ISSN 2519-2310

COMPUTER SCIENCE AND CYBERSECURITY

ISSUE 4(8) 2017

V. N. Karazin Kharkiv National University Publishing

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ
MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені В.Н.КАРАЗІНА
ХАРЬКОВСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ имени В.Н. КАРАЗИНА
V.N. KARAZIN KHARKIV NATIONAL UNIVERSITY

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА
КОМПЬЮТЕРНЫЕ НАУКИ И КИБЕРБЕЗОПАСНОСТЬ
COMPUTER SCIENCE AND CYBERSECURITY
(CS&CS)

Issue 4(8) 2017

Заснований 2015 року

Міжнародний електронний науково-теоретичний журнал
Международный электронный научно-теоретический журнал
International electronic scientific journal

The journal publishes research articles on theoretical, scientific and technical problems of effective facilities development for computer information communication systems and on information security problems based on advanced mathematical methods, information technologies and technical means.

Journal is published quarterly.
Approved for placement on the Internet by Academic Council of the Karazin Kharkiv National University (April 27, 2018, protocol No.5).

Editorial office:
Karazin Kharkiv National University
Svobody sq., 6, office 315a, Kharkiv, 61022, Ukraine
Phone: +38 (057) 705-10-83
E-mail: *cscsjournal@karazin.ua*
Web-page: *http://periodicals.karazin.ua/cscs (Open Journal System)*

Published articles have been internally and externally peer reviewed

TABLE OF CONTENTS

Issue 4(8) 2017

UDC 004.056.55

NTRU PRIME IIT UKRAINE ENCRYPTION ALGORITHM WITH CONSIDERATION KNOWN ATTACKS ANALYSIS

Ivan Gorbenko[1], Olena Kachko[2], Maryna Yesina[1]

[1] V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
gorbenkoi@iit.kharkov.ua, rinayes20@gmail.com
[2] JSC «Institute of Information Technologies», Kharkiv, Kharkiv National University of Radio Electronics, Nauka Ave., 14, Kharkov, 61022, Ukraine
kachko@iit.com.ua, iit@iit.kharkov.ua

Reviewer: Roman Oliynikov, Doctor of Sciences (Engineering), Full Professor, V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
roliynykov@gmail.com

Received on November 2017

Abstract: *The paper deals with the modern cryptographic transformations of the asymmetric end-to-end encryption type, namely – NTRU-like cryptographic systems. A new cryptographic system NTRU Prime IIT Ukraine was created based on existing cryptographic transformations of this type (cryptographic algorithms NTRU (ANSI X9.98-2010) and NTRU Prime). A brief description of this cryptographic system is given and an analysis of its resistance to known attacks is made. At the end of the work, conclusions are made and recommendations on the features, advantages and possibilities of using the new cryptographic asymmetric algorithm of end-to-end encryption NTRU Prime IIT Ukraine are given.*

Keywords: *NTRU Prime, Attack, Ring, End-to-End Encryption, Field, Quotient Ring.*

1 Introduction

In 2016-2017 there were the series of important events, that have significantly affected to the intensive development of post-quantum cryptography. To them should be referred the statement on the Internet – Alfred J. Menezes and Neal Koblitz article [2], organization and conduction by NSA and NIST USA VII international conference on post quantum cryptography [5, 6]. An extremely important event was the publication in the USA report «Report on Post – Quatum Cryptography. NISTIR 8105 (DRAFT)» [3], in which fully confirmed the possibility of electronic signature (ES) asymmetric cryptographic primitives successful quantum cryptanalysis and the main problems and opportunities, and stages of their decision are identified.

NIST USA announced a competition to develop the standards of post-quantum asymmetric cryptographic primitives [5], understanding the need to find new electronic signature and asymmetric encryption type cryptographic transformation, which will be relevant and can be applied in post-quantum period. The specified one due to two factors. First, there is significant progress in the development of quantum computers, including experimental demonstration of physical qubits realization are carried out, which can be scaled up to larger systems. A confirmation of this is the successive announcement of IBM 20, 50 and 53 qubits quantum computers [26,27].

Second, likely transition to post-quantum cryptography will not be easy, because it is unlikely to be a simple replacement of the current asymmetric cryptographic primitives standards. Significant efforts will be needed to develop, standardize and implement a new post-quantum cryptosystems. Therefore, should be a significant transition stage, when as current and post-quantum cryptographic primitives are used.

Applications were received by NIST until November 30, 2017. They relate to: asymmetric encryption algorithms and ES. Subsequently, their detailed analysis and comparison is expected, with a period of up to 3 years. This indicates the significant complexity of the problem to be solved.

The European Union has also started the preparation of a new post-quantum standards. A new direction "Quantum-Safe Cryptography" are formed by European Organization for Standardization

ETSI in the cluster "Security" [1,4,7]. According to the results of these studies are predicted the groups standards for post-quantum period adoption. ETSI has published a group report "Quantum-Safe Cryptography. Quantum-Secure infrastructure" [1], in which fixed bases of perspective infrastructure, provided algorithms, described primitives types, that will be used. Separately requirements are nominated and estimation criteria are formed for future candidates.

With the participation of the authors of this article for the NIST USA competition, a cryptographic algorithm for NTRU Prime IIT Ukraine [10], developed using NTRU [8] and NTRU Prime [9], was presented. The objective of this paper is a general overview and description of the proposed cryptographic transformation, implementation specificity, estimation and comparison of the main characteristics and indicators from [8-10] according to cryptographic stability criteria from existing and potentially possible attacks.

2 Problem formulation

On the basis of the analysis of a number of sources [8, 9] concerning the existing encryption algorithms, their features, advantages and disadvantages, as well as resistance to attacks, it was determined that on their basis it is possible to create a new encryption algorithm, which will combine the main advantages of existing ones and will not have certain disadvantages. As a result of extensive research, the essence of the candidate was substantiated, its implementations, wich has the advantages of relatively well-known were developed, made tests and estimations of the main characteristics. In November 2017 a full set of project descriptions and program implementations were sent and received by NIST USA [5]. It is considered necessary to consider the article as the first stage of the preliminary study of our proposal and to familiarize the general public with the problem of creating a post-quantum standard of asymmetric encryption. Thus, the objective of this paper is to justify and outline the main ideas for constructing a post-quantum standard of asymmetric encryption, to analyze the state of work in the indicated direction, to indicate the essence of the difference between the «NTRU Prime IIT Ukraine» proposal and known ones, and to discuss the results of the estimation and testing in relation to requirements imposed by NIST USA.

An analysis of the requirements for post-quantum cryptographic transformations of asymmetric encryption allows us to conclude that the main, and unconditional requirement for «NTRU Prime IIT Ukraine», is the requirement of cryptographic stability regarding known and potentially possible attacks. The specified attacks can be implemented using both classical attacks based on the use of classical computer systems and classical mathematical methods, as well as on the basis of quantum computers and corresponding mathematical and software methods.

Obviously, that cryptographic asymmetric transformations should provide protection from both classical and quantum cryptanalysis methods. The above should be taken into account, if possible, during the construction and analysis of post-quantum cryptographic transformations in general, and the adoption of post-quantum standards of asymmetric cryptographic transformations on their basis.

3 Description and analysis of general parameters of modern NTRU-like encryption algorithms

Let's consider the existing today encryption algorithms and created on their basis a new encryption algorithm «NTRU Prime IIT Ukraine» [8-10].

Analysis of NTRU encryption algorithm. NTRU – the first public key cryptosystem not based on factorization or discrete logarithmic problem. NTRU is based on the shortest vector problem in a lattice. Operations are based on objects in a truncated polynomial ring $R = \mathbf{Z}[x]/(x^n - 1)$, polynomial degree at most $n-1$.

NTRU parameters are as follows: n – the polynomials in the ring R have degree $n-1$ (non-secret); q – the large modulus to which each coefficient is reduced (non-secret); p – the small modulus to which each coefficient is reduced (non-secret); f – a polynomial that is the private key; g – a polynomial that is used to generate the public key h from f (secret but discarded after ini-

tial use); h – the public key, also a polynomial; r – the random "blinding" polynomial (secret but discarded after initial use); d – coefficient.

The encryption of message m is carried out according to the formula $c = rh + m$.

Decryption is performed as follows: using a private polynomial f it is calculated polynomial $a = f \cdot e (\mathrm{mod}\, q)$. Then the polynomial $b = a \bmod p$ is calculated. Another private polynomial f_p is used to compute $c = f_p \cdot b (\mathrm{mod}\, p)$, where c is an output message m.

More details about the NTRU algorithm is described in [8].

4 Analysis of NTRU Prime encryption algorithm

The NTRU Prime cryptosystem is proposed as one of the alternative variants of the asymmetric NTRU method in order to get rid of the weaknesses inherent in NTRU, which are associated with undesirable structural properties of the ring $\mathbf{Z}_q[x]/(x^n - 1)$: in many cases, a ring of this type has a subrings and a factor-rings of a high order. Unlike NTRU, NTRU Prime uses a ring $\mathbf{Z}_q[x]/(x^n - x - 1)$, which provided that the proper selection of numbers q and n, is a field, that does not contain its own subfields. In addition, the Galois group of polynomial $x^n - x - 1$ over the field Q is a symmetric group S_n, which excludes the possibility of attacking a certain type on the cryptosystem.

In NTRU Prime, the public key is calculated by the formula $h = g/3f$ that it matters to create an effective secret key transfer protocol. However, to construct an asymmetric encryption system, it is desirable to use the traditional formula $h = 3g/f$.

The decryption of messages in the cryptosystem NTRU Prime occurs correctly on condition $q > 48t$.

Details about the NTRU Prime algorithm is described in [9].

5 Analysis of NTRU Prime IIT Ukraine encryption algorithm

The given asymmetric encryption scheme is a modification of the NTRU scheme, and differs from the latter only in two aspects:

1. Instead of the ring $\mathbf{Z}_q[x]/(x^n - 1)$ used in NTRU, a field $\mathbf{Z}_q[x]/(x^n - x - 1)$ is used, as in the NTRU Prime cryptosystem [9]. According to [9], this prevents cryptosystem attacks of some kind and precludes the use of (at least potentially) weaknesses of the standard NTRU cryptosystem that are associated with the existence of non-trivial subrings or truncated rings of ring $\mathbf{Z}_q[x]/(x^n - 1)$.

2. In the proposed scheme, polynomials F and r are arbitrary t-small, that is, they have $2t$ non-zero coefficients equal to ± 1, whereas in [8] each of these polynomials has exactly t nonzero coefficients equal to 1 and -1 correspondingly. A similar remark is also valid for a polynomial g, which is an arbitrary small polynomial in a modified cryptosystem and has the same number of non-zero coefficients, which are equal 1 and -1 in NTRU. This difference is not significant, however, it provides the opportunity to expand the amount of key space in comparison with NTRU without losing the effectiveness of algorithms implementation for key generation and messages encryption-decryption.

In this algorithm, the secret key is any pair of polynomials (f, g), where $f = (1 + 3F) \bmod q$, $F, g \in R/3$, $\| F \|_1 = 2t$, and the corresponding public key is a polynomial $h = 3g/f \in R/q$.

Encryption of the message m is carried out according to the formula $c = m + rh$, where r – the random equal probability t-small polynomial, h – public key, and the addition and multiplication are carried out in the field R/q.

To retrieve a message m by message c using a secret key (f,g), we must calculate $m' = (cf \pmod q) \bmod 3$ and put $m'' = (m' f^*) \bmod 3$. That is, only polynomials f and f^* are used to decrypt messages, where f^* there is an inverse to an element $f \bmod 3$ in the ring $R/3$.

In «NTRU Prime IIT Ukraine» using the appropriate estimates as specified in the description of the algorithm, can (it is allowed) to significantly weaken the condition for decryption of messages in comparison with NTRU Prime, namely, to replace it with a condition $q > 32t$. This, in turn, allows you to reduce the value q compared to NTRU Prime, while maintaining the decryption correct. More details about the «NTRU Prime IIT Ukraine» algorithm is described in [10].

6 Analysis of algorithm taking into account known attacks on «NTRU Prime IIT Ukraine»

Let's analyze the stability of the encryption algorithm «NTRU Prime IIT Ukraine» [10] for known attacks.

Meet-in-the-middle

It should be noted that this attack is currently being implemented on ordinary computers, but without language, it is possible to implement it on quantum computers.

The task of recovery the secret key $(f = (1+3F) \bmod q, g)$ by the public key h of the cryptosystem is reduced to solving the equation $(h' + Fh') \bmod q = g$ for unknown $F, g \in R/3$, where $\| f \|_1 = 2t$ and $h' = (3^{-1} h) \bmod q$. This problem can be formulated in such way.

Let $\Phi = \{F \in R : \| F \|_\infty = 1, \| F \|_1 = 2t\}$. We must find a polynomial $F \in \Phi$ such that

$$\| (h' + h'F) \bmod q \|_\infty = 1. \quad (1)$$

The complexity of solving the task by enumeration of all polynomials $F \in \Phi$ requires $|\Phi| = 4^t \binom{n}{2t}$ operations. To reduce the complexity you can apply attacks under the general name «meet in the middle». We describe the general scheme of conducting such attacks, based on the ideas of works [11,13,14].

We assign sets $\Phi_1, \Phi_2 \subseteq \mathbf{Z}^n$ such that each vector $F \in \Phi$ has a single representation in the form $F = F_1 + F_2$, where $F_1 \in \Phi_1$, $F_2 \in \Phi_2$, and a certain mapping $D : Z_q{}^n \to \{0,1\}^r$, where $r \le n$.

The algorithm for solving the equation (1) relative to the unknown $F \in \Phi$ consists of two stages, on the first of which the table is built, which consists of all pairs $(h'F_1 (\bmod q), D(h'F_1 (\bmod q)))$, located by non-growing integers corresponding to binary vectors $D(h'F_1 (\bmod q))$, where $F_1 \in \Phi_1$. Then, on the second stage, for each $F_2 \in \Phi_2$, the vector $D(-h' - h'F_2 (\bmod q))$ is searched for among the other pairs components that are in constructed table. The algorithm completes successfully in case of finding vectors $F_1 \in \Phi_1$, $F_2 \in \Phi_2$ such that $D(h'F_1 (\bmod q)) = D(-h' - h'F_2 (\bmod q))$ and $\| (h' + h'(F_1 + F_2)) \bmod q \|_\infty = 1$.

Note that in [9,11,13,14], for various variants of the NTRU cryptosystem, heuristic complexity estimates of meet in the middle attacks are presented based on explicit or implicit assumptions regarding the mapping D and distribution of vectors in a table, that is constructed on the first stage. Along with that, regardless of mapping D choice, the maximum complexity of the described algorithm is limited below by the value $|\Phi_1| + |\Phi_2| \ge 2\sqrt{|\Phi_1||\Phi_2|}$, which, in its turn, is at leas

$$\text{t } 2\sqrt{|\Phi|} = 2^{t+1} \binom{n}{2t}^{1/2}.$$

Thus, in order to ensure the resistance of cryptosystem «NTRU Prime IIT Ukraine», according to the meet-in-the-middle attacks, values n and t are selected for the given security parameter k, based on the condition

$$2^k \le 2^{t+1}\binom{n}{2t}^{1/2}. \quad (2)$$

Let's consider later the attacks in terms of their stability in the application of quantum algorithms [8, 20-24], and first consider the attack “meet-in-the-middle”.

Let B – the set of Boolean polynomials of degree N. Also let $B(d)$ – B subset, whose polynomial has d coefficients 1, and $N-d$ coefficients 0. $T(d+,d-)$ – the set of polynomials, where the number of coefficients 1 equals $d+$, and the number of coefficients –1 is equal $d-$, and the others are 0.

The “meeting-in-the-middle” attack allows cryptanalyst under certain conditions to calculate the user private key that is selected from space of 2^N elements in time $O\left(2^{N/2}\right)$. The proposed attack is implemented as follows [9]. The private keys space ($f=(1+pF) mod\ q$) f is divided into two large parts $f_1 \| f_2$, where f_1 and f_2 have a length $N/2$ of $d/2$ units each, whereby the same number of units is achieved by cyclic shift f when dividing into two parts. Under this condition, based on ($h = p(f_q^{-1} * g)\ mod\ q$), when $p = 2$, the condition is fulfilled:

$$f \cdot h = g (\mathrm{mod}\, q). \quad (3)$$

Substituting instead of f its representation in the form $f_1 \| f_2$ we have that

$$(f_1 \| f_2) \cdot h = g (\mathrm{mod}\, q). \quad (4)$$

Comparison (4) can be presented in the form

$$f_1 \cdot h = g - f_2 \cdot h (\mathrm{mod}\, q). \quad (5)$$

Finally, (5) can be presented in the form

$$(f_1 \cdot h)_i = \{1,0\} - (f_2 \cdot h)_i (\mathrm{mod}\, q) \forall i. \quad (6)$$

In fact for f the condition that half of the units fall into the first $N/2$ records can not be fulfilled. As shown in [23], there is at least one torsion f that will satisfy this property, and as a private key there will be any torsion f.

Under these conditions, the attack consists of the following steps.

1. A number k is determined that satisfies the condition

$$2^k \ge \binom{N/2}{d/2}. \quad (7)$$

Next, the memory is allocated to 2^k baskets for storing polynomials. Then the larger k will be chosen, than the faster the algorithm will run, but more memory will be required.

2. $N/2$ zeros are added to the polynomial f_1 and their selection is carried out. Browsing will take $\binom{N/2}{d/2}$ steps. Each value f_1 is written to the basket in such way that the number of the basket to which the polynomial will be placed is equal to the most significant bits of the first k coeffi-

cients $f \cdot h = g(\mathrm{mod}\, q)$. We will mark each basket as $label\_f_1$. In this case, in some baskets there will be several values of the polynomials.

3. Then the polynomials f_2 are sorted in the same way and the baskets $label\_f_2$ are formed, but zero bits are added to the beginning. The formed polynomial is placed in baskets whose number is formed as follows – the most significant bits for the first k polynomial coefficients $-f_2 * h(\mathrm{mod}\, q)$, as well as the most significant bits for the first k polynomial coefficients $-f_2 * h(\mathrm{mod}\, q)$ to each coefficient of which is added 1.

4. In the case if in the record f_2 a polynomial f_1 contains in the basket, it is considered a good candidate for recovery f. The cryptanalyst calculates $(f_1 \| f_2) \cdot h = g(\mathrm{mod}\, q)$. If it consists of $\{0,1\}$, then the private key is found.

Thus, in an attack with the use of the method "meet-in-the-middle" type it is established that this algorithm can always return the result, which is most likely a private key f, or a cyclic shift f.

According to [25], the temporal and spatial complexity of the "meet-in-the-middle" attack can be estimated as

$$O(\frac{C_{N/2}^{d/2}}{\sqrt{N}}). \tag{8}$$

In general, (8) allows you to estimate the complexity of temporal and spatial attack on the algorithm NTRU. The above ratio can be used to compare the complexity of the "full disclosure" attack with attacks based on quantum algorithms.

Attack on the lattices

We note that this type of attack is implemented on ordinary computers, but in the future it can be implemented on quantum computers.

For any $h \in R/q$ we denote $L(h)$ the lattice in the vector space R^{2n+1} generated by the rows of the matrix

$$\begin{pmatrix} 1 & 0_{1\times n} & h' \\ 0_{n\times 1} & I_n & H \\ 0_{n\times 1} & 0_{n\times 1} & qI_n \end{pmatrix}, \tag{9}$$

where I_n – the unit matrix of order n, H – $n\times n$ matrix, whose i-th row is equal to the vector of polynomial coefficients $(x^i h) \bmod (x^n - x - 1)$, $i \in \overline{0, n-1}$, $h' = (3^{-1} h) \bmod q$, 3^{-1} – the of ring R/q element, reversed to 3:

$$3^{-1} = (5+q)/6, \text{ if } q \equiv 1 \bmod 3; \quad 3^{-1} = (5-q)/6, \text{ if } q \equiv -1 \bmod 3.$$

The following statement refines on (for the case of considered cryptosystem) the main result of work [15].

Statement 1. If the vector $(f = (1+3F) \bmod q, g)$ is the cryptosystem secret key, which corresponds to the public key h, then

$$(1, F, g) \in L(h) \tag{10}$$

and

$$\| (F, g) \|_2 = \left(\sum_{i=0}^{n-1} |F_i|^2 + \sum_{i=0}^{n-1} |g_i|^2 \right)^{1/2} \le \sqrt{n+2t}. \tag{11}$$

On the other hand, if the vector (F, g) satisfies (10) and has a length

$$\| (F,g) \|_2 < \frac{q-2}{12(\sqrt{n}+\sqrt{2t})}, \quad (12)$$

then with the help of the vector $f = (1+3F) \bmod q$ you can recovery any input message m by cryptogram $c = E_h(m,r)$, supposing that $m = (cf \,(\bmod q)) \bmod 3$.

Proof. The first part of the statement follows directly from the above definitions.

To prove the second part we consider the cryptogram $c = (m+rh) \bmod q$ received as a result of converting an input message $m \in R/3$ using the public key h and t-small polynomial r.

