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

O. Finko¹, D. Samoylenko²

Kuban State University of Technology.
Moscow street, 2, Krasnodar 350072, Russia
¹oinko@member.ams.org, ²sam@eml.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 influences 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 blockCS functioning in the field 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 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:

\[ C \rightarrow E_{k_1}: M, \]
\[ M \rightarrow D_{k_2}: C, \]

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 \( M_1, M_2, ..., M_{m} \), where \( M_i \) – \( m \)-bitblock of plaintext. Accordingly, encryption operations and decryption operations will be required to obtain cryptogram sequence \( C_1, C_2, ..., C_n \). Therefore, the transformations (1) and (2) can be rewritten as

\[
\begin{align*}
C_1 & \rightarrow E_{k_{1,1}}: M_1, \\
C_2 & \rightarrow E_{k_{1,2}}: M_2, \\
\vdots & \vdots \vdots \\
C_n & \rightarrow E_{k_{1,n}}: M_n, \\
M_1 & \rightarrow D_{k_{1,1}}: C_1, \\
M_2 & \rightarrow D_{k_{1,2}}: C_2, \\
\vdots & \vdots \vdots \\
M_n & \rightarrow D_{k_{1,n}}: C_n;
\end{align*}
\]

Where \( k_{1,j} \neq k_{2,j} \) or \( k_{1,j} \neq k_{2,j} \) (\( i = 1, 2, ..., n \)) in corresponding cases.

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

\[
\begin{align*}
C_1 & = [c_{1}^{(1)} c_{m-1}^{(1)} ... c_{0}^{(1)}], \\
C_2 & = [c_{1}^{(2)} c_{m-1}^{(2)} ... c_{0}^{(2)}], \\
\vdots & \vdots \vdots \vdots \\
C_n & = [c_{1}^{(n)} c_{m-1}^{(n)} ... c_{0}^{(n)}];
\end{align*}
\]

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

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

\[
\begin{align*}
C_1(x) & = c_{m-1}^{(1)} x^{m-1} + c_{m-2}^{(1)} x^{m-2} + ... + c_{0}^{(1)}, \\
C_2(x) & = c_{m-1}^{(2)} x^{m-1} + c_{m-2}^{(2)} x^{m-2} + ... + c_{0}^{(2)}, \\
\vdots & \vdots \vdots \vdots \\
C_n(x) & = c_{m-1}^{(n)} x^{m-1} + c_{m-2}^{(n)} x^{m-2} + ... + c_{0}^{(n)};
\end{align*}
\]

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

We will represent \( C(x) \) as the least non-negative polynomial residues on the polynomial grounds \( m_i(x) \), such as...
\[ \gcd \left( m_i(x), m_j(x) \right) = 1, \quad \text{where } i \neq j; \quad i, j = 1, 2, \ldots, n, \quad \text{and} \quad 0 \leq \deg C_i(x) < \deg m_i(x), \quad \text{where } \deg C_i(x) \text{ is the power of polynomial } (i = 1, 2, \ldots, n). \]

Then we can consider cryptogram set \( \{C_1(x), C_2(x), \ldots, C_n(x)\} \) as a single information unit of the modulor polynomial code (MPC) on the polynomial bases system \( m_1(x), m_2(x), \ldots, m_n(x) \). According to the Chinese Remainder Theorem for polynomials [9, 10] for a given set of pairwise relatively prime polynomials \( m_1(x), m_2(x), \ldots, m_n(x) \) and a set of polynomials \( C_1(x), C_2(x), \ldots, C_n(x) \), such that \( \deg C_i(x) < \deg m_i(x) \) the simultaneous congruences

\[
\begin{align*}
C(x) &= C_1(x) \mod m_1(x), \\
C(x) &= C_2(x) \mod m_2(x), \\
&\vdots \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \ Quad
Then

\[
r_C(x) = \text{Quotient} \left( \frac{C_i(x)k_i(x)}{m_i(x)} \right),
\]

where \( \text{Quotient} \left( \frac{C_i(x)k_i(x)}{m_i(x)} \right) \) is the least integer from the division of \( C_i(x)k_i(x) \) on the basis of \( m_i(x) \), for \( i = 1, 2, ..., n \). To obtain \( C_{n+1}(x) \) equation (7) taking into account (8) will look like

\[
C_{n+1}(x) = C_i(x)\beta_i(x)(x) \mod m_{n+1}(x) + \ 
+ C_2(x)\beta_2(x)(x) \mod m_{n+1}(x) + ... \ 
+ C_n(x)\beta_n(x)(x) \mod m_{n+1}(x) - \ 
- r_C(x)\mu(x) \mod m_{n+1}(x),
\]

where

\[
\beta_i(x) = B_i(x) \mod m_{n+1}(x), \quad \mu(x) = M(x) \mod m_{n+1}(x),
\]

for \( i = 1, 2, ..., n \).

