1)} \quad \cdots \quad g_0^{(1)}], \\ \mathbf{G}_2(x) &= [g_{m-1}^{(2)} \quad g_{m-2}^{(2)} \quad g_{m-3}^{(2)} \quad \cdots \quad g_0^{(2)}], \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \mathbf{G}_n(x) &= [g_{m-1}^{(n)} \quad g_{m-2}^{(n)} \quad g_{m-3}^{(n)} \quad \cdots \quad g_0^{(n)}], \\ \mathbf{A}(x) &= [a_{m-1} \quad a_{m-2} \quad a_{m-3} \quad \cdots \quad a_0]. \end{aligned}$$

We obtain

$$\begin{aligned} C_{n+1}(x) &= x^{m-1}\left(a_{m-1} \oplus (g_{m-1}^{(1)} \oplus \ldots \oplus g_{m-1}^{(n)})\right) + \\ &+ x^{m-2}\left(a_{m-2} \oplus (g_{m-2}^{(1)} \oplus \ldots \oplus g_{m-2}^{(n)})\right) + \\ &+ x^{m-3}\left(a_{m-3} \oplus (g_{m-3}^{(1)} \oplus \ldots \oplus g_{m-3}^{(n)})\right) + \ \ldots \\ &\ldots + \left(a_0 \oplus (g_0^{(1)} \oplus \ldots \oplus g_0^{(n)})\right) \bmod m_{n+1}(x) = \\ &= \sum_{j=0}^{m-1} x^j \left((a_j \oplus g_j^{(1)}) \oplus \ldots \oplus (a_j \oplus g_j^{(n)})\right) \bmod m_{n+1}(x). \end{aligned}$$

According to the Chinese Remainder Theorem for polynomials, the above transformations allow us without direct determination of $C(x)$ to get the final equation in order to calculate $C_{n+1}(x)$.

4. Noise stability estimation CS

The need to assess the reliability of data transmission appears due to the ability of CS to detect and correct mistakes. To solve the problem, let us calculate the reliability of data transmission through the communication channel for the proposed multichannel CS and prototype CS that utilizes linear codes.

Under reliability we understand degree of conformity between cryptograms received and cryptograms transferred. Numerically, the reliability of data transmission will be characterized as a probability of guaranteed error detection in cryptograms on the receiving side of the CS.

Let us introduce a presumption: errors of multiplicity q in the transmitted sequence of cryptograms $C_1(x), \dots, C_n(x), \dots, C_{n+r}(x)$ occur independently of each other and their distribution obeys the binomial law:

$$P(q) = \sum_{q=1}^{n} \binom{n}{q} p^q (1-p)^{n-q}.$$

In order to assess the extent of the destructive effect on the transmitted sequence of cryptograms $C_1(x), \dots, C_n(x), \dots, C_{n+r}(x)$, it is necessary to know the value of p of probability of erroneous cryptogram $C_i(x)$ reception. P of probability of erroneous cryptogram $C_i(x)$ reception is constant and is calculated if the pattern of distortions caused by the actions of a cryptanalyst is known.

Actions of a cryptanalyst on a cryptogram $C_i(x)$ are analytical, so the effects of such actions are unpredictable and random for the receiving side. Let us introduce a presumption: distortions caused by actions of a cryptanalyst on the cryptogram $C_i(x)$ are equiprobable.

Let p_{cr} be the possibility of distortion of the cryptogram's $C_i(x)$ bit caused by the actions of cryptanalyst. Based on the presumptions and considering $d_{\min}$ let's determine the possibility of distortion of the cryptogram $C_i(x)$ for the CS prototype, caused by the actions of a cryptanalyst:

$$p_{cr_1} = 2^{-h} p_{cr} \sum_{t=i+1}^{h} \binom{h}{t},$$

where $\sum_{t=i+1}^{h} \binom{h}{t}$ – the total amount of distortions in the cryptogram $C_i(x)$ that cannot be determined by this method of control; $i+1 \le t \le h$ – multiplicity of errors that cannot be determined by this method of control; h – cryptogram's block length; 2^h – the total amount of possible distortions.

For multichannel CS, the possibility of distortions of the cryptogram $C_i(x)$ caused by actions of a cryptanalyst, equals:

$$p_{cr_2} = 2^{-h} p_{cr} \sum_{i=1}^{t} \binom{h}{t} = p_{cr},$$

as CS controls errors of any multiplicity within a single cryptogram $C_i(x)$.

In that case the possibility of guaranteed detection of errors for CS prototype using linear code is equal:

$$P_{er_1} = \sum_{q=1}^{n} \binom{n}{q} p_{cr_1}^q (1 - p_{cr_1})^{n-q}.$$

For the given CS, the possibility of guaranteed detection of errors equals

$$P_{er_2} = \sum_{q=0}^{d_{\min}-1} \binom{l}{q} p_{cr_2}^q (1 - p_{cr_2})^{l-q},$$

where $l = n + r$.