Based on condition (10), the equality $(3g) \bmod q = (fh) \bmod q$ is valid. Note that $f \neq 0$, because otherwise $F = 3^{-1}$, $g = 0$ $\| (F,g) \|_2 \geq \frac{q-5}{6} > \frac{q-2}{12(\sqrt{n}+\sqrt{2t})}$, because $q > 48$, which contradicts the condition (12).

Using the estimate ($\| uv \|_\infty \leq 2 \| u \|_\infty \| v \|_1$) and formula (12), we obtain that

$$\| mf + 3rg \|_\infty \leq \| m \|_\infty + 3(\| mF \|_\infty + \| rg \|_\infty) \leq 1 + 6(\| m \|_2 \| F \|_2 + \| g \|_2 \| r \|_2) \leq$$

$$\leq 1 + 6(\| m \|_2 + \| r \|_2) \| (F,g) \|_2 \leq 1 + 6(\sqrt{n}+\sqrt{2t}) \| (F,g) \|_2 < q/2.$$

It follows that $(cf) \bmod q = (mf + 3rg) \bmod q = mf + 3rg$, and therefore,

$$(cf \,(\bmod q)) \bmod 3 = (mf + 3rg) \bmod 3 = (m(1+3F)) \bmod 3 = m.$$

The statement is proven.

Thus, the task of recovery the cryptosystem secret key by its public key h is reduced to find a sufficiently short vector (with the first coordinate equal to one) in the lattice $L(h)$. Taking the usual heuristic assumption that the desired vector is the shortest non-zero vector of the lattice $L(h)$, we conclude that the secret key recovery is equivalent to solving the problem of the shortest vector problem (SVP) for this lattice. Note that the latter problem is equivalent to finding vector which is closest to the vector $(0_{1\times n}, h')$ in the lattice generated by the rows of the matrix $\begin{pmatrix} I_n & H \\ 0_{n\times 1} & qI_n \end{pmatrix}$ (closest vector problem (CVP)).

The inverse of a function E_h task or, equivalently, the recovery of the input message $m \in R/3$ by the output cryptogram $c = (m+rh) \bmod q$, where $r \in R/3$, $\| r \|_1 = 2t$, also reduces to the search for the shortest (or short enough) vector of the lattice $L(h,c)$ generated by the rows of the matrix

$$\begin{pmatrix} 1 & 0_{1\times n} & c \\ 0_{n\times 1} & I_n & H \\ 0_{n\times 1} & 0_{n\times 1} & qI_n \end{pmatrix}.$$

Both lattices $L(h)$, $L(h,c)$ have the same form and belong to the class of modular lattices.

Hybrid attack

It should be noted that this attack is now implemented on ordinary computers, but it is also possible to implement it in the future and on quantum ones.

A hybrid attack on the classic NTRU cryptosystem was proposed in [13] and was subsequently researched in many publications. A certain result of these studies is the work [16], which shows that the complexity estimates of the hybrid attack received earlier for different cryptosystems are very inaccurate due to false assumptions and questionable heuristic considerations, that are used to obtain these estimates.

Note that certain heuristic assumptions are also used in [16], so the question of well-grounded estimates of the hybrid attack complexity is the subject of further researches.

In relation to the cryptosystem under consideration, a hybrid attack is carried out in this way [16].

Consider the lattice $L(h)$ generated by the rows of the matrix (9), fix the number $r \in \overline{1, n-1}$ and write the matrix H in the form $H = \begin{pmatrix} H_1 \\ H_2 \end{pmatrix}$, where H_1 and H_2 are integer matrixes of size $r \times n$ and $(n-r) \times n$, respectively. An arbitrary vector $F \in Z^n$ will be written in the form $F = (F_1, F_2)$, where $F_1 \in Z^r$, $F_2 \in Z^{n-r}$.

Note that the vector $(1, F, g)$ belongs to the lattice $L(h)$ if and only if there is a vector $x \in Z^n$ such that

$$F_1(0_{r\times 1}, 0_{r\times(n-r)}, H_1) = -(1, F_2, x)\begin{pmatrix} 1 & 0_{1\times(n-r)} & h' \\ 0_{(n-r)\times 1} & I_{n-r} & H_2 \\ 0_{n\times 1} & 0_{n\times(n-r)} & qI_n \end{pmatrix} + (1, F_2, g). \quad (13)$$

The last equality is equivalent to the vector $F_1(0_{r\times 1}, 0_{r\times(n-r)}, H_1) - (1, F_2, g)$ that belongs to a lattice $L_r(h)$ generated by the rows of the matrix

$$\begin{pmatrix} 1 & 0_{1\times(n-r)} & h' \\ 0_{(n-r)\times 1} & I_{n-r} & H_2 \\ 0_{n\times 1} & 0_{n\times(n-r)} & qI_n \end{pmatrix}.$$

According to [16], a hybrid attack depends on the parameters r, l, c_{-1}, c_1 and is aimed to finding a vector $(1, F_1, F_2, g) \in L(h)$ that satisfies the following conditions:

(a) F_1 is a small vector that has precisely $2c_{-1}$ coordinates equal to -1, and $2c_1$ coordinates, that equal to 1;

(b) (F_2, g) is a small vector, that has an Euclidean norm l.

The attack consists of two stages, on the first – a reduced lattice $L_r(h)$ basis B constructed in one way or another. Next, on the second stage, vectors of F_1, that satisfy the condition (a), by which vectors $(\nu, F_2, g) = \mathrm{NP}_B(\hat{F}_1)$ are calculated, where $\nu \in Z$ and $\mathrm{NP}_B(\hat{F}_1)$ is a result of Babai algorithm application to the vector $\hat{F}_1 = F_1(0_{r\times 1}, 0_{r\times(n-r)}, H_1)$ and basis B of the lattice $L_r(h)$. Mentioned algorithm finds a "sufficiently short" vector $e = \mathrm{NP}_B(\hat{F}_1)$ for which $\hat{F}_1 - e \in L$, provided that the basis B is "sufficiently well" reduced [17].

From equation (13) and condition (b) it follows that the vector $\hat{F}_1$ is close to the lattice $L_r(h)$, so it is natural to look for the nearest to it vector of this lattice in the form $\hat{F}_1 - \mathrm{NP}_B(\hat{F}_1)$. In addition, on the basis of equality (13), for any $F_1 \in Z^r$ vector $(1, F_1, F_2, g)$ belongs to lattice $L(g)$, if $\mathrm{NP}_B(\hat{F}_1) = (1, F_2, g)$. Therefore, all that remains to be checked for a vector $\mathrm{NP}_B(\hat{F}_1)$ on the second stage of an attack is equality $\nu = 1$ and condition (b).

In order to speed up the search for vectors in the second stage, the method of meet in the middle is used: instead of the vectors F_1 satisfying condition (a), small vectors f_1 of length r, each of which have exactly c_{-1} coordinates, that are equal to -1, and c_1 the coordinates, that are equal to 1, are sorted. Each vector f_1 is stored in a hash table with addresses of a certain set $A(f_1)$, which de-

pends only on the vector $\mathrm{NP}_B(\hat{f}_1)$, where $\hat{f}_1 = f_1(0_{r\times 1}, 0_{r\times(n-r)}, H_1)$, and consists of some binary vectors of length $2n-r+1$. The set of addresses is constructed so, that $A(f_1') \cap A(f_1'') \neq \varnothing$ if the difference between vectors $\mathrm{NP}_B(\hat{f}_1')$ and $\mathrm{NP}_B(\hat{f}_1'')$ is a small vector.

Each time when in the search process it is performed repeatedly to the table at the same address, that is, for some vectors f_1', f_1'' that are enumerated, the condition $A(f_1') \cap A(f_1'') \neq \varnothing$ is fulfilled, the vector (F_1, F_2, g) is calculated, where $F_1 = f_1' + f_1''$, $(\nu, F_2, g) = \mathrm{NP}_B(\hat{f}_1') + \mathrm{NP}_B(\hat{f}_1'')$ for which the conditions (a) and (b) and equality $\nu = 1$ are verified. Therefore, the attack ends successfully, if there is a pair of small vectors f_1', f_1'' satisfying the following conditions:

(a′) each of the vectors f_1', f_1'' has exactly c_{-1} coordinates equal to -1, and c_1 coordinates that are equal to 1;

(b′) the vector $F_1 = f_1' + f_1''$ satisfies the condition (a);

(c′) vector $\mathrm{NP}_B(\hat{F}_1)$ equals to $\mathrm{NP}_B(\hat{f}_1') + \mathrm{NP}_B(\hat{f}_1'')$, has the first coordinate $\nu = 1$ and satisfies the condition (b).

In [16] using heuristic considerations, the formula for the described second stage attack complexity is obtained:

$$T_2(\delta, r) = \frac{2^{15} r!}{c_{-1}! c_1! (r - c_{-1} - c_1)!} \left(\binom{2c_{-1}}{c_{-1}} \binom{2c_1}{c_1} p\,|S| \right)^{-1/2} \frac{1}{\tilde{p}}, \tag{14}$$

where

$$p = \prod_{i=1}^{2n-r+1} \left(1 - \frac{1}{r_i B\left(\frac{2n-r}{2}, \frac{1}{2}\right)} \int_{-r_i-1}^{-r_i} \int_{\max\{-1, z-r_i\}}^{z+r_i} (1-t^2)^{\frac{2n-r-2}{2}} dt dz \right), \tag{15}$$

$$|S| = 2 + 2(n-t-1) p_S, \tag{16}$$

$$p_S = \frac{p_{\mathrm{NP}} 2^{-4c_1} r!}{(2c_{-1})!(2c_1)!(r - 2c_{-1} - 2c_1)!} \binom{n-r}{4t-4c_1} \binom{n}{2t}^{-1}, \tag{17}$$

$$p_{\mathrm{NP}} = \prod_{i=1}^{2n-r+1} \left(1 - \frac{2}{r_i B\left(\frac{2n-r}{2}, \frac{1}{2}\right)} \int_{-1}^{\max\{-r_i, -1\}} (1-t^2)^{\frac{2n-r-2}{2}} dt \right), \tag{18}$$

$$\tilde{p} = 1 - (1 - p_S)^{n-t}. \tag{19}$$

In formulas (15), (18) $B(\cdot,\cdot)$ denotes the Euler beta-function, and the numbers r_i are determined by the formulas

$$r_i = \frac{R_i(\delta)}{2l},\ i \in \overline{1, 2n-r+1}, \tag{20}$$

where

$$R_i(\delta) = q, \text{ if } 1 \le i \le 2n - r + 1 - \mu;$$

$$R_i(\delta) = q^{-2(i-(2n-r+1-\mu)-1)+\mu} q^{\frac{\mu-(n-r)}{\mu}}, \text{ if } 2n-r+1-\mu < i \le 2n-r+1,$$

$$\mu = \min\left\{2n-r+1, \left\lfloor \sqrt{\frac{n-r}{\log_q \delta}} \right\rfloor\right\},\ \delta > 1.$$

It is recommended to use the following parameter values:

$$|c_{-1}| = |c_1| = \left\lceil \frac{rt}{2n} \right\rceil,\ l = \sqrt{\frac{2n}{3} + \frac{2t(n-r)}{n}}. \tag{21}$$

To estimate the first stage of a hybrid attack (the construction of a reduced basis B of lattice L), a traditional approach is used [18]. It is believed that the basis B is constructed using the Korkin-Zolotarev block algorithm: BKZ 2.0 [19] (which is considered to be one of the best algorithms for solving similar problems nowadays). The BKZ 2.0 algorithm depends on the natural parameters β and m, which denote the so-called *block length* and the *number of iterations* respectively, and allows to build the reduced Korkin-Zolotarev basis of a complete lattice of dimension $2n-r+1$ by $2^{E(\beta,m,2n-r+1)}$ operations, where

$$E(\beta, m, 2n-r+1) = 0{,}000784314\beta^2 + 0{,}366078\beta + \log((2n-r+1)m) + 0{,}875 \tag{22}$$

(note that formula (22) is an empirical estimate based on the results of computational experiments [18]).

The degree of the reduced basis quality, which is built using the algorithm, is the so-called root Hermite factor: the number $\delta > 1$ determined by the formula

$$\| b_1 \|_2 = \delta^{2n-r+1} \left(\det L(H_2, h)\right)^{\frac{1}{2n-r+1}} = \delta^{2n-r+1} q^{\frac{n}{2n-r+1}},$$

where b_1 is the shortest vector in the built basis. [19] describes the BKZ 2.0 algorithm simulator, which allows to calculate such values β and m by the input parameter $\delta > 1$, that application of the BKZ 2.0 with these parameters to any input basis of the full lattice of the dimension $2n-r+1$ leads to its reduced basis with the root factor of Hermite δ.

The complexity $T_1(\delta, r)$ calculation of the hybrid attack first stage is carried out as follows:

1) using BKZ 2.0 algorithm simulator [19], find β and m by the input data $2n-r+1$ and δ;
2) put

$$T_1(\delta, r) = 2^{E(\beta,m,2n-r+1)}, \tag{23}$$

where $E(\beta, m, 2n-r+1)$ is determined by the formula (22).

The total complexity of the hybrid attack is calculated by the formula

$$T(\delta, r) = T_1(\delta, r) + T_2(\delta, r); \tag{24}$$

with this estimation of the cryptosystem stability in relation to this attack is the number $T_{\min} = \min\{T(\delta, r) : \delta > 1, r \in \overline{1, n-1}\}$.

According to [16], to calculate the value $T_{\min}$, $\delta_r > 1$ should be found for each $r \in \overline{1, n-1}$ so that $T(\delta_r, r) = \min\{T(\delta, r) : \delta > 1\}$ and set $T_{\min} = \min\{T(\delta_r, r) : r \in \overline{1, n-1}\}$. To find δ_r it can be applied an iterative algorithm (dichotomy) as $T_1(\delta, r)$ is decreasing, and $T_2(\delta, r)$ − an increasing function

of the parameter $\delta > 1$: the desired value δ_r is approximately equal to the equation root $T_1(\delta, r) = T_2(\delta, r)$.

Thus, using the formulas (14), (23), (24), we can estimate the resistance of the considered cryptosystem in relation to the hybrid attack. To ensure resistance at the k-th level it is sufficient to fulfill the condition

$$2^k \le T_{\min}. \tag{25}$$

Sieving methods

Such attacks today are realized on ordinary computers, but in the future they may be implemented on quantum computers.

In recent years, a number of algorithms for solving SVP and CVP problems with sieving methods have been proposed. The most effective of known algorithms have heuristic complexity $(3/2)^{N/2+o(1)}$ with $N \to \infty$, where N – the dimension of the lattice, with the residual term $o(1)$ that is positive [20, 21]. Since in our case $N = 2n+1$, to ensure the resistance of the cryptosystem relative to the attacks based on the sieving methods, it is sufficient to fulfill the condition

$$2^k \le (3/2)^n. \tag{26}$$

7 Conclusions

1. An analysis of the requirements for post-quantum cryptographic transformations of asymmetric encryption allows us to conclude that the basic, and unconditional requirement for cryptographic transformation «NTRU Prime IIT Ukraine», is the requirement of cryptographic stability regarding known and potentially possible attacks. These attacks can be implemented using classical attacks based on the use of classical computer systems and classical mathematical methods, as well as on the basis of quantum computers and corresponding mathematical and programmatic methods.
2. Obviously, cryptographic asymmetric transformations should provide protection from both classical and quantum methods of cryptanalysis. The above should be taken into account, if possible, in the construction and analysis of general-type post-quantum transformations, and the adoption of their post-quantum standards of asymmetric cryptographic transformations.
3. In the cryptosystem «NTRU Prime IIT Ukraine» as the main cryptographic transformation, as in NTRU Prime, unlike NTRU, the transformation is used in the finite field. The above makes it impossible to conduct a series of potential attacks regarding the cryptographic system «NTRU Prime IIT Ukraine» and eliminates the potential weaknesses present in the NTRU cryptosystem. They are mainly related to the existence of non-trivial subfields or factor rings of the factor (truncated) polynomials ring.
4. In the cryptosystem «NTRU Prime IIT Ukraine» polynomials F and r are arbitrary t-small, they have $2t$ non-zero coefficients (+1, −1), whereas in NTRU, each of these polynomials has exactly t nonzero coefficients equal to 1 and −1 respectively. The same is true for the polynomial g used in the cryptosystem «NTRU Prime IIT Ukraine», which is an arbitrary small polynomial with $2t$ nonzero coefficients (+1, −1). Specified allows to expand the size of the key space in comparison with NTRU without losing the efficiency of algorithms implementation for the keys formation and implementation of encryption and decryption algorithms.
5. To ensure the stability of the cryptosystem relative to the attack with a known open message, which is based on the overview of the vectors $b \in \{0,1\}^{l_2}$, the value l_2 (taking into account the quantum algorithms of overview) should be at least $2k$, where k – the security parameter. In this case, the length of the initial state of the gamma generator used to obtain the vector b must be at least $2k + 64$ bits.

6. For the «NTRU Prime IIT Ukraine» cryptosystem, the most effective of known potential attacks, it is necessary to justify the choice of parameters n, t,and q depending on the security parameter k. It is necessary to ensure that the following conditions are met:
   a) choose a simple number n in such a way that it satisfies the inequality (26);
   b) for a given n choice, if it exists, a natural t, that satisfies the inequalities (2);
   c) for the given n and t choose a prime $q \geq 48t+3$ such, that the polynomial $x^n - x - 1$ was irreducible over the field $\mathbf{Z}_q$, and the condition (25) was fulfilled.
7. An adequate condition for the cryptographic stability of the «NTRU Prime IIT Ukraine» cryptographic transformation with the given three parameters (n,t,q) is the unconditional fulfillment of the condition (25).

References

[1] ETSI GR QSC 001 V.1.1.1 (2016-07). Quntum-Safe Cryptography (QSC); Quantum-safe algorithmic framework. [Electronic resource]. – Access mode: https://portal.etsi.org/webapp/workProgram/Report_WorkItem.asp?wki_id =46690.

[2] Koblitz Neal A riddle wrapped in an enigma / Neal Koblitz, Alfred J. Menezes // – Access mode: https://eprint.iacr.org/2015/1018.pdf.

[3] Lily Chen Report on Post-Quatum Cryptography. NISTIR 8105 (DRAFT) / Lili Chen, Stephen Jordan, Yi-Kai-Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone // – Access mode: http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf.

[4] Mosca M. "Setting the Scene for the ETSI Quantum-safe Cryptography Workshop" / M. Mosca // E-proceedings of "1st Quantum-Safe-Crypto Workshop", Sophia Antipolis, Sep 26-27, 2013. – Access mode: http://docbox.etsi.org/Workshop/2013/201309_CRYPTO/eproceedings_Crypto_2013.pdf.

[5] Post-quantum crypto project. [Electronic resource]. – Access mode: http://csrc.nist.gov/groups/ST/post-quantum-crypto/index.html.

[6] Proposed Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process. [Electronic resource]. – Access mode: http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/call-for-proposals-draft-aug-2016.pdf.

[7] Quantum Safe Cryptography and Security. An introduction, benefits, enablers and challenges Access mode: http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf.

[8] American National Standard for Financial Services – Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry – ANSI X9.98–2010, 2010. – 284 p.

[9] Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, Christine van Vredendaal: NTRU Prime. – Access mode: https://ntruprime.cr.yp.to/ntruprime-20160511.pdf.

[10] Kachko O. G. The optimization of NTRU-like algorithm for asymmetric encryption with "inconvenient parameters" / O. G. Kachko, L. V Makutonina, O. S. Akolzina //. Mathematical and computer modeling. Series: Engineering, 15 (2017), 79–85. (in Ukrainian)

[11] Hoffstein J. NTRU: a ring based public key cryptosystem / J. Hoffstein, J. Pipher, J. H. Silverman // Algorithmic Number Theory, Third International Symposium, Portland, Oregon, USA, June 21 – 25, 1998. – Proceedings. – Springer, 1998. – P. 267–288.

[12] Campbell P., Groves M., Shepherd D. SOLYLOQUI: a cautionary tale, 2014. – Access mode: http:docbox.etsi.org /Workshop/2014/201410_CRYPTO/S07_Systams_and_Ayyacks/S07_Groves_Annex.pdf.

[13] Howgrave-Graham N. A hibrid lattice-reduction and the meet-in-the-midle attack against NTRU / N. Howgrave-Graham // Advances in Cryptology – CRYPTO 2007. – Proceedings. – Springer-Verlag. – 2007. – P. 150–169.

[14] Howgrave-Graham N. A meet-in-the-midle attack on an NTRU private key / N. Howgrave-Graham, J. H. Silverman, W. Whyte // Technical report, NTRUCryptosystems, June 2003. Report, 2003.

[15] Coppersmith D. Lattice attack on NTRU / D. Coppersmith, A. Shamir // Advances in Cryptology – EUROCRYPT'97. – Proceedings. – Springer-Verlag. – 1997. – P. 52–61.

[16] Wunderer Th. Revising the hibrid attack: improved analysis and refined security estimates. – Access mode: http://eprint.iacr.org /2016/733.

[17] Babai L. On Lova′sz′ lattice reduction and the nearest lattice point problem / L. Babai // Combinatorica. – 1986. – Vol. 5. – № 6(11). – P. 1–13.