Let’s perform

\[
G_1(x) = C_i(x)\beta_i(x)(x) \mod m_{n+1}(x) = \ 
= g_{m-1}^{(1)}x^{m-1} + g_{m-2}^{(1)}x^{m-2} + g_{m-3}^{(1)}x^{m-3} \cdots + g_0^{(1)},
\]

\[
G_2(x) = C_2(x)\beta_2(x)(x) \mod m_{n+1}(x) = \ 
= g_{m-1}^{(2)}x^{m-1} + g_{m-2}^{(2)}x^{m-2} + g_{m-3}^{(2)}x^{m-3} \cdots + g_0^{(2)},
\]

\[
G_i(x) = C_i(x)\beta_i(x)(x) \mod m_{n+1}(x) = \ 
= g_{m-1}^{(i)}x^{m-1} + g_{m-2}^{(i)}x^{m-2} + g_{m-3}^{(i)}x^{m-3} \cdots + g_0^{(i)};
\]

\[
A(x) = r_C(x)\mu(x) \mod m_{n+1}(x) = \ 
= a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + a_{m-3}x^{m-3} \cdots + a_0.
\]

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

\[
G_1(x) = \left( g_{m-1}^{(1)} g_{m-2}^{(1)} g_{m-3}^{(1)} \cdots g_0^{(1)} \right),
\]

\[
G_2(x) = \left( g_{m-1}^{(2)} g_{m-2}^{(2)} g_{m-3}^{(2)} \cdots g_0^{(2)} \right),
\]

\[
G_i(x) = \left( g_{m-1}^{(i)} g_{m-2}^{(i)} g_{m-3}^{(i)} \cdots g_0^{(i)} \right),
\]

\[
A(x) = \left( a_{m-1} a_{m-2} a_{m-3} \cdots a_0 \right).
\]

We obtain

\[
C_{n+1}(x) = x^m(c_{n+1}(x) + \cdots + c_n(x)(x) \mod m_{n+1}(x) = \ 
= \sum_{i=0}^{n-1} x^i \beta_i(x) g_i^{(i)} \mod m_{n+1}(x)
\]

According to the Chinese Remainder Theorem for polynomials, the above transformations allow us without direct determination \( f(C(x)) \) 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 \( C_1(x), \ldots, C_n(x), \ldots, C_{n+r}(x) \) occur independently of each other and their distribution obeys the binomial law:

\[
P(q) = \sum_{q=1}^{n} \left( \begin{array}{c} n \\ q \end{array} \right) p^q (1-p)^{n-q}.
\]

In order to assess the extent of the destructive effect on the transmitted sequence of cryptograms \( C_1(x), \ldots, C_n(x), \ldots, C_{n+r}(x) \), it is necessary to know the value of \( p \) of probability of erroneous cryptogram \( C_i(x) \) reception. 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 a 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:

\[
p_{cr_1} = 2^{-h} p_{cr} \sum_{t=1}^{h} \left( \begin{array}{c} h \\ t \end{array} \right) p_t^h (1-p_t)^{h-t},
\]

Where \( \sum_{t=1}^{h} \left( \begin{array}{c} h \\ t \end{array} \right) \) – the total amount of distortions in the cryptogram \( C_i(x) \) that cannot be determined by this method of control; \( 1 \leq t \leq h \) – 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:

\[
p_{cr_2} = 2^{-h} p_{cr} \sum_{t=1}^{r} \left( \begin{array}{c} h \\ t \end{array} \right) = p_{cr},
\]

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:

\[
P_{cr_1} = \sum_{q=1}^{n} \left( \begin{array}{c} n \\ q \end{array} \right) p_{cr_1}^q (1-p_{cr_1})^{n-q}.
\]

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

\[
P_{cr_2} = \sum_{q=0}^{d_{min}-1} \left( \begin{array}{c} l \\ q \end{array} \right) p_{cr_2}^q (1-p_{cr_2})^{l-q},
\]

where \( l = n + r \).

Dependence \( P_{cr_1} \) and benefit \( P_{cr_2} - P_{cr_1} \) from the redundancy coefficient (linear – in the first case and modular – in the second case) of the used code with consideration of the limits \( p_{cr} = 1.5 \times 10^{-3}, l = 12 \), 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](image)

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 restrictions imposed on the process of obtaining the keys and compliance of operating.

**References**


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](http://www.mathnet.ru/eng/person/40004)

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