Dependence P_{er_1}, P_{er_2} and benefit $P_{er_2} - P_{er_1}$ from the redundancy coefficient (linear – in the first case and modular – in the second case) of the used code with consideration of the limits $p_{cr} = 1{,}5 \times 10^{-1}$, $l = 12$, are shown on the picture 2. Here $K_r = 1 - \frac{n}{l}$ – redundancy coefficient.

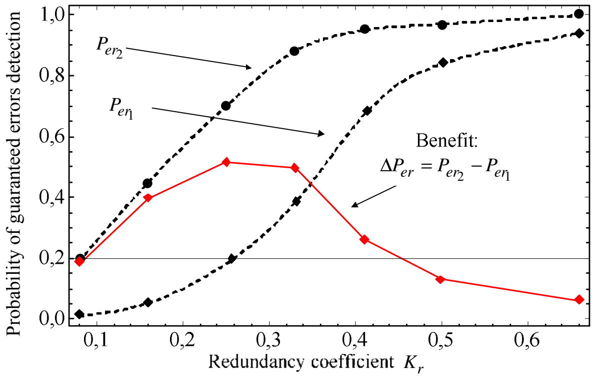

Figure 2. Dependence of the guaranteed detectable errors from the redundancy coefficient

Therefore, this article proposes an interference-stable CS operated in the ring of polynomials GF(2) oriented for use in the contemporary and prospective multiuser encoding communication channels. A distinctive feature of the proposed CS is a complete invariance to the multiplicity of message errors in encrypted communication channels with a limited number of individual users. In addition to the increase of the interference stability, the increase of the imitation resistance of CS is achieved, too. Also a significant advantage is that the proposed CS is based on the existing single-channel CS. If the initial CS is certified, then the issue of certification of the proposed CS can be solved with consideration of restriction imposed on the process of obtaining the keys and compliance of operating.

References

[1] W. Goboy, D. Periera, "A proposal of a cryptography algorithm with techniques of error correction" Computer Communications 20(15), pp. 1374-1380, 1997. (journal style)

[2] R.J. McEliece, "Pablic-key cryptosystem based on algebraic coding theory" In DSN Progress Report 42-44, pp. 114-116, 1978.

[3] O. Finko, "The group control asymmetric cryptographic system methods of modular arithmetics" XIV International workshop Synthesis and Complexity of controlling systems (MSU of Lomonosova; Nizhny Novgorod state pedagogical university); Under edition of the academician of the Russian Academy of Sciences O.B. Lupanova, pp. 85-86, 2003. (conference style)

[4] O. Finko, "Constructions that control errors on the base of active cryptographic standards" VIII International conference Discrete models in the theory of control systems (MSU of Lomonosova), pp. 318-320, 2009. (conference style)

[5] O. Finko, "Multichannel modular system stable to distortion of cryptograms," in team monograph Cryptographic methods of information security, Radiotekhnika, Moscow, 2007. (book chapter style)

[6] O. Finko, D. Samoylenko, "Cryptographic system in polynomial residue classes for channels with noise and simulating attacker" Radio communication theory and equipment 4, pp. 39-44, 2010. (journal style)

[7] B. Schneier, "Applied Cryptography". John Wiley & Sons, Inc. 1996. (book style)

[8] A. Menezes, P. van Oorschot, S. Vanstone, "Handbook of Applied Cryptography". CRC Press, 1997. (book style)

[9] E.R. Berlekamp, "Algebraic Coding Theory". McGraw-Hill. New York. 1968. (book style)

[10] R.E. Blahut, "Theory and practice of error control codes". Addison-Wesley PC. Massachusetts.1984. (book style)

[11] D. Mandelbaum, "Error correction in residue arithmetic", IEEE Trans. Comput., 21(6), pp. 538-545, 1972. (journal style)

[12] N. Szabo and R. Tanaka, "Residue Arithmetic and its Application to Computer Technology". McGraw-Hill. New York. 1967. (book style)

Oleg Finko - professor, Doctor of Technical Sciences. Professor of Department of computer technologies and information security of the Kuban State University of Technology. Research interests - a residue number system, the use of error-correcting coding techniques in cryptography, multi-biometric encryption, digital signature algorithms improve, secure electronic document systems, parallel computing logic by modular numerical polynomials. URL: http://www.mathnet.ru/eng/person/40004

Dmitriy Samoylenko - PhD, Research interests - a system of residual classes in cryptography, the use of error-correcting coding techniques in cryptography.