[18] Hoffstein J., Pipher J., Schanck J.M., Silverman J.H., Whyte W., Zhang Z. Choosing parameters for NTRUEncrypt. – Access mode: http://eprint.iacr.org/2015/708.

[19] Chen Y. BKZ 2.0: better lattice security estimates / Y. Chen, P.Q. Nguyen // Advances in Cryptology – ASIACRYPT 2011. – Proceedings. – Springer-Verlag. – 2011. – P. 1–20.

[20] Gorbenko Yu. I. Special'na tema / Yu. I. Gorbenko, R. S. Ganzja // Zbirnyk naukovyh prac', vyp.2(22) Special'ni telekomunikacijni systemy ta zahyst informacii', prym.№59 DSSZZI Ukrai'ny. – S. 17–26.

[21] Gorbenko Yu. I. Analiz stijkosti populjarnyh kryptosystem proty kvantovogo kryptoanalizu na osnovi algorytmu Grovera / Yu. I. Gorbenko, R. S. Ganzja // Zahyst informacii': Naukovo-praktychnyj zhurnal, 2014. – Tom 16, №2. – S. 106–112.

[22] Gorbenko Yu. I. Analiz shljahiv rozvytku kryptografii' pislja pojavy kvantovyh komp'juteriv / Ju. I. Gorbenko, R. S. Ganzja // Visnyk Nacional'nogo universytetu «L'vivs'ka Politehnika». Serija «Komp'juterni systemy ta merezhi», 2014. – № 806. – S. 40–49.

[23] J. Silverman and A. Odlyzko, NTRU Report 004, Version 2, A Meet-The Middle Attack on an NTRU Private Key, Technical Report, NTRU Cryptosysytems, (2003).

[24] A Chosen-Ciphertext Attack against NTRU. [Electronic resource]. – Access mode: http://www.iacr.org/archive/crypto2000/18800021/18800021.pdf.
[25] Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms : ISO/IEC 9796-2:2010. – 54 p.
[26] IBM Raises the Bar with a 50-Qubit Quantum Computer. [Electronic resource]. – Access mode: https://www.technologyreview.com/s/609451/ibm-raises-the-bar-with-a-50-qubit-quantum-computer/?utm_campaign=add_this&utm_source=twitter&utm_medium=post.
[27] Sozdan pervyi kvantovyi komp'yuter na 53 kubitakh. [Electronic resource]. – Access mode: https://hightech.fm/2017/11/30/53-qubit.

Рецензент: Роман Олійников, д.т.н., проф., Харківський національний університет імені В.Н. Каразіна, м. Харків, Україна. E-mail: roliynykov@gmail.com.

Надійшло: Листопад 2017.

Автори:

Іван Дмитрович Горбенко, доктор технічних наук, професор, лауреат Державної премії України, професор кафедри безпеки інформаційних систем і технологій, ХНУ імені В.Н. Каразіна, майдан Свободи 4, м. Харків, 61022, Україна.
E-mail: gorbenkoi@iit.kharkov.ua.

Качко Олена Григорівна, кандидат технічний наук, начальник відділу програмування АТ «Інститут інформаційних технологій», професор кафедри програмної інженерії, Харьковский національний университет радіоелектроніки, проспект Науки 14, м. Харків, 61022, Україна.
E-mail: iit@iit.kharkov.ua.

Марина Віталіївна Єсіна, кандидат технічний наук, старший викладач кафедри безпеки інформаційних систем і технологій, ХНУ імені В.Н. Каразіна, майдан Свободи 4, м. Харків, 61022, Україна.
E-mail: rinayes20@gmail.com.

Аналіз алгоритму направленого шифрування NTRU Prime IIT Ukraine з урахуванням відомих атак.

Анотація. У роботі розглянуто сучасні криптографічні перетворення типу асиметричне направлене шифрування, а саме – NTRU-подібні криптографічні системи. На основі існуючих криптографічних перетворень цього типу (криптографічні алгоритми NTRU (ANSI X9.98-2010) та NTRU Prime) створено нову криптографічну систему NTRU Prime IIT Ukraine. Наведено короткий опис цієї криптографічної системи та проведено аналіз її стійкості до відомих атак. В кінці роботи зроблено висновки та наведено рекомендації щодо особливостей, переваг та можливості застосування нового криптографічного асиметричного алгоритму направленого шифрування NTRU Prime IIT Ukraine.

Ключові слова: атака, кільце, направлене шифрування, поле, фактор-кільце.

Рецензент: Роман Олейников, д.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, г. Харьков, Украина. E-mail: roliynykov@gmail.com.

Поступила: Ноябрь 2017.

Авторы:

Иван Дмитриевич Горбенко, доктор технических наук, профессор, лауреат Государственной премии Украины, профессор кафедры безопасности информационных систем и технологий, ХНУ имени В. Н. Каразина, площадь Свободы 4, г. Харьков, 61022, Украина.
E-mail: gorbenkoi@iit.kharkov.ua.

Качко Елена Григорьевна, кандидат технических наук, начальник отдела программирования АО «Институт информационных технологий», профессор кафедры программной инженерии, Харьковский национальный университет радиоэлектроники, проспект Науки 14, г. Харьков, 61022, Украина.
E-mail: iit@iit.kharkov.ua.

Марина Витальевна Есина, кандидат технических наук, старший преподаватель кафедры безопасности информационных систем и технологий, ХНУ имени В. Н. Каразина, площадь Свободы 4, г. Харьков, 61022, Украина.
E-mail: rinayes20@gmail.com.

Анализ алгоритма направленного шифрования NTRU Prime IIT Ukraine с учетом известных атак.

Аннотация. В работе рассмотрены современные криптографические преобразования типа ассиметричное направленное шифрование, а именно – NTRU-подобные криптографические системы. На основе существующих криптографических преобразований этого типа (криптографические алгоритмы NTRU (ANSI X9.98-2010) и NTRU Prime) создана новая криптографическая система NTRU Prime IIT Ukraine. Приведено краткое описание этой криптографической системы и проведен анализ ее устойчивости к известным атакам. В конце работы сделаны выводы и приведены рекомендации касательно особенностей, преимуществ та возможности применения нового криптографического ассиметричного алгоритма направленного шифрования NTRU Prime IIT Ukraine.

Ключевые слова: атака, кольцо, направленное шифрование, поле, фактор-кольцо.

UDC 681.142.01

DATA SINGLE-ERROR CORRECTION METHOD OF A RESIDUE CLASS CODE

Viktor Krasnobayev[1], Sergey Koshman[1], Alina Yanko[2], Sergey Moroz[3]

[1] V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
v.a.krasnobaev@gmail.com, s_koshman@ukr.net
[2] Poltava National Technical Yuri Kondratyuk University, Pershotravnevyi avenue 24, Poltava, 36011, Ukraine
al9_yanko@ukr.net
[3] Kharkiv Petro Vasylenko National Technical University of Agriculture, Rizdviana st., 19, Kharkiv, 61052, Ukraine
frost9i@ukr.net

Reviewer: Sergii Kavun, Doctor of Sciences (Economics), Ph.D. (Engineering), Full Prof., Kharkiv Educational and Research Institute of the University of Banking , Kharkiv, Ukraine
kavserg@gmail.com

Received on November 2017

Abstract: *The method of correction of single errors in the residue class (RC) is considered in this article. The results of analysis of arithmetic code correcting possibilities showed high efficiency of the use of position-independent code structures in RC, due to the presence in the non-position code structure of primary and secondary redundancy. Examples of correction of the data single errors witch presented by the code of RC are made in the article.*

Keywords: *non-positional code structure, residue classes, positional numeral systems, minimum code distance, error-control coding, data diagnosing and correction.*

1 Introduction

In general, in order to verify, diagnose and correct errors a code structure requires a certain error-correcting capability. In this case, code is required to be introduced to data duplication, i.e. information redundancy should be implemented. All of the above fully refers to a non-positional code structure (NCS) in residue classes (RC) [1-3].

For each random RC the amount of redundancy $R = M_0 / M$ uniquely determines correction capability of a non-positional error-correcting code. Error correcting codes in RC can have any given values of minimum code distance (MCD) $d_{\min}^{(RC)}$, which depends on the value of redundancy R. The acquainted theorem [1] establishes a link between error-correcting code redundancy R, the value of MCD $d_{\min}^{(RC)}$, and the amount of RC check bases k.

Error-correcting code has MCD values $d_{\min}^{(RC)}$ in case when the degree of redundancy R is not less than the product $d_{\min}^{(RC)} - 1$ of RC bases. On the one hand we get $R \geq \prod_{i=1}^{d_{\min}^{(RC)}-1} m_{q_i}$, but on the other hand $R = M_0 / M = \prod_{i=1}^{n+k} m_i / \prod_{i=1}^{n} m_i = \prod_{i=1}^{k} m_{n+i}$. In this case, it's correct to state that $d_{\min}^{(RC)} - 1 = k$, or

$$d_{\min}^{(RC)} = k + 1. \quad (1)$$

There are two approaches to solve the problem of providing NCS with all required error-correcting properties in RC.

The first approach. If the requirements for error-correcting properties of NCS are known, for example, depending on amount of errors being detected $t_{\text{det.}}$ or corrected $t_{cor.}$ required information redundancy R should be introduced, using the amount of k or the value $\{m_{n+k}\}$ of check bases. Redundancy R determines minimum code distance $d_{\min}^{(RC)}$ of NCS in RC.

Then, according to the error-control coding (ECC) theory for an ordered $(m_i < m_{i+1})$ RC we have that

$$t_{\text{det.}} \le d_{\min}^{(RC)} - 1, \tag{2}$$

$$t_{\text{det.}} \le k; \tag{3}$$

$$t_{cor.} \le \left[\frac{d_{\min}^{(RC)} - 1}{2} \right], \tag{4}$$

$$t_{cor.} \le \left[\frac{k}{2} \right]. \tag{5}$$

The second approach. For a given NCS $A_{RC} = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| ... \| a_{n+k})$ (for a given value k) its error-correcting capabilities (determined by the $d_{\min}^{(RC)}$ value) of RC code are defined by the expressions (3) and (5).

Note that, if an ordered RC is extended by adding k check bases to *n* information modules, then MCD $d_{\min}^{(RC)}$ of the error-correcting code is increased by the value *k* (see expression (1)).

The values of $d_{\min}^{(RC)}$ can be also increased by decreasing the number *n* of information bases, i.e. by transitioning to less accurate calculations. It's clear that in RC between error-correcting R properties of error-control codes and calculation accuracy W inverse proportion exists. The same computer can perform arithmetical calculations or any other math operations both with high W accuracy but a low error-correcting R capability and with lower W accuracy, but with a higher capability R of error detection and correction in order to verify, diagnose and correct data faults, as well as to demonstrate higher data processing performance (the time to execute basic operations is inversely proportional to *n* information bases in RC) [2, 4, 5].

2 The main part

Now we'll analyze the process of single-error correcting data capability in RC given the minimal information redundancy by introduction of a single $(k = 1)$ check base. In this case, according to the error control coding theory in RC [1, 2], MCD is equal to the value $d_{\min}^{(RC)} = k + 1$. If $k = 1$, then MCD is $d_{\min}^{(RC)} = 2$, which, as according to the general error control coding theory, ensures any single-error detection (an error in one of the residues a_i $(i = \overline{1, n+1})$) in NCS.

In general, just as in the positional numeral system (PNS), the process of data error correction in RC consists of three stages. The first stage – data checking (correctness or incorrectness verification of the initial number A_{RC}). On the second stage diagnosing the false $\tilde{A}_{RC}$ number (detection of a single corrupted residue $\tilde{a}_i$ of the number $\tilde{A}_{RC}$ to the base m_i in RC). And, finally, on the third stage correcting the invalid residue $\tilde{a}_i$ to its true value a_i of the number, i.e. correcting false $\tilde{A}_{RC}$ number (getting the correct number $A_{RC} = \tilde{A}_{cor.}$).

The degree of information redundancy R (code error-correcting property) is estimated by the value of MCD $d_{\min}^{(PNS)}$. As previously noted, the value of MCD is defined by the ratio $d_{\min}^{(RC)} = k + 1$, where k is the amount of check bases in an ordered RC.

Let's start with the NCS $A_{RC} = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| ... \| a_{n+k})$ in RC having a minimal $(k = 1)$ additional information redundancy. In this situation it's considered that $d_{\min}^{(RC)} = 2$.

According to the error control coding theory in PNS if the minimum code distance is granted to be $d_{\min}^{(PNS)} = 2$, a single error in a code structure is ensured to be detected. In PNS a single error is

understood as a corruption of a single information bit, for instance $0 \to 1$ or $1 \to 0$. In order to correct this single error it's required to ensure the condition, when $d_{\min}^{(PNS)} = 3$.

Contrary to PNS, a single error in RC is understood as a corruption of a single residue a_i modulo m_i. Inasmuch as the residue a_i of the number $A_{RC} = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| a_{n+1})$ modulo m_i contains $z = \{[\log_2(m_i - 1)] + 1\}$ binary bits, then it's formally correct to be considered that if $d_{\min}^{(RC)} = 2$ $(k = 1)$ is within limits of a single residue a_i, an error cluster can be detected in RC, with its length not exceeding z binary bits. However in RC, as it is shown in literature [1, 2, 5], there are some cases when a single errors can be corrected while $d_{\min}^{(RC)} = 2$.

In the light of specific features and properties of NCS representation in RC an error-correcting capability given $d_{\min}^{(RC)} = 2$ can be explained in the following manner.

1. A single error in PNS and in RC are different concepts, as it was shown before. With that being said, MCD $d_{\min}^{(PNS)}$ for PNS and $d_{\min}^{(RC)}$ for RC has different meaning and measure.

2. Existing (implicitly) intrinsic (natural, primal) information redundancy in NCS, being stored in residues $\{a_i\}$ due to their forming procedure, has a positive effect (from the perspective of increasing data jam-resistance, transfer and processing reliability) that kicks in only with the presence of a subsidiary (artificial, secondary) information redundancy. An artificial information redundancy in NCS is being introduced by using (additionally to n information bases) k check bases in RC. A distinguishing feature of RC is its significant display of the intrinsic information redundancy only if the subsidiary one is also present, due to introduction of check bases.

3. As shown in [1,2,5], error control code in RC with mutually prime bases has the MCD value of $d_{\min}^{(RC)}$ only if the information redundancy level is not less than the product of any $d_{\min}^{(RC)} - 1$ bases of a given RC.

The availability and interaction of primary and secondary redundancies during the subsidiary tests (time redundancy usage) of error-correcting process, which may provide a single-error error-correcting capability in RC, while $d_{\min}^{(RC)} = 2$ (given $k = 1$).

Indeed, according to the expressions (3) and (5) for an ordered RC following conclusions can be made: with a single $(k = 1)$ check base m_{n+1} in RC, the NCS $A = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| a_{n+1})$ can have several values of $d_{\min}^{(RC)}$. In this case, it depends on the value of check residue m_{n+1}. If, for every different RC modulus condition $m_i < m_{n+1}$ $(i = \overline{1, n})$ is met, then conclusion can be made that $d_{\min}^{(RC)} = 2$, as according to the expression (1), and $t_{\text{det.}} = 1$, according to the expression (2). If the condition $m_i \cdot m_j < m_{n+1}$ $(i, j = \overline{1, n};\ i \neq j)$ is met across the totality of $\{m_i\}$ information bases for a random modulus pair, then $d_{\min}^{(RC)} = 3$ and $t_{\text{det.}} = 2$.

Thus, for the NCS in RC given $k = 1$, the MCD $d_{\min}^{(RC)}$ can vary, depending on the value of RC check base m_{n+1}. Assume, RC is given information bases $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_4 = 7$ and moreover $m_k = m_{n+1} = m_5 = 11$. In this case error verification of any single corrupted NCS residue can be ensured.

Assume, for example, $m_k = m_{n+1} = 61$. Ad hoc, we'll draw up a Table 1, mapping information bases to check bases. As Table 1 shows, number representation specificity in RC in some cases allows not only to detect an error, but to find a place of its occurrence with the use of a single check base, which would be impossible to do in the PNS, utilizing existing methods of detecting and correcting errors.

Let's assume, that in the corrupted ($\tilde{A} \geq M$) number $\tilde{A} = (a_1 \| a_2 \| ... \| a_{i-1} \| \tilde{a}_i \| a_{i+1} \| ... \| a_n \| a_{n+1})$

the error $\tilde{a}_i = (a_i + \Delta a_i) \bmod m_i$ is verified to be present in the residue a_i modulo m_i.

Table 1 – Research results of error-correcting capabilities of error control codes in RC ($l = 1$)

$m_k = m_{n+1} = m_5 = 61;\ d_{\min}^{(RC)} = k+1 = 2,\ \prod_{i=1}^{3} m_i \le m_5$.							Max. amount of detec-table data errors in RC	Max. amount of correc-table data errors in RC
RC information bases				$\prod_{r=1}^{k'} m_{i_r} \le m_{n+1}$	k'	$d_{\min}^{(RC)'} = k'+1$		
$m_1 = 3$	$m_2 = 4$	$m_3 = 5$	$m_4 = 7$					
+	–	–	–	$3 < 61$	1	2	1	0
–	+	–	–	$4 < 61$	1	2	1	0
–	–	+	–	$5 < 61$	1	2	1	0
–	–	–	+	$7 < 61$	1	2	1	0
+	+	–	–	$3 \cdot 4 = 12 < 61$	2	3	2	1
+	–	+	–	$3 \cdot 5 = 15 < 61$	2	3	2	1
+	–	–	+	$3 \cdot 7 = 21 < 61$	2	3	2	1
–	+	+	–	$4 \cdot 5 = 20 < 61$	2	3	2	1
–	+	–	+	$4 \cdot 7 = 28 < 61$	2	3	2	1
–	–	+	+	$5 \cdot 7 = 35 < 61$	2	3	2	1
+	+	+	–	$3 \cdot 4 \cdot 5 = 60 < 61$	3	4	3	2

We'll take a look at the ratio, which makes it possible to correct an error in a given due $\tilde{a}_i$ [1].

It's clear that:

$$\tilde{A} = \left(A + \Delta A\right) \bmod M_0. \tag{6}$$

Basing on that the error magnitude can be equated to $\Delta A = (0 \| 0 \| ... \| 0 \| \Delta a_i \| 0 \| ... \| 0 \| 0)$, then the correct ($A < M$) number A can be expressed as follows:

$$A = (\tilde{A} - \Delta A) \bmod M_0 = \left[\left(a_1 \| a_2 \| ... \| a_{i-1} \| \tilde{a}_i \| a_{i+1} \| ... \| a_n \| a_{n+1}\right) - \left(0 \| 0 \| ... \| 0 \| \Delta a_i \| 0 \| ...\right.\right.$$

$$\left.\left. ... \| 0 \| 0\right)\right] \bmod M_0 = [a_1 \| a_2 \| ... \| a_{i-1} \| (\tilde{a}_i - \Delta a_i) \bmod m_i \| a_{i+1} \| ... \| a_n \| a_{n+1}] \bmod M_0.$$

We'll quantify the value of A. Inasmuch number A is correct, i.e. is contained in numerical interval $[0, M)$, then the following inequality will be fulfilled:

$$A = \left(\tilde{A} - \Delta A\right) \bmod M_0 < M\ . \tag{7}$$

Basing on the value of the error ΔA is equal to $\Delta A = \Delta a_i \cdot B_i$, then the inequality (7) will be expressed as:

$$\begin{aligned}
&\tilde{A} - \Delta a_i \cdot B_i - r \cdot M_0 < M \ \text{ or} \\
&\tilde{A} - \Delta a_i \cdot B_i - r \cdot M_0 < M_0 / m_{n+1} (r = 1, 2, 3, ...), \\
&\tilde{A} - (\tilde{a}_i - a_i) \cdot B_i - r \cdot M_0 < M_0 / m_{n+1}, \\
&\tilde{A} - (a_i - \tilde{a}_i) \cdot B_i - r \cdot M_0 < M_0 / m_{n+1}, \\
&\left(a_i - \tilde{a}_i\right) \cdot B_i < M_0 / m_{n+1} - \tilde{A} + r \cdot M_0, \\
&a_i - \tilde{a}_i < (M_0 / m_{n+1}) / B_i - \tilde{A} / B_i + r \cdot M_0 / B_i, \\
&a_i < \tilde{a}_i + (M_0 / m_{n+1}) / B_i - \tilde{A} / B_i + r \cdot M_0 / B_i.
\end{aligned} \tag{8}$$

Since the orthogonal base of RC module m_i takes the form of $B_i = \bar{m}_i \cdot M_0 / m_i$, then the expres-

sion (8) shows up as:

$$a_i < \tilde{a}_i + (m_i + r \cdot m_i \cdot m_{n+1}) / (\bar{m}_i \cdot m_{n+1}) - \tilde{A} / B_i \qquad \text{or}$$

$$a_i < \tilde{a}_i + m_i \left(1 + r \cdot m_{n+1}\right) / (\bar{m}_i \cdot m_{n+1}) - \tilde{A} / B_i . \qquad (9)$$

Inasmuch as the value of the residue a_i is a natural number, then the value of $m_i(1 + r \cdot m_{n+1}) / (\bar{m}_i \cdot m_{n+1}) - \tilde{A} / B_i$, as shown in the expression (9), should be an integer. Thus, taking an integral part of the last ratio, the formula for correcting error in the residue $\tilde{a}_i$ of the number $\tilde{A}$ will be:

$$a_i = (\tilde{a}_i + [m_i \cdot \left(1 + r \cdot m_{n+1}\right) / (\bar{m}_i \cdot m_{n+1}) - \tilde{A} / B_i) \bmod m_i]. \qquad (10)$$

We'll have a look at the examples of error correction in RC.

Example №1. Perform data verification of the number $A_{RC} = (0 \| 0 \| 0 \| 0 \| 5)$ and correct it if required, when RC was given information $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_5 = 7$ and check $m_k = m_5 = 11$ bases. Thereby, $M = \prod_{i=1}^{n} m_i = \prod_{i=1}^{4} m_i = 420$ and $M_0 = M \cdot m_{n+1} = 420 \cdot 11 = 4620$. Orthogonal RC bases B_i $(i = \overline{1, n+1})$ are shown in Table 2.

I. Data verification of $A_{RC} = (0 \| 0 \| 0 \| 0 \| 5)$. According to the control procedure [1] the value will be defined as:

Table 2 – Orthogonal RC bases B_i $(l = 1)$

$B_1 = (1 \| 0 \| 0 \| 0 \| 0) = 1540, \quad \bar{m}_1 = 1$
$B_2 = (0 \| 1 \| 0 \| 0 \| 0) = 3465, \quad \bar{m}_2 = 3$
$B_3 = (0 \| 0 \| 1 \| 0 \| 0) = 3696, \quad \bar{m}_3 = 4$
$B_4 = (0 \| 0 \| 0 \| 1 \| 0) = 2640, \quad \bar{m}_4 = 4$
$B_5 = (0 \| 0 \| 0 \| 0 \| 1) = 2520, \quad \bar{m}_5 = 6$

$$A_{PNS} = \left(\sum_{i=1}^{n+1} a_i \cdot B_i\right) \bmod M_0 = \left(\sum_{i=1}^{5} a_i \cdot B_i\right) \bmod M_0 = (a_1 \cdot B_1 + a_2 \cdot B_2 + a_3 \cdot B_3 +$$

$$a_4 \cdot B_4 + a_5 \cdot B_5) \bmod M_0 = (0 \cdot 1540 + 0 \cdot 3465 + 0 \cdot 3696 + 0 \cdot 2640 + 5 \cdot 2520) \bmod 4620 =$$

$$= (5 \cdot 2520) \bmod 4620 = 12600 (\bmod 4620) = 3360 > 420 .$$

Thus, in the process of data verification it was evaluated, that $A_{RC} = 3360 > M = 420$. In this case, with the possibility of only single errors appearing, conclusion is made that the number in question $\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$ is incorrect ($3360 > M = 420$).

In order to correct the number $\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$ data is required to be verified first, i.e. corrupted residue $\tilde{a}_i$ has to be detected. Once done, the true value of the residue a_i modulo m_i needs to be defined, whereupon the corrupted residue $\tilde{a}_i$ should be corrected.

II. Data diagnosing of $\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$. According to the mapping method [1,2], possible projections $\tilde{A}_j$ of the number $\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$ are:

$$\tilde{A}_1 = (0 \| 0 \| 0 \| 5), \ \tilde{A}_2 = (0 \| 0 \| 0 \| 5), \ \tilde{A}_3 = (0 \| 0 \| 0 \| 5),$$

$$\tilde{A}_4 = (0 \| 0 \| 0 \| 5) \text{ and } \tilde{A}_5 = (0 \| 0 \| 0 \| 0).$$

Computational formula for the values $\tilde{A}_{j\,PNS}$ of PNS number projections is written as [1]:

$$\tilde{A}_{j\,PNS} = \left(\sum_{\substack{i=1; \\ j=\overline{1,\,n+1.}}}^{n} a_i \cdot B_{ij} \right) \bmod M_j = (a_1 \cdot B_{1j} + a_2 \cdot B_{2j} + \ldots + a_n \cdot B_{nj}) \bmod M_j . \qquad (11)$$

According to the expression (11) we'll compute all the values of $\tilde{A}_{j\,PNS}$. Once done, we will make $(n+1)$ comparison of the $\tilde{A}_{j\,PNS}$ numbers to the number $M = M_0 / m_{n+1}$. If there are any numbers not being contained in the informational numeric interval $[0, M)$, which contains k correct numbers (i.e. $\tilde{A}_k \geq M$), among $\tilde{A}_i$ projections, then conclusion is made that these k residues of the number A are not corrupted. Only the residues among the rest $[(n+1)-k]$ number $\tilde{A}_{RC}$ residues can be false.

The set of the active quotient residues for a given RC and the totality of the quotient B_{ij} orthogonal bases are shown in Table 3 and Table 4 respectively.

Table 3 – Set of the active quotient RC residues ($l = 1$)

j \ i	m_1	m_2	m_3	m_4	M_j
1	4	5	7	11	1540
2	3	5	7	11	1155
3	3	4	7	11	924
4	3	4	5	11	660
5	3	4	5	7	420

Table 4 – The totality of the quotient orthogonal RC bases B_{ij} ($l = 1$)

B_{ij} j \ i	1	2	3	4
1	385	616	1100	980
2	385	231	330	210
3	616	693	792	672
4	220	165	396	540
5	280	105	336	120

Now then (Table 4):

$$\tilde{A}_{1PNS} = \left(\sum_{i=1}^{4} a_i \cdot B_{i1} \right) \bmod M_1 = (a_1 \cdot B_{11} + a_2 \cdot B_{21} + a_3 \cdot B_{31} + a_4 \cdot B_{41}) \bmod M_1 =$$
$$= (0 \cdot 385 + 0 \cdot 616 + 0 \cdot 1100 + 5 \cdot 980) \bmod 1540 = 280 < 420 .$$

Arriving at conclusion, that the residue a_1 of the number $\tilde{A}_1$ is possibly a corrupted residue $\bar{a}_1$;

$$\tilde{A}_{2PNS} = \left(\sum_{i=1}^{4} a_i \cdot B_{i2} \right) \bmod M_2 = (a_1 \cdot B_{12} + a_2 \cdot B_{22} + a_3 \cdot B_{32} + a_4 \cdot B_{42}) \bmod M_2 =$$
$$= (0 \cdot 385 + 0 \cdot 231 + 0 \cdot 330 + 5 \cdot 210) \bmod 1155 = 1050 > 420 .$$

Hence, the residue a_2 is ensured being not corrupted;

$$\tilde{A}_{3PNS} = \left(\sum_{i=1}^{4} a_i \cdot B_{i3} \right) \bmod M_3 = (a_1 \cdot B_{13} + a_2 \cdot B_{23} + a_3 \cdot B_{33} + a_4 \cdot B_{43}) \bmod M_3 =$$
$$= (0 \cdot 616 + 0 \cdot 693 + 0 \cdot 792 + 5 \cdot 672) \bmod 924 = 588 > 420 .$$

Deduced, the residue a_3 is ensured being not corrupted;

$$\tilde{A}_{4PNS}=\left(\sum_{i=1}^{4}a_i\cdot B_{i4}\right)\bmod M_4=(a_1\cdot B_{14}+a_2\cdot B_{24}+a_3\cdot B_{34}+a_4\cdot B_{44})\bmod M_4=$$
$$=(0\cdot 220+0\cdot 165+0\cdot 369+5\cdot 540)\bmod 660=60<420.$$

Conclusion: the residue a_4 modulo m_4 of the number $\tilde{A}_4$ is possibly a corrupted residue $\bar{a}_4$;

$$\tilde{A}_{5PNS}=\left(\sum_{i=1}^{4}a_i\cdot B_{i5}\right)\bmod M_5.\ \text{Since}\ M_5=M=420,$$

the residue $\bar{a}_5$ of the check module $m_k=m_5$ will be always among the totality of possibly corrupted residues $\bar{a}_i$ of RC number.

Overall conclusion. During data diagnosing of $\tilde{A}=(0\|0\|0\|0\|5)$ in NCS, the residues $a_2=0$ and $a_3=0$ were ensured not being corrupted. The residues to the bases m_1, m_4 and m_5 might be corrupted, i.e. the residues $\bar{a}_1=0$, $\bar{a}_4=0$ and $\bar{a}_5=5$. In this case it's required to correct the residues $\bar{a}_1$, $\bar{a}_4$ and $\bar{a}_5$.

III. Correcting data errors $\tilde{A}_{3360}=(0\|0\|0\|0\|5)$. According to the acquainted [1] expression:

$$a_i=\left(\bar{a}_i+\left[\frac{m_i\cdot(1+r\cdot m_{n+1})}{m_{n+1}\cdot\bar{m}_i}-\frac{\tilde{A}}{B_i}\right]\right)\bmod m_i,\qquad(12)$$

we will correct possibly $\bar{a}_1$, $\bar{a}_4$ and $\bar{a}_5$ corrupted residues a_1, a_4 and a_5, where $r=1,2,3,\ldots$.

It turns out that:

$$a_1=\left(\bar{a}_1+\left[\frac{m_1\cdot(1+r\cdot m_{n+1})}{m_{n+1}\cdot\bar{m}_1}-\frac{\tilde{A}}{B_1}\right]\right)\bmod m_1=\left(0+\left[\frac{3\cdot(1+r\cdot 11)}{11\cdot 1}-\frac{3360}{1540}\right]\right)\bmod 3=$$
$$=(0+[3,27-2,18])\bmod 3=(0+[1,09])\bmod 3=(0+1)\bmod 3=1;$$
$$a_4=\left(\bar{a}_4+\left[\frac{m_4\cdot(1+r\cdot m_{n+1})}{m_{n+1}\cdot\bar{m}_4}-\frac{\tilde{A}}{B_4}\right]\right)\bmod m_4=\left(0+\left[\frac{7\cdot 12}{11\cdot 4}-\frac{3360}{2640}\right]\right)\bmod 7=$$
$$=(0+[1,9-1,27])\bmod 7=(0+[0,63])\bmod 7=(0+0)\bmod 7=0;$$
$$a_5=\left(\bar{a}_5+\left[\frac{m_{n+1}\cdot(1+r\cdot m_{n+1})}{m_{n+1}\cdot\bar{m}_{n+1}}-\frac{\tilde{A}}{B_5}\right]\right)\bmod m_{n+1}=\left(5+\left[\frac{11\cdot(1+11)}{11\cdot 6}-\frac{3360}{2520}\right]\right)\bmod 11=$$
$$=(5+[2-1,3])\bmod 11=(5+[0,7])\bmod 11=(5+0)\bmod 5=0.$$

With accordance to the computed residues $a_1=1$, $a_4=0$ and $a_5=0$ we are correcting (recovering) the corrupted number $\tilde{A}_{3360}=(0\|0\|0\|0\|5)$, i.e. the corrected number becomes $\tilde{A}_{cor.}=(1\|0\|0\|0\|5)$.

To validate corrected data, as according to the acquainted [1] expression, we'll define the value of the number $\tilde{A}_{cor.}=(1\|0\|0\|0\|5)$ in the following way (see Table 2):

$$\tilde{A}_{cor.PNS}=\left(\sum_{i=1}^{5}a_i\cdot B_i\right)\bmod M_0=(a_1\cdot B_1+a_2\cdot B_2+a_3\cdot B_3+a_4\cdot B_4+a_5\cdot B_5)\bmod M_0=$$
$$=(1\cdot 1540+0\cdot 3465+0\cdot 3696+0\cdot 2640+5\cdot 2520)\bmod 4620=14140(\bmod 4620)=280.$$

Thus $280<M=420$, the number $\tilde{A}_{280}=(1\|0\|0\|0\|5)$ is correct.

In order to validate correctness of the number $\tilde{A}_{3360}$ we'll make a computation and comparison of the values to the correct residues $a_2=0$ and $a_3=0$. In this case they are $a_2=\left(0+\left[\frac{4\cdot(1+11)}{11\cdot 3}-\frac{3360}{3465}\right]\right)\bmod 4=0$ and $a_3=\left(0+\left[\frac{5\cdot(1+11)}{11\cdot 4}-\frac{3360}{3696}\right]\right)\bmod 5=0$. The result-

ed computations $a_2 = 0$ and $a_3 = 0$ of the residues modulo m_2 and m_3 in RC verified correctness of the corrupted number $\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$. Thus, the original number $\tilde{A}_{RC} = (0 \| 0 \| 0 \| 0 \| 5)$ is corrupted $\tilde{A}_{3360}$, wherein the single error $\Delta a_1 = 1$ occurred modulo m_1. This error made the correct number A_{280} being corrupted $\tilde{A}_{3360}$.

In order to verify if the correct number A_{280} is true, subsidiary tests on the process of corruption and correction of the number A_{280} modulo $m_1 = 3$ are required. The amount of possible N_{CC} incorrect (corrupted) $\tilde{A}_{RC}$ codewords (if only a single error occurred) for each correct A_{RC} number are

$$N_{CC} = \sum_{i=1}^{n+1} m_i - (n+1).$$

Test results have shown that corruption of the residue a_1 modulo $m_1 = 3$ of the correct number A_{280} can produce only two incorrect numbers: $\tilde{A}_{3360} = (\tilde{0} \| 0 \| 0 \| 0 \| 5)$ and $\tilde{A}_{1820} = (\tilde{2} \| 0 \| 0 \| 0 \| 5)$. This points to the fact that the corrected number $A_{cor.} = A_{280} = (1 \| 0 \| 0 \| 0 \| 5)$ is both correct (is contained in the interval [0, 420)) and true.

The trueness of the resulted number $A_{280} = (\hat{1} \| 0 \| 0 \| 0 \| 5)$ is confirmed by the fact that the single error $\Delta a_1 = 2$ to the base $m_1 = 3$ converts $(\tilde{A} = (A + \Delta A) \bmod M_0 =$ $= (1 \| 0 \| 0 \| 0 \| 5) + (2 \| 0 \| 0 \| 0 \| 0) = \left[(1+2) \bmod 3 \| 0 \| 0 \| 0 \| 5\right] = (\tilde{0} \| 0 \| 0 \| 0 \| 5))$ this number to the unique incorrect number $\tilde{A}_{3360} = (\tilde{0} \| 0 \| 0 \| 0 \| 5)$.

Example №2. Assume, the correct number is $A_{280} = (1 \| 0 \| 0 \| 0 \| 5)$ and assume that $\Delta a_1 = 1$. In this case $\tilde{A} = (A + \Delta A) \bmod M_0 = (1 \| 0 \| 0 \| 0 \| 5) + (1 \| 0 \| 0 \| 0 \| 0) =$ $= \left[(1+1) \bmod 3 \| 0 \| 0 \| 0 \| 5\right] = (\tilde{2} \| 0 \| 0 \| 0 \| 5)$. This RC number is relevant to the number 1820 in PNS, i.e. the number $\tilde{A}_{1820}$ is incorrect. We'll correct the number $\tilde{A}_{1820}$ now.

Data diagnosing should be made ahead of correcting the number $\tilde{A}_{1820}$. To do this we'll map projections A_j ($j = \overline{1, 5}$) of the number $\tilde{A}_{1820} = (2 \| 0 \| 0 \| 0 \| 5)$ first. Resulted RC code structures are: $\tilde{A}_1 = (0 \| 0 \| 0 \| 5)$, $\tilde{A}_2 = (2 \| 0 \| 0 \| 5)$, $\tilde{A}_3 = (2 \| 0 \| 0 \| 5)$, $\tilde{A}_4 = (2 \| 0 \| 0 \| 5)$ and $\tilde{A}_5 = (2 \| 0 \| 0 \| 0)$.

All the projections of $\tilde{A}_{j\,PNS}$ are:

$$\tilde{A}_{1PNS} = (5 \cdot 980) \bmod 1540 = 280 < 420 = M;$$

$$\tilde{A}_{2PNS} = (2 \cdot 385 + 5 \cdot 231) \bmod 1155 = 1925 \left(\bmod 1155\right) = 770 > 420 = M;$$

$$\tilde{A}_{3PNS} = (2 \cdot 616 + 5 \cdot 672) \bmod 924 = 4592 \left(\bmod 924\right) = 896 > 420 = M;$$

$$\tilde{A}_{4PNS} = (2 \cdot 220 + 5 \cdot 540) \bmod 660 = 3140 \left(\bmod 660\right) = 500 > 420 = M;$$

$$\tilde{A}_{5PNS} = 2 \cdot 280 (\bmod 420) = 560 \left(\bmod 420\right) = 140 < 420 = M.$$

Inasmuch as $\tilde{A}_{2PNS}$, $\tilde{A}_{3PNS}$ and $\tilde{A}_{4PNS} > 420$, the conclusion is made that the residues $a_2 = 0$, $a_3 = 0$ and $a_4 = 0$ of the number $\tilde{A}_5 = (2 \| 0 \| 0 \| 0 \| 5)$ are not corrupted. Only the residues a_1 and a_5 can be corrupted $\bar{a}_1 = 2$ and $\bar{a}_5 = 5$.

We obtain, that:

$$a_1 = \left(\bar{a}_1 + \left[\frac{m_1 \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \bar{m}_1} - \frac{\tilde{A}}{B_1} \right] \right) \bmod m_1 = \left(2 + \left[\frac{3 \cdot (1+11)}{11 \cdot 1} - \frac{1820}{1540} \right] \right) \bmod 3 =$$

$$= \left(2 + [3,27 - 1,18]\right) \bmod 3 = \left(2 + [2,09]\right) \bmod 3 = (2+2) \bmod 3 = 4 (\bmod 3) = 1.$$

Hence, the corrected residue modulo m_1 is $a_1 = 1$. In a like manner the residue $a_5 = 5$.

Applying the results a_1 and a_5 the corrupted number $\tilde{A}_{1820} = (\tilde{2} \| 0 \| 0 \| 0 \| 5)$ is corrected. As a final result the corrected number is $A_{280} = (1 \| 0 \| 0 \| 0 \| 5)$.

Example №3. Performing verification of the number $A_{RC} = (0 \| 0 \| 0 \| 2 \| 1)$. In case corruption was detected, data diagnosing and correction should be made.

I. Data checking of $A_{RC} = (0 \| 0 \| 0 \| 2 \| 1)$. According to the acquainted control procedure A_{PNS} will be calculated using expression:

$$A_{PNS} = \left(\sum_{i=1}^{n+1} a_i \cdot B_i \right) \bmod M_0 = (0 \cdot 1540 + 0 \cdot 3465 + 0 \cdot 3696 + 2 \cdot 2640 + 1 \cdot 2520) \bmod 4620 =$$

$$= 7800 (\bmod 4620) = 3180 > 420.$$ This number is incorrect $\tilde{A}_{3180}$.

II. Data diagnosing of $\tilde{A}_{3180} = (0 \| 0 \| 0 \| 2 \| 1)$. All possible projections $\tilde{A}_j$ of the number $\tilde{A}_{3180}$ are: $\tilde{A}_1 = (0 \| 0 \| 2 \| 1)$, , $\tilde{A}_3 = (0 \| 0 \| 2 \| 1)$, $\tilde{A}_4 = (0 \| 0 \| 0 \| 1)$ and $\tilde{A}_5 = (0 \| 0 \| 0 \| 2)$.

Calculating the values of all of five projections $\tilde{A}_j$ in PNS:

$$\tilde{A}_{1RC} = (0 \| 0 \| 2 \| 1) = \tilde{A}_{1PNS} = (a_1 \cdot B_{11} + a_2 \cdot B_{21} + a_3 \cdot B_{31} + a_4 \cdot B_{41}) \bmod M_1 =$$
$$= (0 \cdot 385 + 0 \cdot 616 + 2 \cdot 1100 + 1 \cdot 980) \bmod 1540 = 100 < M = 420;$$
$$\tilde{A}_{2RC} = (0 \| 0 \| 2 \| 1) = \tilde{A}_{2PNS} = (a_1 \cdot B_{12} + a_2 \cdot B_{22} + a_3 \cdot B_{32} + a_4 \cdot B_{42}) \bmod M_2 =$$
$$= (0 \cdot 385 + 0 \cdot 231 + 2 \cdot 330 + 1 \cdot 210) \bmod 1155 = 870 > M = 420;$$
$$\tilde{A}_{3RC} = (0 \| 0 \| 2 \| 1) = \tilde{A}_{3PNS} = (a_1 \cdot B_{13} + a_2 \cdot B_{23} + a_3 \cdot B_{33} + a_4 \cdot B_{43}) \bmod M_3 =$$
$$= (0 \cdot 616 + 0 \cdot 693 + 2 \cdot 792 + 1 \cdot 672) \bmod 924 = 418 < M = 420;$$
$$\tilde{A}_{4RC} = (0 \| 0 \| 0 \| 1) = \tilde{A}_{4PNS} = (a_1 \cdot B_{14} + a_2 \cdot B_{24} + a_3 \cdot B_{34} + a_4 \cdot B_{44}) \bmod M_4 =$$
$$= (0 \cdot 220 + 0 \cdot 165 + 2 \cdot 396 + 1 \cdot 540) \bmod 660 = 540 > M = 420;$$
$$\tilde{A}_{5RC} = (0 \| 0 \| 0 \| 2) = \tilde{A}_{5PNS} = (a_1 \cdot B_{15} + a_2 \cdot B_{25} + a_3 \cdot B_{35} + a_4 \cdot B_{45}) \bmod M_5 =$$
$$= (0 \cdot 280 + 0 \cdot 105 + 2 \cdot 336 + 1 \cdot 120) \bmod 420 = 240 < M = 420.$$

The calculations of the $\tilde{A}_{j\,PNS}$ values and comparing them to the verification interval $[0, 420)$ range of correct RC numbers A_{RC} resulted in following. The totality of the residues $a_2 = 0$ and $a_4 = 0$ is correct (residues are not being corrupted), while the residues $\bar{a}_1 = 0$, $\bar{a}_3 = 0$ and $\bar{a}_5 = 1$ of the incorrect number $\tilde{A}_{3180} = (0 \| 0 \| 0 \| 2 \| 1)$ might be incorrect (could have been corrupted).

III. Correcting possibly corrupted residues $\bar{a}_1$, $\bar{a}_3$ and $\bar{a}_5$ of the number $\tilde{A}_{3180}$.

Possibly corrupted residues $\bar{a}_1 = 0$, $\bar{a}_3 = 0$ and $\bar{a}_5 = 1$ required to be corrected using expression

$$a_i = \left(\tilde{a}_i + \left[\frac{m_i \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \bar{m}_i} - \frac{\tilde{A}}{B_i} \right] \right) \bmod m_i.$$

Then:

$$a_1 = \left(\bar{a}_1 + \left[\frac{m_1 \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \bar{m}_1} - \frac{\tilde{A}}{B_1} \right] \right) \bmod m_1 = \left(0 + \left[\frac{3 \cdot (1 + r \cdot 11)}{11 \cdot 1} - \frac{3180}{1540} \right] \right) \bmod 3 =$$
$$= (0 + [3,27 - 2,06]) \bmod 3 = (0 + [1,21]) \bmod 3 = (0 + 1) \bmod 3 = 1.$$

Hence, $a_1 = 1$.

For the value $\bar{a}_3$ it is:

$$a_3 = \left(\tilde{a}_3 + \left[\frac{m_3 \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \bar{m}_3} - \frac{\tilde{A}}{B_3} \right] \right) \bmod m_3 = \left(0 + \left[\frac{5 \cdot (1 + r \cdot 11)}{11 \cdot 4} - \frac{3180}{3696} \right] \right) \bmod 5 =$$
$$= (0 + [1,36 - 0,86]) \bmod 5 = (0 + [0,5]) \bmod 5 = (0 + 0) \bmod 5 = 0.$$

In this case $a_3 = 0$.

For the residue $\bar{a}_5$ value is:

$$a_5 = \left(\tilde{a}_5 + \left[\frac{m_5 \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \bar{m}_5} - \frac{\tilde{A}}{B_5} \right] \right) \bmod m_5 = \left(1 + \left[\frac{11 \cdot (1 + r \cdot 11)}{11 \cdot 6} - \frac{3180}{2520} \right] \right) \bmod 11 =$$

$$= \left(1 + [2 - 1,26]\right) \bmod 11 = \left(1 + [0,74]\right) \bmod 11 = (1 + 0) \bmod 11 = 1.$$

Obtaining that $a_5 = 1$.

Using the calculated values $a_1 = 1$, $a_3 = 0$ and $a_5 = 1$ of the recovered residues the corrupted number $\tilde{A}_{RC} = (0 \| 0 \| 0 \| 2 \| 1)$ can be corrected, becoming $A_{RC} = (1 \| 0 \| 0 \| 2 \| 1)$. Verified by $100 < 420$.

3 Conclusions of research

Contrary to PNS (positional numeral system), arithmetic RC (residue class) codes feature additional correcting properties. Thus, NCS (non-positional code structure) involves both intrinsic and subsidiary information redundancies, that in some cases results in allowing to correct single errors in RC, while MCD is $d_{\min}^{(RC)} = 2$. However, correcting single errors requires performing subsidiary tests of data checking, i.e. time redundancy usage, additionally to information redundancy. Examples of specific implementation of a single error correcting procedures were introduced, that prove reviewed method is possible to be implemented in order to correct data errors in RC.

References

[1] Akushskii I. Ya. Mashinnaya arifmetika v ostatochnykh klassakh / I. Ya. Akushskii, D. I. Yuditskii – M.: Sov. Radio, 1968. – 440 s.

[2] Krasnobayev V. A. A method for increasing the reliability of verification of data represented in a residue number system / V. A. Krasnobayev, S. A. Koshman, M. A. Mavrina // Cybernetics and Systems Analysis. – November 2014. – Volume 50, Issue 6, pp. 969-976.

[3] Modeli i metody obrabotki dannykh v sisteme ostatochnykh klassov: [monografiya] / [Krasnobaev V. A., Koshman S. A. i dr.] – Khar'kov: OOO "V dele", 2017. – 197 s.

[4] Stasev Yu.V., Kuznetsov A.A., Nosik A.M. Formation of pseudorandom sequences with improved autocorrelation properties // Cybernetics and Systems Analysis, Volume 43, Issue 1, January 2007, Pages 1 – 11.

[5] Karpenko O., Kuznetsov A., Sai V. Stasev Yu.. Discrete Signals with Multi-Level Correlation Function // Telecommunications and Radio Engineering. - Volume 71, 2012 Issue 1. pp. 91-98.

Рецензент: Сергій Кавун, доктор економічних наук, к.т.н., проф., Харківський інститут банківської справи УБС НБУ, Харків, Україна.
E-mail: kavserg@gmail.com

Надійшло: Листопад 2017.

Автори:
Віктор Краснобаєв, д.т.н., проф.., Харківський національний університет імені В. Н. Каразіна, Харків, Україна.
E-mail: v.a.krasnobaev@gmail.com

Сергій Кошман, к.т.н., доцент, Харківський національний університет імені В. Н. Каразіна, Харків, Україна.
E-mail: s_koshman@ukr.net

Аліна Янко, к.т.н., Полтавський національний технічний університет імені Юрія Кондратюка, Полтава, Україна.
E-mail: al9_yanko@ukr.net

Сергій Мороз, к.т.н., Харківський національний технічний університет сільського господарства імені Петра Василенка, Харків, Україна.
E-mail: frost9i@ukr.net

Метод виправлення однократних помилок даних, що представлені кодом класу лишків.

Анотація. У даній статті розглянуто метод виправлення однократних помилок у класі лишків (КЛ). Результати аналізу коригувальних можливостей арифметичного коду показали високу ефективність використання непозиційних кодових структур у КЛ, за рахунок наявності у непозиційній кодової структурі первинної та вторинної надмірності. У статті наведені приклади виправлення одноразових помилок даних, що представлені кодом КЛ.

Ключові слова: непозиційна кодова структура, клас лишків, позиційна система числення, мінімальна кодова відстань, завадостійке кодування, діагностика та корекція даних.

Рецензент: Сергей Кавун, доктор экономических наук, к.т.н., проф., Харьковский институт банковского дела УБД НБУ, пр. Победы, 55, г. Харьков, 61174, Украина.
E-mail: kavserg@gmail.com

Поступила: Ноябрь 2017.

Авторы:
Виктор Краснобаев, д.т.н., проф., Харьковский национальный университет имени В. Н. Каразина, Харьков, Украина.
E-mail: v.a.krasnobaev@gmail.com

Сергей Кошман, к.т.н., доцент, Харьковский национальный университет имени В. Н. Каразина, Харьков, Украина.
E-mail: s_koshman@ukr.net

Алина Янко, к.т.н., Полтавский национальный технический университет имени Юрия Кондратюка, Полтава, Украина.
E-mail: al9_yanko@ukr.net

Сергей Мороз, к.т.н., Харьковский национальный технический университет сельского хозяйства имени Петра Василенка, Харьков, Украина.
E-mail: frost9i@ukr.net

Метод исправления однократных ошибок данных, представленных кодом класса вычетов.

Аннотация. В данной статье рассмотрен метод исправления однократных ошибок в классе вычетов (КВ). Результаты анализа корректирующих возможностей арифметического кода показали высокую эффективность использования непозиционных кодовых структур в КВ, за счёт наличия в непозиционной кодовой структуре первичной и вторичной избыточности. В статье приведены примеры исправления однократных ошибок данных, представленных кодом КВ.

Ключевые слова: непозиционная кодовая структура, класс вычетов, позиционная система счисления, минимальное кодовое расстояние, помехоустойчивое кодирование, диагностика и коррекция данных.

УДК 004.9: 621.391.7

МЕТОДЫ ФОРМИРОВАНИЯ И ОБРАБОТКИ OFDM СИГНАЛОВ В СОВРЕМЕННЫХ БЕСПРОВОДНЫХ ДИСКРЕТНЫХ КОММУНИКАЦИОННЫХ СИСТЕМАХ

Александр Замула, Владислав Морозов

Харьковский национальный университет имени В.Н. Каразина, площадь Свободы, 4, г. Харьков, 61022, Украина
zamylaaa@gmail.com, ilissar@hotmail.com

Рецензент: Вячеслав Харченко, д.т.н., проф., академик Академии наук прикладной радиоэлектроники, Национальный аэрокосмический университет им. М. Є. Жуковского, Харьков, Украина
v_s_kharchenko@ukr.net

Поступила Декабрь 2017

***Аннотация**: Рассмотрены технологии формирования сигналов, используемых в системах связи и телекоммуникаций, а также приводится краткий анализ перспективных технологий, которые могут найти применение в беспроводных системах связи широкополосного доступа. Показано, что широко используемая схема модуляции OFDM обладает рядом недостатков, которые могут привести к снижению показателей эффективности систем. Представлены альтернативные технологии формирования сигналов, в частности, технология W-OFDM, позволяющие устранить известные недостатки технологии OFDM.*

***Ключевые слова:** множественный доступ, сотовая связь, частотное разделение, помехоустойчивость, интерференция, оконная обработка, пик-фактор, модуляция.*

1 Введение

Современные беспроводные системы (например, спутниковые системы связи, системы мобильной телефонной связи и др.), относятся к многопользовательским системам. При проектировании таких систем основной проблемой является выбор необходимого способа множественного доступа, т. е возможности одновременного использования многими абонентами данной системы канала связи с минимальным взаимным влиянием [1,2].

Широкополосные сигналы активно используются в современных высокоскоростных системах сотовой связи стандартов WiMax, Mobile WiMax, MBWA, беспроводных дискретных коммуникационных системах, например LTE и Wi-Fi, при передаче информации цифрового телевидения (DVB-T) и радио (DRM, DAB), в системах радиолокации и т.д. Использование сигналов с ортогональным частотным разделением каналов и мультиплексированием (*Orthogonal frequency – division multiplexing, далее - OFDM*), в том числе в указанных системах передачи информации, позволяет повысить не только информационную емкость системы в условиях многолучевого распространения при ограниченной полосе пропускания, но и скорость приема-передачи данных, приблизив её к пропускной способности канала, увеличить скрытность передачи и помехоустойчивость системы.

В настоящее время идут интенсивные процессы развития, исследования и стандартизации технологий для пятого поколения сетей сотовой связи (далее 5G). При этом, наиболее приоритетными задачами данного направления работ считаются: достижение максимальной скорости передачи данных (до 20 Гбит/сек); обеспечение плотности пользовательских устройств (до 10^6 устройств/км^2); предоставление пользователям сервисов сверхнадежной коммуникации с малой задержкой (URLLC) (задержка передачи данных - не более 1 ms) [3,4]. В качестве возможных решений для достижения вышеуказанных характеристик для сетей 5G рассматриваются: - использование спектра в миллиметровом диапазоне [5]; - новые виды модуляции сигналов и методы кодирования; - методы множественного доступа; - усовершенствованные технологии синтеза архитектуры антенн и сетей [5-6]. Помимо этого, заслуживают самого пристального внимания исследования, проводимые в рамках следующих направлений:

- ортогональное мультиплексирование с частотным разделением каналов с фильтрованием (F-OFDM) [7-9];
- технология пространственного кодирования сигнала (MIMO) [10];
- облачные сети радиосвязи (CRAN) [11];
- технологии ортогонального частотного разделения каналов с кодированием (C-OFDM) [12] и др.

2 Принципы технологии OFDM

Развитие технологий беспроводных коммуникаций постоянно формировалось на основе исследований форм сигналов. В качестве примера можно привести успех четвертого поколения (4G) связи, который базируется, в том числе, на использовании схемы цифровой модуляции OFDM.

Основная идея OFDM состоит в том, что для достижения высокой скорости передачи, в частотной области применяется деление полного диапазона частот сигнала на некоторое число неперекрывающихся частотных подканалов с меньшими скоростями. При этом каждый подканал (поднесущая) модулируется отдельным символом, затем эти каналы мультиплексируются по частоте и данные передаются параллельно по ортогональным подканалам. По сравнению с передачей использующей одну несущую, этот подход обеспечивает повышенную устойчивостью к узкополосной интерференции и искажениям в канале связи. Также обеспечивается более высокий уровень «гибкости» системы, так как параметры модуляции, такие как размер созвездия, скорость кодирования, могут быть выбраны независимо для каждого подканала.

В структуру OFDM модема входят передатчик и приемник. В передатчике исходный последовательный поток информационных битов (Рис. 1) кодируется помехоустойчивым кодом (*согласно рекомендации LTE 3GPP TS 36.211 используется сверточный турбокод с базовой скоростью 1/3*), перемежается (П) и демультиплексируется на N параллельных подпотоков.

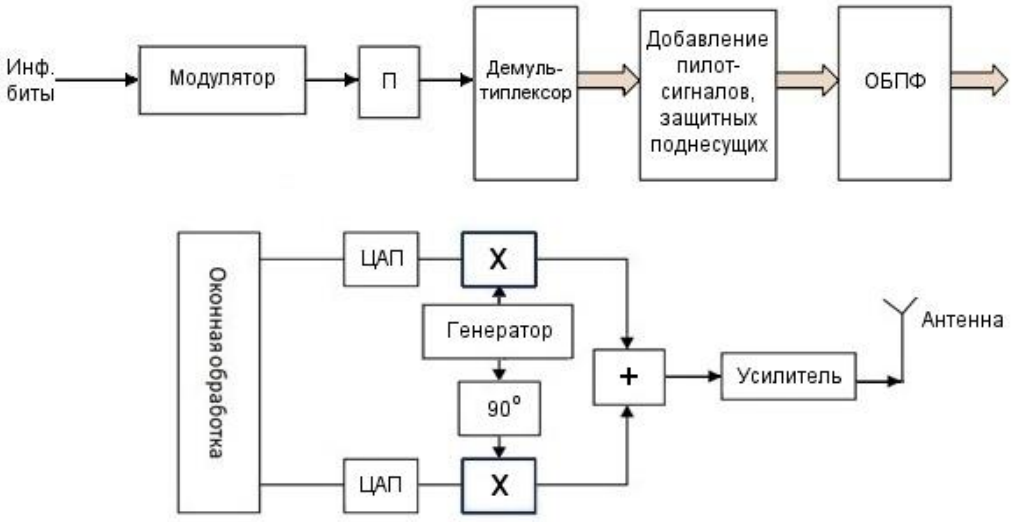

Рис. 1 – Структурная схема

Далее каждый из потоков отображается в поток символов с помощью процедуры фазовой (BPSK, QPSK, 8-PSK) или амплитудно-фазовой квадратурной модуляции (QAM). При использовании модуляции BPSK получается поток двоичных чисел (1 и -1), при QPSK, 8-PSK, QAM — поток комплексных чисел. Помимо поднесущих, на которых передается информация, существуют служебные поднесущие. К ним относятся защитные интервалы, пилот-сигналы и дополнительная служебная информация для синхронизации приемника и передатчика, и режимов их работы. Пилот-сигналы могут иметь фиксированное положение на под-

несущих, или переменное, изменяющееся от символа к символу OFDM в кадрах. При этом благодаря вставке между смежными подканалами достаточного по длительности защитного интервала, исключается спектральное перекрытие. В этом случае снижается межканальная интерференция (межбитовая интерференция, ICI), уменьшается вероятность битовой ошибки, а значит, повышается пропускная способность системы беспроводного доступа.

Процедура умножения на комплексную экспоненту с соответствующей частотой подканала и затем суммирование всех подканалов для формирования OFDM сигнала аналогична операции обратного преобразования Фурье. В связи с этим для формирования требуемого OFDM-символа применяют аппарат быстрого обратного преобразования Фурье (ОБПФ), что значительно упрощает реализацию модуляторов.

Сохранение ортогональности является необходимым для того, чтобы приемник мог правильно распознать информацию на поднесущих. Для этого необходимо выполнить следующие условия: - приемник и передатчик должны быть синхронизированы; - аналоговые компоненты передатчика и приемника должны быть очень высокого качества; - используемый канал передачи данных не должен быть многопутным (многолучевым).

К сожалению, на практике в системах радиосвязи, многолучевое искажение практически неизбежно, что приводит к искажениям полученного сигнала. Для устранения такого рода помех необходимо выбрать защитный интервал, длительность которого больше, чем максимальная задержка распространения в канале передачи. Таким образом, можно компенсировать большинство видов интерференции между каналами (интерференцию между поднесущими) и между смежными блоками передачи (т.е. межсимвольную интерференцию (ISI)). Для уменьшения внеполосного излучения сигналов используется оконная обработка временного сигнала, окном типа «приподнятый косинус».

Далее цифро-аналоговые преобразователи (ЦАП) преобразуют в аналоговый вид отдельно действительную и мнимую компоненты. После прохождения через фильтр нижних частот сигнал поступает на квадратурный смеситель, который переносит полезный спектр OFDM-сигнала на несущую частоту. Далее эти сигналы суммируются, усиливаются, и формируется сигнал OFDM.

Широкое использование цифровой схемы модуляции OFDM обусловлено целым рядом полезных отличительных свойств данной технологии:

- устойчивость к последствиям многолучевого распространения электромагнитных волн; - высокая помехоустойчивость к узкополосным помехам;

- устойчивость к межсимвольной интерференции за счет того, что продолжительность символа во вспомогательной поднесущей значительно больше в сравнении с задержкой распространения, чем в традиционных схемах модуляции;

- высокая спектральная эффективность в сравнении с традиционными системами с частотным разделением каналов за счет большого количества поднесущих;

- возможность использования различных схем модуляции для разных поднесущих, что позволяет адаптироваться к конкретным условиям распространения радиосигнала и обеспечить требуемое качество принимаемых сигналов;

- относительная простота реализации необходимых методов цифровой обработки и др.

3 Перспективные технологии формирования сигналов в современных мобильных системах телекоммуникаций

Эффективность современного поколения систем мобильной связи в значительной степени основывается на использовании, в том числе, OFDM модуляции. Однако для обеспечения дальнейшего прогресса и перехода на более совершенные технологии связи пятого поколения необходим пересмотр и совершенствование технологии OFDM, равно как и широкое внедрение других технологий. В этом контексте, следует выделить следующие принципиальные отличия технологии 5G от технологий мобильной коммуникации предыдущего поколения [4-5]:

1. Смешанная нумерология. Одной из целей 5G является обеспечить использование различных сервисов, в частности eMBB, mMTC и URLLC. Предполагается, что технология 5G должна поддерживать более гибкое использование доступной полосы частот для увелечение пропускной способности. Для этого необходимо разработать и внедрить различные варианты использования доступных частотных и временных ресурсов для различных услуг.

2. Ощутимое увеличение пропускной способности – предполагается трехкратный рост эффективности использования спектра сигнала в 5G в сравнении с сервисами eMBB [3]. С целью повышения пропускной способности в сетях 5G предусматривается уменьшить защитные интервалы [4].

3. Поддержка асинхронной передачи данных. В сетях 4G при асинхронной передаче данных базовая станция постоянно синхронизируется с абонентским оборудованием для уменьшения взаимных помех между несущими частотами (*inter-carrier interference – ICI*) [4]. При этом потери, вызванные такими помехами, негативно сказываются на различных сервисах, в частности mMTC, которые связаны с массовым подключением абонентов сети. Поддержка сетями 5G асинхронной передачи данных направлена на решение проблем, связанных с ICI и обеспечение работы при множественных подключениях [4].

Как уже отмечалось выше, ортогональное частотное уплотнение (OFDM) - это схема доступа, которая используется в современных сетях 4G. Для обеспечения доступа к сети используются два отдельных сигнала - сигнал OFDM в нисходящем канале и сигнал множественного доступа с частотным уплотнением и одной несущей (SC-FDMA) в восходящем канале. Преимущества данной схемы связаны с возможностью передачи сигналов на множестве несущих. Данная схема (OFDM) имеет целый ряд недостатков, в частности:

– высокую чувствительность к частотным сдвигам и сдвигам тактовой частоты; – высокое отношение пикового уровня мощности сигнала к среднему пик-фактору (PAPR);

– снижение спектральной эффективности ввиду использования защитных интервалов;

– чувствительность к эффекту Доплера;

– перекрытие полос поднесущих, приводящие к появлению межбитовой интерференции;

– чувствительность к нелинейностям усилителей и смещению постоянной составляющей при использовании быстрого преобразования Фурье.

Кроме того, чувствительность к частотным сдвигам и сдвигам тактовой частоты обуславливает необходимость периодического добавления сигналов синхронизации в общий объем используемых сигналов и требует синхронизации работы устройства и сети перед началом сеанса связи (обмена данными). А отсутствие непрерывности (фазовый переход) между двумя символами во время генерации символов OFDM инициирует спектральные скачки в частотной области, что приводит к интенсивным внеполосным излучениям.

Ограниченные возможности сигналов на основе схемы OFDM модуляции стали предпосылкой для продолжения исследований с целью выбора кандидатов сигналов для последующих поколений (стандартов) сетей мобильной связи, в частности 5G. В связи с этим, одной из актуальных задач, подлежащих решению, является выполнение требования существенного сокращения задержки при введении в перечень услуг перспективных сетей связи новых служб и приложений. Наряду с этим, появляется необходимость в формировании циклического префикса и уменьшении длительности символов. Эти соображения привели к созданию целого ряда технологий формирования сигналов:

– с обобщенным частотным уплотнением (GFDM);

– с несколькими несущими на базе набора фильтров (FBMC);

– OFDM с временным разделением (w-OFDM);

– универсальный фильтруемый сигнал с несколькими несущими (UFMC);

– ортогональное мультиплексирование с частотным разделением каналов с фильтрованием F-OFDM и др.

Также проводятся исследования новых схем множественного доступа, в том числе: множественного доступа с разреженным кодом (SCMA), неортогонального множественного доступа (NOMA) и множественного доступа с распределением ресурсов (RSMA).

Технология UFMC [13], в значительной степени, рекомендована для преодоления проблемы интерференции (ICI) при множественном доступе пользователей в режиме асинхронной передачи и основана на частотном разделении и мультиплексировании посредством применения операции фильтрации группы поднесущих. UFMC является обобщенной версией техники фильтрования множества боковых полос (БП). Боковые полосы обрабатываются фильтром одновременно, вместо обработки каждой БП в отдельности. Таким образом уменьшаются взаимные помехи для БП в сравнении с традиционным OFDM. Также, применение операций фильтрации БП нацелено на увеличение эффективности ряда приложений коммуникаций, например, таких как системы с сверхмалой задержкой пакетов. Данный вид модуляции оказывается более предпочтительным для подобных приложений по отношению к схеме модуляции FBMC.

FBMC является одним из наиболее известных форматов модуляции с расширением спектра в беспроводных коммуникациях [14]. Данная модуляция обеспечивает значительное преимущество в формировании каждой поднесущей и облегчает гибкое использование спектрального ресурса, позволяет удовлетворить различным системным требованиям, таким как низкая задержка, множественный доступ и другие, что приводит к улучшению показателей помехозащищенности системы в условиях рассеивания сигнала во временной и частотной областях [15]. Так, например прямоугольные фильтры более предпочтительны для каналов, распределенных во времени, в то время как фильтр с характеристикой типа «приподнятый косинус» более устойчив против частотного рассеивания. Однако, несмотря на все очевидные выгоды, получаемые при использовании FBMC, значительная длина фильтров приводит к возникновению следующих последствий: – большой длительности символа, что является проблемой не только для приложений с требованиями малой задержки или большим количеством пользователей в коммуникациях; – увеличению вычислительной сложности для технологии MIMO детектирования. Указанные обстоятельства, в конечном итоге, ведут к проблемам в работе всех основных приложений 5G.

GFDM является блоковой схемой модуляции с частотным уплотнением каналов, разработанной для работы с разнообразными приложениями 5G, обеспечивая изменяемую форму сигнала [16]. Для улучшения показателей надежности и задержки в коммуникациях без коррекции ошибок, можно использовать GFDM сигналы вместе с преобразованием Уолша-Адамара. При комбинировании GFDM с квадратурной амплитудной модуляцией, в системах с множественным доступом, решается проблема внутрисистемных помех при условии использования неортогональных фильтров. С другой точки зрения, GFDM можно рассматривать в качестве схемы с гибкой настройкой отдельных блоков, а не только лишь одной несущей в целом. При манипуляции соответствующих параметров сигнала GFDM, возможно получение различных форм сигнала таких как OFDM, частотное выравнивание с единой несущей (SC-FDE) и др. Несмотря на весьма перспективные возможности, которые открываются благодаря применению сигналов с GFDM, данный вид модуляции является вычислительно сложным [16].

F-OFDM применяется к каналу нисходящей линии связи 4G. Для F-OFDM сконфигурированный фильтр применяется к символу OFDM во временной области для снижения уровня внеполосного излучения сигнала поддиапазона, сохраняя ортогональность комплексных доменов OFDM-символов. Поскольку полоса пропускания фильтра соответствует полосе пропускания сигнала, затрагиваются только несколько поднесущих, близких к краю. Основное соображение заключается в том, что длина фильтра может превышать длину циклического префикса для F-OFDM [6]. При этом снижается уровень межсимвольной интерференции, что обусловлено выбранной конструкцией фильтра с использованием оконной обработки (с мягким усечением). Генерация F-OFDM сигнала основана на формировании блока из M близлежащих БП в ряде последовательных OFDM символов [17]. В частности, во время обработки каждого символа, в передатчике формируются параметры: значение размерности обратного быстрого преобразования Фурье (ОБПФ) равное N, длительность M «информационных символов» вместе с циклическим префиксом, где $N > M$. Информационные символы могут быть

точками созвездий (*constellation points*) как в OFDM. Аналитически указанное можно представить в следующем виде:

$$s(n) = \sum_{l=0}^{L-1} s_l(n - l(N + Ng)) \tag{1}$$

и

$$S_l(n) \equiv \sum_{m=m`}^{m`+M-1} d_{l,m} e^{j2\pi mn/N}, -N_g \le n < N, \tag{2}$$

где Ng – длина циклического префикса (CP), d - информационный символ поднесущей m OFDM системы, L обозначает количество OFDM символов, а $\{m_0, m_{0+1}, \ldots, m_{0+M-1}\}$ - выбранный набор поднесущих. Сигнал F-OFDM формируется при обработке сигнала s(n) с помощью соответствующего фильтра, т.е.

$$\tilde{s}(n) = s(n) * f(n). \tag{3}$$

Пропускная способность фильтра равна сумме пропускной способности выбранных БП, а временные затраты - это длительность символа OFDM. В приемнике полученный сигнал сначала проходит через фильтр f (−n), который идентичен фильтру передатчика. Принятый сигнал обрабатывается с использованием стандартных OFDM преобразований, а затем отфильтрованный сигнал разделяется на последовательность отдельных OFDM символов с удалением циклического префикса. При этом к каждому символу применяется БПФ размерности N и далее выделяют информационные символы из соответствующих поднесущих.

Фильтр для F-OFDM должен удовлетворять следующим критериям: иметь плоскую полосу пропускания по поднесущим в поддиапазоне; иметь острую переходную полосу для минимизации защитных полос. Данные критерии соответствуют фильтру с прямоугольным частотным откликом. Чтобы удовлетворять указанным требованиям, фильтр нижних частот реализуется с помощью «окна», которое эффективно обрезает импульсную характеристику и обеспечивает плавные переходы к нулю на обоих концах [18] Таким образом, реализация F-OFDM привносит дополнительно, к существующей процедуре обработки CP-OFDM, этап фильтрации, причем, как на стороне передачи, так и на стороне приема.

Технология W-OFDM. Для уменьшения внеполосного излучения сигналов используется оконная обработка временного сигнала, окном типа «приподнятый косинус». Известно, что спектр OFDM сигнала имеет множество боковых лепестков, которые медленно затухают в частотной области, что приводит к увеличению внеполосного излучения. Для снижения внеполосного излучения OFDM-символа используют защитные поднесущие, которые добавляют по краям OFDM сигнала. С этой же целью применяется оконная обработка сигнала. Такая обработка сигнала позволяет осуществлять плавный переход между окончанием предыдущего и началом последующего символа. Такой переход осуществляется с помощью перекрытия во времени префикса текущего символа и суффиксом предыдущего символа посредством их суммирования. Окно «приподнятый косинус» имеет вид

$$h(t) = \begin{cases} 1, 0 \le |t| \le \dfrac{T(1-\beta)}{2}; \\ \dfrac{1}{2}\left(1 + \cos\left[\dfrac{\pi}{\beta + T}\left(|t| - \dfrac{T(1-\beta)}{2}\right)\right]\right), \ \dfrac{T(1-\beta)}{2} \le |t| \le \dfrac{T(1+\beta)}{2}; \\ 0, \end{cases} \tag{4}$$

где T – длительность символа, β – спад, принимающий значения в интервале от 0 до 1.

Для данной технологии важным является выбор длительности окна спада. Значение длительности окна приподнятого косинуса необходимо выбирать равной или меньшей длительности циклического префикса. В этом случае применение оконной обработки для формирования символов OFDM позволяет значительно снизить внеполосное излучение. Кроме того, на уровень внеполосного излучения оказывает влияние и выбор защитного интервала между

поднесущими. Так, например, как утверждает группа исследователей в работе [19], чем длиннее защитный интервал, тем меньше уровень внеполосного излучения.

4 Выводы

В работе представлен краткий обзор технологий формирования сигналов, используемых в современных системах связи и телекоммуникаций, а также проведен анализ перспективных технологий, которые, потенциально могут найти свое применение в перспективных системах, в том числе беспроводных системах связи широкополосного доступа.

Подчеркнуто, что широко известная схема модуляции OFDM имеет ряд недостатков, которые могут привести к снижению показателей эффективности систем, в которых она применяется. К основным из недостатков следует отнести:

- снижение помехоустойчивости приема сигналов, обусловленное воздействием межсимвольных и межканальных помех;
- OFDM сигнал имеет относительно высокое значение пик-фактора, что приводит к чрезмерным энергетическим затратам.

Рассмотрены известные альтернативные технологии формирования сигналов, в частности, технология формирования сигналов, основанная на оконной обработке сигналов, обеспечивающая низкий уровень внеполосных излучений.

Ссылки

[1] Gorbenko I.D., Zamula A.A., Semenko Ye.A. Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications // Telecommunications and Radio Engineering. - Volume 75, 2016 Issue 2, pages 169-178.
[2] I.D. Gorbenko, A.A. Zamula Cryptographic signals: requirements, methods of synthesis, properties, application in telecommunication systems Telecommunications and Radio Engineering. - Volume 76, 2017 Issue 12, pages 1079-1100.
[3] ITU-R, Recommendation M.2083-0, “IMT Vision - Framework and overall objectives of the future development of IMT for 2020 and beyond”, ITU recommendation, Sept. 2015.
[4] Pen Guan et. al., “5G Field Trials: OFDM-Based Waveforms and Mixed Numerologies” IEEE Journal on Selected Areas in Communications, vol. 35, no. 6, pp. 1234-1243, March 2017.
[5] T. S. Rappaport, et al., “Millimeter Wave Mobile Communications for 5G Cellular: It Will Work!”, IEEE Access, vol. 1, pp. 335-349, 2013.
[6] J.G. Andrews, et al., “What will 5G be?”, IEEE Journal on Selected Areas in Communications, vol. 32, no. 6, pp. 1065-1082, June 2014.
[7] J. Abdoli, et al., “Filtered OFDM: A new waveform for future wireless systems”, Proc. IEEE SPAWC, pp. 66-70, Jun. 2015.
[8] X. Zhang, et al., “Filtered-OFDM – Enabler for Flexible Waveformin The 5th Generation Cellular Networks”, Proc. IEEE GLOBECOM, pp. 1-6, Dec. 2015.
[9] Li, Jialing, et al., “A resource block based filtered OFDM scheme and performance comparison”, Proc. IEEE ICT, pp. 1-5, May 2013.
[10] T. L. Marzetta, “Noncooperative Cellular Wireless with Unlimited Numbers of Base Station Antennas”, IEEE Transactions on Wireless Communications, vol. 9, no. 11, pp. 3590-3600, Nov. 2010.
[11] China Mobile Research Institute, “C-RAN: The Road Towards Green RAN”, white paper, 2011. [Online]. Available: http://labs.chinamobile.com/cran/.
[12] H. Nikopour, et al., “Sparse code multiple access”, Proc. IEEE PIMRC, pp. 332-336, Sept. 2013.
[13] 5G Forum. (2016, Mar.). 5G white paper: 5G vision, requirements, and enabling technologies [Online]. Available: http://kani.or.kr/5g/whitepaper/5G%20Vision,%20Requirements,%20and%20Enabling%20Technologies.pdf
[14] B. Farhang Boroujeny,“Filter bank multicarrier modulation: a waveform candidate for 5G and beyond,”Advances in Electrical Engineering, vol. 2014, Dec. 2014. doi:10.1155/2014/482805.
[15] Zekeriyya Esat Ankaralı et. al., “Enhanced OFDM for 5G RAN”, June 2017, doi: 10.3969/j. issn. 1673-5188. 2017. S1. 002.
[16] A. Şahin, I. Güvenç and H. Arslan,“A survey on multicarrier communications: prototype filters, lattice structures, and implementation aspects, ”IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1312-1338, Aug. 2014. doi:10.1109/SURV.2013.121213.00263
[17] Huawei and HiSilicon, “f-OFDM scheme and filter design,”3GPP Standard Contribution (R1‑165425), Nanjing, China, May 2016”.
[18] R1-165425. "F-OFDM scheme and filter design." 3GPP TSG RAN WG1 meeting 85. Huawei; HiSilicon. May 2016.
[19] V.P. Fedosov, D.G. Kovtun, A.A. Legin, A.V. Lomakina Issledovanie modeli OFDM signala s malym urovnem vnepolosnogo izlucheniya / Izvestiya YuFU. Tekhnicheskie nauki. 2016, S. 6-16.

Reviewer: Vyacheslav Kharchenko, Doctor of Technical Sciences, Professor, Academician of the Academy of Sciences of Applied Radio Electronics, National Aerospace University named after. M. E. Zhukovsky, Kharkiv, Ukraine.
E-mail: v_s_kharchenko@ukr.net

Received: December 2017

Authors:
Zamula Alexandr, Doctor of Technical Sciences, Professor of the Department of Information Systems and Technologies Security, V. N. Karazin Kharkiv National University, 4 Svobody Sq., Kharkiv, 61022, Ukraine.
E-mail: zamylaaa@gmail.com

Morozov Vladislav, postgraduate student of the Department of Information Systems and Technologies Security, V. N. Karazin Kharkiv National University, 4 Svobody Sq., Kharkiv, 61022, Ukraine.
E-mail: morozov@boiko.com.ua

Methods for forming and processing OFDM signals in modern wireless discrete communication systems.

Abstract. The considers technologies of signal generation used in communication and telecommunication systems, as well as provides an brief analysis of promising technologies that can be used in wireless broadband access communication systems. It is shown that the widely used OFDM modulation scheme has a number of shortcomings that can lead to a decrease in the system efficiency indicators. Are presented alternative signal generation technologies, in particular, technology W-OFDM, which eliminate the known shortcomings of OFDM technology.

Keywords: multiple access, cellular communication, frequency separation, noise immunity, interference, window processing, peak factor, modulation.

Рецензент: Вячеслав Харченко, д.т.н., проф., академік Академії наук прикладної радіоелектроніки, Національний аерокосмічний університет ім. М. Є. Жуковського, Харків, Україна.
E-mail: v_s_kharchenko@ukr.net

Надійшло: Грудень 2017.

Автори:
Олександр Замула, доктор технічних наук, професор кафедри безпеки інформаційних систем і технологій, Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, м. Харків, 61022, Україна.
E-mail: zamylaaa@gmail.com

Владислав Морозов, аспірант кафедри безпеки інформаційних систем і технологій, Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, м. Харків, 61022, Україна.
E-mail: morozov@boiko.com.ua

Методи формування і обробки OFDM сигналів в сучасних бездротових дискретних комунікаційних системах.

Анотація. У статті розглянуті технології формування сигналів, використовуваних в системах зв'язку і телекомунікацій, а також наводиться короткий аналіз перспективних технологій, які можуть знайти застосування в бездротових системах зв'язку широкосмугового доступу. Показано, що широко використовувана схема модуляції OFDM має низку недоліків, які можуть призвести до зниження показників ефективності систем. Представлені альтернативні технології формування сигналів, зокрема, технологія W-OFDM, що усувають відомі недоліки технології OFDM.

Ключові слова: множинний доступ, стільниковий зв'язок, частотне розділення, завадостійкість, інтерференція, віконна обробка, пік-фактор, модуляція.

UDC 004.056.55

ALGEBRAIC IMMUNITY OF SYMMETRIC CIPHERS

Aleksandr Kuznetsov[1], Roman Serhiienko[2], Dmytro Prokopovych-Tkachenko[3], Yuri Tarasenko[3], Ivan Belozertsev[1]

[1] V. N. Karazin Kharkiv National University, Svobody sq., 6, Kharkiv, 61022, Ukraine
kuznetsov@karazin.ua, ivanbelozersevv.jw@gmail.com

[2] National Army Academy named after Hetman Petro Sahaidachnyi, 32 Heroes of Maidan street, Lviv, 79012, Ukraine
romanserg69@gmail.com

[3] University of Customs and Finance, 2/4 Volodymyr Vernadsky str., Dnipro, 49000, Ukraine
omega2@email.dp.ua, me_dnepr@ua.fm

Reviewer: Anton Alekseychuk, Doctor of Sciences (Engineering), Full Prof., National Technical University of Ukraine "Kyiv Polytechnic Institute", Prosp. Peremohy, 37, Kyiv, 03056, Ukraine
alex-dtn@ukr.net

Received on November 2017

Abstract. *A key component of modern symmetric ciphers are nonlinear blocks (non-linear substitutions, substitution tables, S-boxes) that perform functions of hiding statistical links of plaintext and ciphertext, mixing and disseminating data, and introducing nonlinearity into the encryption procedure to counter various crypto-analytical and statistical attacks. The effectiveness of a symmetric cipher, its resistance to the majority of known cryptographic attacks and the level of information technology security provided by it directly depend on the performance of nonlinear nodes (balance, nonlinearity, autocorrelation, correlation immunity etc.). In this paper various methods for calculating algebraic immunity are examined, their interrelation is studied, and the results of comparative studies of the algebraic immunity of nonlinear blocks of the most well-known modern symmetric ciphers are presented.*

Keywords: *symmetric ciphers, algebraic immunity, nonlinear substitution blocks.*

1 Introduction

Cryptographic transformation plays an important role in ensuring the security of modern information systems and technologies [1, 2]. Symmetric ciphers because of their simplicity, efficiency and multifunctionality are used in almost all modern cryptographic protocols, and also as an integral part of other cryptographic primitives: hashing, pseudorandom sequence generation, password generation etc. Consequently, analysis and investigation of methods for synthesizing symmetric cryptographic primitives, the development and theoretical justification of criteria and performance indicators, including individual units of modern cyphers is important and relevant scientific and technical problem.

A key component of modern symmetric ciphers are nonlinear blocks (non-linear substitutions, substitution tables, S-boxes) that perform functions of hiding statistical links of plaintext and ciphertext, mixing and disseminating data, and introducing nonlinearity into the encryption procedure to counter various crypto-analytical and statistical attacks. Thus, the effectiveness of a symmetric cipher, its resistance to the majority of known cryptographic attacks and the level of information technology security provided by it directly depend on the performance of nonlinear nodes (balance, nonlinearity, autocorrelation, correlation immunity etc.).

Certain indices of the effectiveness of non-linear blocks of symmetric ciphers were considered in [3-9]. The concept of algebraic immunity was first introduced in [10,11] for estimating the stability of Boolean functions to the so-called algebraic cryptanalysis, proposed in [12]. In [13] these positions were generalized for Boolean mappings (S-blocks), to calculate algebraic immunity, the mathematical apparatus of Gröbner bases is used.

In this paper various methods for calculating algebraic immunity are examined, their interrelation is studied, and the results of comparative studies of the algebraic immunity of nonlinear blocks of the most well-known modern symmetric ciphers are presented.

2 Algebraic immunity of Boolean functions

The concept of algebraic immunity was first introduced in [10,11] and is considered in detail in the dissertation [14]. We introduce the definitions and notations necessary for the subsequent discussion, following the formulations adopted in [14].

Let $GF(2)$ be a binary field and $GF(2)^n$ – n-dimensional vector space over $GF(2)$.

Boolean function $f(x)$ of n variables is a mapping $f(x):GF(2)^n \to GF(2)$ where $x=(x_1,...,x_n)$.

Truth table of a Boolean function $f(x)$ of n variables is a binary output vector of the values of the function that contains 2^n elements, each element belongs to the set {0, 1}.

Algebraic normal form (Zhegalkin polynomial) of a Boolean function $f(x)$ of n variables is denoted in form:

$$f(x)=a_0 \oplus a_1x_1 \oplus a_2x_2 \oplus ... \oplus a_nx_n \oplus a_{12}x_1x_2 \oplus a_{13}x_1x_3 \oplus ... \oplus a_{(n-1)n}x_{n-1}x_n \oplus ... \oplus a_{123...n}x_1x_2x_3...x_n,$$

where the coefficients $a_i \in \{0,1\}$ and each Boolean function is implemented by the Zhegalkin polynomial uniquely, i.e. each representation of $f(x)$ corresponds to a unique truth table.

Algebraic degree $Deg(f)$ of a Boolean function $f(x)$ is a the number of variables in the longest term of the algebraic normal form of a function having a nonzero coefficient a_i. At the same time we consider $Deg(0)=0$.

Let's denote as V_n the set of all mappings $GF(2)^n \to GF(2)$, i.e. this is the set of all possible Boolean functions $f(x)$ of n variables.

The set V_n we will consider both as the ring of Boolean functions and as a vector (linear) space over the binary field, i. e. $V_n = GF(2)^{2^n}$.

The Boolean function $g \in V_n$ is called the *annihilator* of a function $f \in V_n$, if $f \cdot g = 0$ or $(f+1) \cdot g = 0$.

The set of distinct annihilators of a Boolean function $g(x)$ forms a linear space, let's denote it by $Ann(f)=\{g \in V_n \mid f \cdot g = 0\}$.

Let's denote the linear space of annihilators of degree $\le d$ as

$$A_d^n(f)=\{g \in V_n \mid f \cdot g = 0, Deg(g) \le d\} \subset Ann(f).$$

The concept of annihilators of Boolean functions is closely related to the evaluation of the effectiveness of algebraic cryptanalysis of stream ciphers [10]. In particular, when using a filtering generator (see Fig. 1) of pseudo-random sequences (PRS) the search for the initial state of the linear feedback shift register (LFSR) is associated with a decrease in the degree of the joint system of polynomial Boolean equations.

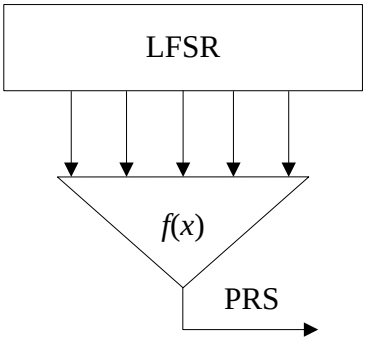

Fig. 1 – Block diagram of the filter generator PRS

Algorithm of algebraic cryptanalysis proposed in [10] allows under certain conditions, regarding the part of the intercepted output sequence (PRS), to find the initial state of the LFSR with time complexity $O\left((S_n^d)^3\right)$, where

$$S_n^d = \sum_{i=0}^{d} \frac{n!}{i!(n-i)!}$$

and d is the least degree of the non-zero annihilator of the filtering Boolean function $f(x)$ or its inversion $f(x)+1$.

Thus, the aim of algebraic cryptanalysis is the search for nonzero annihilators, or at least an estimation of their minimal degree. To this end, the definition of *algebraic immunity* $AI(f)$ of a Boolean function $f \in V_n$ was introduced in [11]:

$$AI(f) = \min\{Deg(g) \mid g \in Ann(f) \text{ or } g \in Ann(f+1)\}.$$

The value of $AI(f)$ is numerically equal to the minimal degree of such a Boolean function $g \in V_n$, that $f \cdot g = 0$ or $(f+1) \cdot g = 0$.

Using the concept of a linear space of annihilators of degree $\le d$ let's denote:

$$AI(f) = \min\{d \mid A_d^n(f) \neq 0 \text{ или } A_d^n(f+1) \neq 0\}, \quad (1)$$

i.e. for evaluating the algebraic immunity of a Boolean function $f \in V_n$ it suffices to find a nonzero basis of the space of annihilators of the least degree of d.

The value d allows to quantify the complexity of algebraic cryptanalysis and, if sufficiently large d, to guarantee the resistance of a stream cryptographic algorithm to an algebraic attack.

Algorithm for computing the algebraic immunity of Boolean functions. One of the algorithms for calculating the algebraic immunity of Boolean functions is presented in the thesis [14]. It is based on the construction of a basis for the linear space of annihilators $A_d^n(f)$ of a given degree d. By increasing d iteratively and repeating the construction of the basis of the space $A_d^n(f)$, we obtain the $AI(f)$ estimation by the formula (1), i.e. through a nonzero basis of annihilators of the least degree.

It is necessary to introduce the following additional notation for description the essence of the algorithm.

Let's denote a monomial with respect to variables $x_1, ..., x_n$ as

$$x^u = \prod_{i=1}^{n} x_i^{u_i} = \begin{cases} x_i, u_i = 1, \\ 1, u_i = 0, \end{cases}$$

where vectors $x, u \in V_2^n, x = (x_1, ..., x_n), u = (u_1, ..., u_n)$.

The degree of the monomial x^u is determined by the Hamming weight (the number of nonzero coordinates) $w_h(u)$ of the vector $u = (u_1, ..., u_n)$, i.e.

$$Deg(x^u) = w_h(u).$$

Taking these notations into account, the Boolean function $f(x)$ in algebraic normal form (in the form of Zhegalkin polynomial) can be written in the form

$$f(x) = \sum_{u \in GF(2)^n} a_u x^u, \; a_u \in GF(2). \quad (2)$$

The function (annihilator) $g \in A_d^n(f)$ can also be represented it in the form of Zhegalkin polynomial

$$g(x) = \sum_{v \in GF(2)^n : w_h(v) \le d} b_v x^v , \quad (3)$$

where $b_v \in GF(2)$ – unknown annihilator coefficients, $w_h(v)$ – Hamming weight of the vector $v = (v_1, ..., v_n)$. The function g belongs to the space $A_d^n(f)$ only if equality $f(x) \cdot g(x) = 0$ holds for any $x \in GF(2)^n$.

By substituting (2) and (3) we obtain

$$f(x) \cdot g(x) = \left(\sum_{u \in GF(2)^n} a_u x^u \right) \left(\sum_{v \in GF(2)^n : w_h(v) \le d} b_v x^v \right) = \sum_{u \in GF(2)^n} \left(\sum_{v \in GF(2)^n : w_h(v) \le d} a_u b_v x^{u \vee v} \right) = 0 ,$$

where $u \vee v = (u_1 \vee v_1, ..., u_n \vee v_n)$, $\vee$ – disjunction (logical OR operation).

After grouping the terms by the common factor, we obtain the equality:

$$\sum_{w \in GF(2)^n} \left(\sum_{a_u, b_v : a_u \vee b_v = w} a_u b_v \right) x^w = 0 , \quad (4)$$

which holds for any $w \in GF(2)^n$. Consequently, a system of linear homogeneous equations is obtained

$$\left\{ \sum_{a_u, b_v : a_u \vee b_v = w} a_u b_v = 0 , \ \forall w \in GF(2)^n \right. \quad (5)$$

relatively unknown coefficients b_v of annihilation $g(x)$.

The solution of the system (5), for example, by the Gauss method, determines the basis of the space $A_d^n(f)$.

Pattern. For $n = 2$ and $d = 1$

$$f(x) = a_{00} + a_{10} x_1 + a_{01} x_2 + a_{11} x_1 x_2 ,$$
$$g(x) = b_{00} + b_{10} x_1 + b_{01} x_2 .$$

After substitution $f(x) \cdot g(x) = 0$ it follows

$$f(x) \cdot g(x) = a_{00} b_{00} + (a_{00} b_{10} + a_{10} b_{10} + a_{10} b_{00}) x_1 + (a_{00} b_{01} + a_{01} b_{01} + a_{01} b_{00}) x_2 +$$
$$+ (a_{10} b_{01} + a_{01} b_{10} + a_{11} b_{00} + a_{11} b_{10} + a_{11} b_{01}) x_1 x_2 = 0,$$

from which it comes to a system of linear homogeneous equations:

$$\begin{cases} a_{00} b_{00} = 0, \\ a_{00} b_{10} + a_{10} b_{10} + a_{10} b_{00} = 0, \\ a_{00} b_{01} + a_{01} b_{01} + a_{01} b_{00} = 0, \\ a_{10} b_{01} + a_{01} b_{10} + a_{11} b_{00} + a_{11} b_{10} + a_{11} b_{01} = 0 \end{cases}$$

relatively unknown b_{00}, b_{10}, b_{01} – coefficients of the function $g(x)$.

Then, for example, for the function $f(x) = x_1 + x_2$ (i.e. for $a_{00} = a_{11} = 0$ and $a_{10} = a_{01} = 1$) we've got the system:

$$\begin{cases} b_{10} + b_{00} = 0, \\ b_{01} + b_{00} = 0, \\ b_{01} + b_{10} = 0, \end{cases}$$

which satisfies only two solutions:

$$b_{00} = b_{10} = b_{01} = 0, \text{ i.e. } g(x) = 0,$$
$$b_{00} = b_{10} = b_{01} = 1, \text{ i.e. } g(x) = 1 + x_1 + x_2.$$

A close inspection shows that $g(x) = 1 + x_1 + x_2$ is indeed an annihilator of the function $f(x) = x_1 + x_2$:

$$f(x) \cdot g(x) = (x_1 + x_2)(1 + x_1 + x_2) = x_1 + x_2 + x_1 + x_1x_2 + x_1x_2 + x_2 = 0.$$

Summarizing the aforesaid, we define the basic steps of **the algorithm for finding the basis of the annihilator space** [14].

Input: $n \in \mathrm{N}, d \in \{1,...,n\}$, function $f(x)$ (given by a list of monomials x^u with nonzero coefficients a_u in (2)).

Output: Linear space $A_d^n(f)$ given in the form of a parametric family of Zhegalkin polynomials in n Boolean variables of degree $\le d$.

Step 1. Represent the functions $f(x)$ and $g(x)$ in the form of the sums (2) and (3), respectively.

Step 2. Expand the brackets in the product $f(x) \cdot g(x)$ and, by grouping the summands $a_u b_v x^w$ by sorting them by $a_u \vee b_v = w$, obtain the equation (4).

Step 3. Compose a system of linear homogeneous equations (5).

Step 4. Find the general solution of the system (5) in parametric form and feed it to the output of the algorithm.

The dissertation [14] gives an estimate $O\left(m \cdot \left(S_n^d\right)^3\right)$ of the bit complexity of the considered algorithm, where m is the number of non-zero coefficients a_u in (2).

Using the considered above algorithm for searching the basis of the annihilator space, we can calculate the algebraic immunity of a Boolean function $f(x)$ by sequentially scanning all the values $d > 0$ until we obtain a nonzero space of annihilators $A_d^n(f)$ or $A_d^n(f+1)$. The minimum value, for which $A_d^n(f) \neq 0$ and/or $A_d^n(f+1) \neq 0$, corresponds to the value of the algebraic immunity of a Boolean function $f(x)$.

Algorithm for calculating algebraic immunity $AI(f)$.

Input: $n \in \mathrm{N}$, function $f(x)$ (given by a list of monomials x^u with nonzero coefficients a_u in (2)).

Output: The value of Algebraic Immunity $AI(f)$.

Step 1. Assign $d = 1$.

Step 2. Calculate the space of annihilators $A_d^n(f)$ and $A_d^n(f+1)$.

Step 3. If $A_d^n(f) = 0$ and $A_d^n(f+1) = 0$ assign $d = d + 1$ and go to step 2.

Step 4. If $A_d^n(f) \neq 0$ and/or $A_d^n(f+1) \neq 0$ assign $AI(f) = d$ and feed it to the output of the algorithm.

3 Algebraic immunity of Boolean mappings (S-boxes)

The concept of algebraic immunity of Boolean functions in [13] is generalized to the case of Boolean mappings $F : GF(2)^n \to GF(2)^n$ (*vector Boolean functions*), which are implemented by substitution blocks (substitution tables, S-boxes) of block symmetric ciphers. To determine the algebraic immunity $AI(F)$ we'll use the terms and definitions from [15].

Let state the natural numbers n, m, and the field K. Let consider a finite system S of m algebraic equations

$$\begin{cases} P_1(x_1, x_2, ..., x_n) = 0, \\ P_2(x_1, x_2, ..., x_n) = 0, \\ ... \\ P_m(x_1, x_2, ..., x_n) = 0 \end{cases} \quad (6)$$

of variables $x_1, x_2, ..., x_n$ with coefficients over the field K.

Let $K[x_1, x_2, ..., x_n]$ is the set of all polynomials in variables $x_1, x_2, ..., x_n$ with coefficients over the field K. On this set the operations of addition and multiplication are defined, and the set itself is called the *polynomial ring*. This ring is commutative (for any elements $a, b \in K[x_1, x_2, ..., x_n]$ holds the equality $a \cdot b = b \cdot a$), with an identity (for all $a \in K[x_1, x_2, ..., x_n]$ holds the equality $a \cdot e = a$, where $e = 1$).

A nonempty subset I of a commutative ring with identity R is called an *ideal* in R (denoted as $I \lhd R$) if the following two conditions are satisfied:

– for any elements $a, b \in I$ element $a - b \in I$;

– for any $a \in I$ и $c \in R$ element $a \cdot c \in R$.

Elements $a_1, a_2, ..., a_k$ constitute the *basis of the ideal*

$$I = (a_1, a_2, ..., a_k) = \{a_1 \cdot r_1 + a_2 \cdot r_2 + ... + a_k \cdot r_k; r_1, r_2, ..., r_k \in R\} \subseteq R.$$

It is said that an ideal $I \lhd R$ *admits a finite basis* if it contains elements $a_1, a_2, ..., a_k$ such that $I = (a_1, a_2, ..., a_k)$.

The fundamental ***Hilbert's basis theorem*** states that each ideal $I \lhd K[x_1, x_2, ..., x_n]$ admits a finite basis, i.e. there are such $f_1(x_1, x_2, ..., x_n)$, $f_2(x_1, x_2, ..., x_n)$, …, $f_k(x_1, x_2, ..., x_n) \in I$, that

$$I = (f_1, f_2, ..., f_k) = \{f_1 \cdot r_1 + f_2 \cdot r_2 + ... + f_k \cdot r_k; r_1, r_2, ..., r_k \in K[x_1, x_2, ..., x_n]\}.$$

Let associate with the system S (6) the ideal I, generated by the polynomials $P_1(x_1, x_2, ..., x_n)$, $P_2(x_1, x_2, ..., x_n)$, …, $P_m(x_1, x_2, ..., x_n)$, corresponding to the equations of the system:

$$I(S) = (P_1, P_2, ..., P_m) = \{P_1 \cdot r_1 + P_2 \cdot r_2 + ... + P_m \cdot r_m; r_1, r_2, ..., r_m \in K[x_1, x_2, ..., x_n]\}.$$

If $F \in I(S)$, then for each solution $(X_1, X_2, ..., X_n)$ of system (6) holds the equality

$$\begin{aligned} &F(X_1, X_2, ..., X_n) = \\ &= P_1(X_1, X_2, ..., X_n) \cdot r_1(X_1, X_2, ..., X_n) + P_2(X_1, X_2, ..., X_n) \cdot r_2(X_1, X_2, ..., X_n) + ... + \\ &+ P_m(X_1, X_2, ..., X_n) \cdot r_m(X_1, X_2, ..., X_n) = \\ &= 0 \cdot r_1(X_1, X_2, ..., X_n) + 0 \cdot r_2(X_1, X_2, ..., X_n) + ... + 0 \cdot r_m(X_1, X_2, ..., X_n) = 0. \end{aligned}$$

If $\{P_1, P_2, ..., P_m\}$ and $\{\overline{P}_1, \overline{P}_2, ..., \overline{P}_k\}$ both are two bases of the same ideal I, then the system of algebraic equations

$$\begin{cases} P_1(x_1, x_2, ..., x_n) = 0, \\ P_2(x_1, x_2, ..., x_n) = 0, \\ ... \\ P_m(x_1, x_2, ..., x_n) = 0, \end{cases} \qquad \begin{cases} \overline{P}_1(x_1, x_2, ..., x_n) = 0, \\ \overline{P}_2(x_1, x_2, ..., x_n) = 0, \\ ... \\ \overline{P}_k(x_1, x_2, ..., x_n) = 0 \end{cases}$$

are equivalent, that is the sets of their solutions coincide.

Consequently, the set of solutions of a system of algebraic equations is uniquely determined by the ideal of the system, and the various bases of the same ideal correspond to equivalent systems [15].

Suppose that there is a certain polynomial $h(x_1, x_2, ..., x_n) \in K[x_1, x_2, ..., x_n]$ and it is required in a finite number of steps to find out whether it belongs to an ideal $I \lhd K[x_1, x_2, ..., x_n]$ given by its basis $I = (f_1, f_2, ..., f_m)$. In other words, it is necessary to solve the so-called *problem of occurrence*: to find out whether there exist such polynomials $r_1(x_1, x_2, ..., x_n)$, $r_2(x_1, x_2, ..., x_n)$, …, $r_m(x_1, x_2, ..., x_n)$, that $h = f_1 \cdot r_1 + f_2 \cdot r_2 + ... + f_m \cdot r_m$ and $h \in I = (f_1, f_2, ..., f_m)$.

The problem of occurrence is solved by simplifying the expression for $h(x_1, x_2, ..., x_n)$ using so called *reduction of a polynomial*. Let's write the polynomial $h(x_1, x_2, ..., x_n)$ as the sum: $h = h_C + h_M$, where h_C – senior monomial, and h_M – the sum of the remaining monomials in h. Suppose also that h_C is divisible by the leading term f_{iC} of one of the polynomials f_i, i.e. $h_C = f_{iC} \cdot Q$ and $h = f_{iC} \cdot Q + h_M$ for some monomial Q. Then the *operation of reduction* is given by

$$h_1 = h - f_i \cdot Q = f_{iC} \cdot Q + h_M - f_{iC} \cdot Q - f_{iM} \cdot Q = h_M + (-f_{iM}) \cdot Q,$$

where f_{iM} - the sum of the remaining monomials in $f_i = f_{iC} + f_{iM}$. Herewith the leading term of the polynomial h_1 is less than the leading term of the polynomial h. If a polynomial h belongs to an ideal $I = (f_1, f_2, ..., f_m)$, then the reduced polynomial h_1 will also belong to this ideal. Indeed if $h \in (f_1, f_2, ..., f_m)$ then $h - h_1 = f_i Q \in (f_1, f_2, ..., f_m)$. Consequently, the problem of occurrence can now be solved no longer for a polynomial h, but for a reduced polynomial h_1. If for a finite number of reductions the polynomial h is reduced to zero (zero belongs to any ideal), then $h \in (f_1, f_2, ..., f_m)$.

Basis $f_1, f_2, ..., f_m$ of ideal $I = (f_1, f_2, ..., f_m)$ is called ***the Gröbner basis*** of this ideal if every polynomial $h \in I$ reduces to zero by means of $f_1, f_2, ..., f_m$. In other words the set of polynomials $f_1, f_2, ..., f_m$ is a Gröbner basis in the ideal $I = (f_1, f_2, ..., f_m)$ if for any $h \in I$ monomial h_C is divisible by one of the monomials $f_{1C}, f_{2C}, ..., f_{mC}$ [15].

For the operation of reduction of polynomials the concept of the leading term is used. In other words, it is assumed that on a set of all monomials of the ring $K[x_1, x_2, ..., x_n]$ the *linear order* (monomial ordering $\prec$) is given that satisfies the properties [16]:

– it follows from $x^u \prec x^v$ that $x^w \cdot x^u \prec x^w \cdot x^v$ for any monomials x^u, x^v, x^w (monomials are defined as (2), i.e. $x, u, v, w \in V_2^n, x = (x_1, ..., x_n), u = (u_1, ..., u_n), v = (v_1, ..., v_n), w = (w_1, ..., w_n)$);

– $1 \preceq x^v$ for any monomial x^u.

Some examples of monomial ordering are cited below:

– *dictionary* or *lexicographic order (lex)*: $x^u \prec_{\text{lex}} x^v$, if such i exists that $u_i < v_i$ and $u_j = v_j$ for $j < i$ (first the variables in monomials in the alphabetical order are ordered, and then the first difference in monomials is found);

– *degree lexicographic order (deglex)*: $x^u \prec_{\text{deglex}} x^v$, if $w_h(u) < w_h(v)$ or $w_h(u) = w_h(v)$, but with that $x^u \prec x^v$ in the alphabetical order (ordered by the sum of powers, in the case of equality of sums – by alphabetical order);

– *degree reverse lexicographic order (degrevlex)*: $x^u \prec_{\text{degrevlex}} x^v$, if $w_h(u) < w_h(v)$ or $w_h(u) = w_h(v)$, but with that $x^u \succ_{\text{lex}} x^v$ in the alphabetical order (ordered by the sum of powers, in the case of equality of sums – by reverse alphabetical order).

The solution of the problem of occurrence, i.e. the ascertainment of membership of a polynomial h to an ideal $I=(f_1, f_2,..., f_m)$, consists in constructing all possible reductions h by means of elements of the Gröbner basis of the ideal I. A polynomial h belongs to an ideal $I=(f_1, f_2,..., f_m)$ if and only if a zero is obtained as a result of reduction [15].

For each ideal $I \lhd K[x_1, x_2,..., x_n]$ there exists a Gröbner basis, and the construction of the Gröbner basis itself is based on the resolving the linkage [15]. The polynomials f_i and f_j have a linkage if their leading terms are both divisible by a non-constant monomial ω. Let $f_{iC}=\omega\cdot q_1$, $f_{jC}=\omega\cdot q_2$, where ω – the greatest common divisor of leading terms f_{iC} and f_{jC}. Let's consider the monomial $F_{i,j}=f_i\cdot q_2-f_j\cdot q_1\in I$ and reduce it using a basis $f_1, f_2,..., f_m$ as long as possible. If the resulting polynomial $F'_{i,j}\equiv 0$, then they say the linkage is solvable. Otherwise, the resulting polynomial $f_{m+1}=F'_{i,j}$ should be added to the basis $f_1, f_2,..., f_m$ of the ideal I after which the procedure for finding and reducing of linkage will be continued. After reducing the finite number of linkages a set $f_1, f_2,..., f_m, f_{m+1},..., f_M$ is obtained in which every linkage is solvable.

In accordance with the ***diamond lemma***, the basis $f_1, f_2,..., f_m$ of an ideal $I \lhd K[x_1, x_2,..., x_n]$ is a Gröbner basis only if there are no unsolvable linkages in it [15].

The resolving of the linkage allows to define the effective algorithm for constructing the Gröbner basis of the ideal $I=(f_1, f_2,..., f_m)$ (***Buchberger's algorithm***).

Step 1. Check whether the linkage in the set $f_1, f_2,..., f_m$ exists. If there are no linkages, then the set $f_1, f_2,..., f_m$ is a Gröbner basis of the ideal $I=(f_1, f_2,..., f_m)$. If linkages exist then go to step 2.

Step 2. Form a polynomial $F_{i,j}=f_i\cdot q_2-f_j\cdot q_1$ with linkage of the polynomials f_i and f_j found in previous step and reduce it by means of a set $f_1, f_2,..., f_m$ as long as this is possible. If the polynomial is reduced to a nonzero polynomial f_{m+1} go to step 3, otherwise go to step 4.

Step 3. Add the polynomial f_{m+1} to the set $f_1, f_2,..., f_m$ and go to step 4.

Step 4. Pick up linkage didn't examined previously and go to step 2. If all the linkages are processed, then we derive the resulting set $f_1, f_2,..., f_m, f_{m+1},..., f_M$ in which all the linkages are solvable. This is the Gröbner basis of ideal $I=(f_1, f_2,..., f_m)$.

To date, other algorithms for constructing the Gröbner basis are known, for example algorithms F4, F5 [17,18]. The Gröbner basis can be simplified in the following methods [15].

1. *Minimization of the Gröbner basis*. If f_i and f_j are two elements of the Gröbner basis, with their leading terms f_{iC} and f_{jC} that are divisible by each other, for example, $f_{jC}\,|\,f_{iC}$, then the polynomial f_i can be removed from the set $f_1, f_2,..., f_m$. The Gröbner basis is called *minimal* if f_{iC} it is not divisible by f_{jC} for all $i\neq j$.
2. *Reduction of the Gröbner basis*. If some member q of the polynomial f_i is divisible by the leading term of the polynomial f_j, then we reduce q it with f_j and use the result of reduction to replace the term q in the polynomial f_i. In this case the Gröbner basis remains a Gröbner basis, the number of elements of the basis does not change, however the degrees of the polynomials $f_1, f_2,..., f_m$ decrease. The Gröbner basis is said to be *reduced* if no member of the polynomial f_i is divisible by the leading term of the polynomial f_j for all $i\neq j$.

The minimal reduced Gröbner basis of the ideal $I \lhd K[x_1, x_2,..., x_n]$ is uniquely defined (with unit coefficients at the highest powers of the basis elements), that is, it doesn't depend on the initial basis of the ideal $I=(f_1, f_2,..., f_m)$ and on the sequence of operations performed (but depends on

the ordering of the variables $x_1, x_2, ..., x_n$) [15]. The concept of a minimal reduced Gröbner basis is used in the work of Jean-Charles Faugère [13] to determine the algebraic immunity of S-blocks (nonlinear complication nodes) of block symmetric ciphers. Let consider a non-linear block (S-box) of the block symmetric cipher (see Fig. 2), which implements the Boolean mapping $S : GF(2)^n \to GF(2)^m$ [1-9].

S-box is defined by a system of algebraic equations over a binary field:

$$\begin{cases} f_1(x_1, x_2, ..., x_n) = y_1, \\ f_2(x_1, x_2, ..., x_n) = y_2, \\ ... \\ f_m(x_1, x_2, ..., x_n) = y_m, \end{cases} \quad (7)$$

i.e. a collective of Boolean polynomials

$$\begin{array}{c} y_1 - f_1(x_1, x_2, ..., x_n), \\ y_2 - f_2(x_1, x_2, ..., x_n), \\ \ldots, \\ y_m - f_m(x_1, x_2, ..., x_n) \end{array} \quad (8)$$

in the ring $K[x_1, x_2, ..., x_n, y_1, y_2, ..., y_m]$ of variables $x_1, x_2, ..., x_n, y_1, y_2, ..., y_m$ with coefficients over the field $K = GF(2)$.

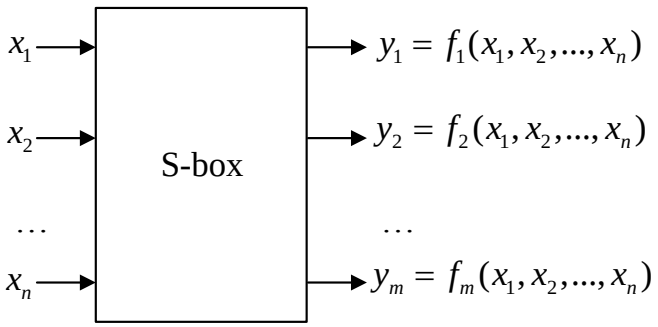

Fig. 2 – Block diagram of a non-linear block of a block symmetric cipher

With the system of equations (7), algebraically defining the structure of an S-block, we associate the ideal I generated by the polynomials (8):

$$I(S) = (y_1 - f_1(x_1, x_2, ..., x_n), y_2 - f_1(x_1, x_2, ..., x_n), ..., y_m - f_m(x_1, x_2, ..., x_n)) =$$
$$= \{(y_1 - f_1) \cdot r_1 + (y_2 - f_1) \cdot r_2 + ... + (y_m - f_m) \cdot r_m; r_1, r_2, ..., r_m \in GF(2)[x_1, x_2, ..., x_n, y_1, y_2, ..., y_m]\}.$$

Algebraic immunity of a non-linear block of a block symmetric cipher is defined as the minimal degree of a polynomial P in an ideal $I(S)$ [13]:

$$AI(S) = \min\{\deg(P), P \in I(S) \lhd GF(2)[x_1, x_2, ..., x_n, y_1, y_2, ..., y_m]\}, \quad (9)$$

and the minimal reduced Gröbner basis of the ideal $I(S)$ for a degree reverse lexicographic order (*degrevlex*) contains a linear basis of polynomials P in $I(S)$, such that $AI(S) = \deg(P)$. In other words, to calculate algebraic immunity $AI(S)$ it is sufficient to construct a minimal reduced Gröbner basis of the ideal $I(S)$ given by equations (8) and to find a polynomial of minimal degree among the elements of this basis. The value of the minimum degree is the value of the algebraic immunity $AI(S)$ of the block symmetric cipher substitution box (S-box).

The link between the algebraic immunity of the S-block (9) and the Boolean function (1) is shown in [19, p. 337]. Consider a Boolean function $f_S(x_1, x_2, ..., x_n, y_1, y_2, ..., y_m): GF(2)^{2n} \to GF(2)$ whose values are defined as follows:

$$f_S(x_1, x_2, ..., x_n, y_1, y_2, ..., y_m) = \begin{cases} 1, \forall i, j: f_i(x_1, x_2, ..., x_n) = y_j, \\ 0, \exists i, j: f_i(x_1, x_2, ..., x_n) \neq y_j. \end{cases}$$

The set of solutions of equation

$$f_S(x_1, x_2, ..., x_n, y_1, y_2, ..., y_m) - 1 = 0$$

coincides with the set of solutions of system (7). Consequently, there are different bases $(f_S - 1)$ and $(y_1 - f_1, y_2 - f_1, ..., y_m - f_m)$ of one ideal of equivalent systems, i.e.

$$I(f_S - 1) = I(y_1 - f_1, y_2 - f_1, ..., y_m - f_m).$$

Ideal of the space of annihilators $Ann(f_S)$ in the ring $GF(2)[x_1, x_2, ..., x_n, y_1, y_2, ..., y_m]$ coincides with the ideal $I(f_S - 1)$, hence, the algebraic immunity (9) of the Boolean mapping $S: GF(2)^n \to GF(2)^m$ coincides with the minimal degree of nonzero polynomials belonging to the annihilator of the function f_S:

$$AI(S) = \min\{D\text{eg}(g) \mid g \in Ann(f_S)\}.$$

Thus, any S-block can be unambiguously described by a Boolean function [19], the algebraic immunity of this function can be calculated, for example, using the algorithm of paragraph 2.

4 Values of algebraic immunity of nonlinear blocks of modern ciphers

In this paper comparative studies of the algebraic immunity of nonlinear blocks of modern symmetric ciphers have been carried out. As objects of research, well-known and standardized on the national and/or international level block symmetric crypto-transformations are chosen:

- cryptographic algorithm AES, standardized in the US as a federal data processing standard FIPS-197 [20], and also internationally as a block cipher in ISO / IEC 18033-3 [21];
- cryptographic algorithm Camellia, standardized internationally as a block cipher in ISO/IEC 18033-3 [21];
- cryptographic algorithm CAST, standardized internationally as a block cipher in ISO/IEC 18033-3 [21];
- cryptographic algorithm SEED, standardized internationally as a block cipher in ISO/IEC 18033-3 [21];
- cryptographic algorithm “Kalyna”, national standard of Ukraine DSTU 7624:2014 [22];
- cryptographic algorithm “Kuznechik”, standardized in Russia as GOST 34.12-2015 [23];
- algorithm of symmetric encryption and integrity control “BelT”, the Republic of Belarus, standardized in STB 34.101.31-2011 [24];
- cryptographic hash function Whirlpool, based on block symmetric crypto-transformations, standardized internationally in ISO/IEC 10118-3:2004 [25].

To calculate algebraic immunity the expression (9) was used. For immediate calculations, the Magma software package [26] is used, which implements a wide range of functions related to algebra, group theory, rings and fields, number theory and many other branches of mathematics.

The tested blocks of the replacements, except for the S-block of the hash function of Whirlpool, were considered in detail in work [9], table 1 shows some results of the research.

The following notations [9] are used in the table:

- B – balance;
- N – non-linearity;

– A – autocorrelation;
– AD – algebraic degree;
– PC –propagation criterion;
– CI – correlation immunity.

Table 1 – Cryptographic properties of non-linear blocks of block ciphers

	B	N	A	AD	PC	CI	AI
AES	+	112	32	7	0	0	2
SEED	–	110	40	7	0	0	2
CAST-128	–	120	0	4	8	0	2
“Camellia”	+	112	32	7	0	0	2
“Kalina”	+	104	72	7	0	0	3
“Kuznechik”	+	102	72	7	0	0	3
“BelT”	+	104	72	7	0	0	3
“Whirlpool”	+	95	80	7	0	0	3

In the last column “AI” of Table 1 the values of the algebraic immunity of nonlinear substitution blocks of modern ciphers are listed. These data are obtained from (9) by constructing Gröbner bases of ideals $I(S)$ given by sets of polynomials (8) from equations (7) of the corresponding S-blocks.

The results obtained are indicative of the insufficient algebraic immunity of nonlinear boxes of block ciphers, which were developed in the late 90s – early 2000s. The algorithms considered (AES, SEED, CAST-128, “Camellia”), represented in the modern international standard ISO / IEC 18033-3, have relatively low algebraic immunity and can potentially be considered as real targets for constructing effective algebraic attacks.

Block symmetric crypto algorithms “Kalyna”, “Kuznechik”, “BelT”, as well as cryptographic function of hashing of Whirlpool, are developed taking into account the possible algebraic attacks. Nonlinear substitution blocks of these algorithms have high algebraic immunity and, apparently, will remain resistant to new methods of algebraic cryptanalysis.

5 Conclusion

Methods of algebraic cryptanalysis since early publications [27,28] have turned from abstract and inapplicable mathematical ideas into a developed section of modern cryptology that is widely discussed in the scientific community. To date, a huge number of research projects have been carried out in this field of knowledge, and obviously, in the coming years, effective algorithms for algebraic cryptanalysis of modern symmetric ciphers should appear.

In this paper some aspects of algebraic cryptanalysis were considered, in particular, methods for calculating the algebraic immunity of non-linear blocks of symmetric ciphers were studied. This concept first was introduced for stream cryptoalgorithms in [10,11], and was generalized in [13] to Boolean mappings, i.e. nonlinear blocks with arbitrary dimension of inputs and outputs. Algebraic immunity, in some sense, characterizes the complexity of solving a system of equations describing a non-linear block and thus allows one to obtain an idea of the resistance of a symmetric cipher to algebraic cryptanalysis. In particular, the algorithm of algebraic cryptanalysis of stream ciphers with filter-generator scheme was proposed in [10]. Complexity of implementing this algorithm is a function of the value of algebraic immunity of a cryptographic Boolean function.

The calculation of the algebraic immunity of a nonlinear block in the general case is associated with the construction of the Gröbner basis of the ideal of the polynomial ring given by polynomials from the equations of the permutation block. This problem is solved by computationally effective algorithms of Buchberger, F4, F5, etc. [15-18]. Moreover, the considered mathematical methods can also be used to search for effective algebraic attacks [19], which confirms the perspective and

relevance of ongoing research in this field.

In this paper the algebraic immunity values substitution boxes of some modern ciphers are given. In particular, it was found out that the cryptoalgorithms developed at the end of the 90s – the beginning of the 2000s do not have the ultimate values of algebraic immunity, i.e. can be considered as targets for potential effective algebraic attacks. Block ciphers of the latest generation ("Kalina", "Kuznechik", "BelT") were developed taking into account the possible application of algebraic cryptanalysis and have uttermost values of algebraic immunity.

A promising direction is further research on methods of algebraic cryptanalysis, in particular, the use of quantum computing technologies to solve systems of algebraic equations that describe a symmetric cipher. According to the authors of this work, in this direction of research the most significant and interesting scientific results are expected.

References

[1] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography – CRC Press, 1997. – 794 p.

[2] Gorbenko I.D., Gorbenko Y.I. Applied cryptology. Theory. Praxis. Exploitation: Textbook for higher educational institutions. – Kharkiv: Publishing house "Fort", 2013. – 880 p.

[3] Bart Preneel. Analysis and Design of Cryptographic Hash Functions. [Electronic resource] – Access mode: homes.esat.kuleuven.be/~preneel/phd_preneel_feb1993.pdf.

[4] Carlet C. Vectorial Boolean functions for // Cambridge Univ. Press, Cambridge. – 95 p. [Electronic resource] – Access mode: www.math.univ-paris13.fr/~carlet/chap-vectorial-fcts-corr.pdf.

[5] Carlet C. Boolean functions for cryptography and error correcting codes // Cambridge Univ. Press, Cambridge. – 2007. – 148 p. [Electronic resource] – Access mode: www1.spms.ntu.edu.sg/~kkhoongm/chap-fcts-Bool.pdf.

[6] Zhuo Zepeng, Zhang Weiguo On correlation properties of Boolean functions // Chinese Journal of Electronics. Jan, Vol.20, 2011, №1, 143-146 pp.

[7] O'Connor L. An analysis of a class of algorithms for S-box construction // J. Cryptology. -1994. – p. 133-151.

[8] Clark J.A., Jacob J.L., Stepney S. The Design of S-Boxes by Simulated Annealing // New Generation Computing. – 2005. – 23(3). – p.219–231.

[9] Kuznetsov A.A., Bielozertsev I.N., Andrushkevich A.V. Analysis and comparative studies of nonlinear substitution blocks of modern block symmetric ciphers // Applied electronics. – Kharkiv: KhNURE. – 2015. – Vol. 14. №4. – p. 343 – 350.

[10] Courtois N., Meier W. Algebraic Attacks on Stream Ciphers with Linear Feedback, Eurocrypt 2003, LNCS 2656, Springer, 2003. – pp. 345-359.

[11] Meier W., Pasalic E., Carlet C: Algebraic Attacks and Decomposition of Boolean Functions, Eurocrypt 2004, LNCS 3027, Springer, 2004. – pp. 474-491.

[12] Nicolas Courtois; Josef Pieprzyk (2002). "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations". LNCS. 2501: 267–287.

[13] Gw´enol´e Ars, Jean-Charles Faug`ere. Algebraic Immunities of functions over finite fields. [Research Report] RR-5532, INRIA. 2005, pp.17.

[14] Bayev Vladimir Valerievich. Effective algorithms for obtaining estimates of the algebraic immunity of Boolean functions: a thesis for the degree of candidate of physical and mathematical sciences: 01.01.09 / Bayev Vladimir Valerievich; [Institution of defense of a thesis: Moskow state university]. - Moskow, 2008. - 101 p.

[15] I.V. Arzhantsev. Gröbner bases and systems of algebraic equations. Summer school. Modern mathematics. Dubna, Yuly 2002. – Moskow: MCNMO, 2003. – 68 p.

[16] AI Zlobin, O. Sokolova. Computer algebra in the Sage system. Tutorial. - Moscow: MSTU named after Bauman, 2011. – 55 p.

[17] Faugère, J.-C. (June 1999). A new efficient algorithm for computing Gröbner bases (F4). Journal of Pure and Applied Algebra. Elsevier Science. 139 (1): 61–88.

[18] Faugère, J.-C. (July 2002). A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). Proceedings of the 2002 international symposium on Symbolic and algebraic computation (ISSAC). ACM Press: 75–83.

[19] Massimiliano Sala, Teo Mora, Ludovic Perret, Shojiro Sakata, Carlo Traverso Gröbner Bases, Coding, and Cryptography. Springer-Verlag Berlin Heidelberg. – 426 p.

[20] FIPS 197. National Institute of Standards and Technology. [Electronic resource]: Advanced Encryption Standard. – 2001. – Available at: http://www.nist.gov/aes.

[21] ISO/IEC 18033-3. Information technology – Security techniques – Encryption algorithms, Part 3: Block ciphers, 80 p.

[22] DSTU 7624:2014. Information technology. Cryptographic security of information. The algorithm of symmetric block transformation. – Kyiv: Ministry of economic development of Ukraine, 2015. – 238 p.

[23] GOST R 34.12-2015. Information technology. Cryptographic security of information. Block ciphers. – Moscow: Standartinform, 2015. – 25p.

[24] STB 34.101.31-2011. Information technology and security. Cryptographic algorithms for encryption and integrity control. – Minsk: Gosstandart, 2011. – 32 p.

[25] ISO/IEC 10118-3:2004. Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions, 94 p.

[26] Magma Computational Algebra System. Available at: http://magma.maths.usyd.edu.au/magma.

[27] Nicolas Courtois, Alexander Klimov, Jacques Patarin, Adi Shamir. Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. Proceeding EUROCRYPT'00 Proceedings of the 19th international conference on Theory and application of cryptographic techniques. P. 392-407.

[28] Nicolas Courtois, Josef Pieprzyk. Cryptanalysis of Block Ciphers with Overdefined Systems of Equations. Advances in cryptology – ASIACRYPT 2002. P.267-287.
[29] Andrey Pyshkin. Algebraic Cryptanalysis of Block Ciphers Using Grobner Bases. Dissertation zur Erlangung des Grades Doktor rerum naturalium. Technischen Universit¨at Darmstadt. – Darmstadt, 2008, 118 p.

Рецензент: Антон Олексійчук, д.т.н., доцент, Інститут спеціального зв'язку та захисту інформації національного технічного університету України «КПІ», пр. Перемоги, 37, г. Киев, 03056, Україна.
E-mail: alex-dtn@ukr.net

Надійшло: Листопад 2017.

Автори:
Олександр Кузнецов, д.т.н., проф., академік Академії наук прикладної радіоелектроніки, Харківський національний університет ім. В. Н. Каразіна, пл. Свободи, 6, Харків, 61022, Україна. E-mail: kuznetsov@karazin.ua

Роман Сергієнко, Національна академія сухопутних військ імені гетьмана Петра Сагайдачного, вул. Героїв Майдану, 32, м. Львів, 79026, Україна. E-mail: romanserg69@gmail.com

Дмитро Прокопович-Ткаченко, Університет митної справи та фінансів, вул. Володимира Вернадського, 2/4, м. Дніпро, 49000, Україна. E-mail: omega2@email.dp.ua

Юрій Тарасенко, Університет митної справи та фінансів, вул. Володимира Вернадського, 2/4, м. Дніпро, 49000, Україна.
E-mail: me_dnepr@ua.fm

Іван Білозерцев, студент, Харківський національний університет імені В.Н. Каразіна, пл. Свободи, 6, Харків, 61022, Україна.
E-mail: ivanbelozersevv.jw@gmail.com

Алгебраїчний імунітет симетричних шифрів.

Анотація. Ключовим компонентом сучасних симетричних шифрів є нелінійні вузли (нелінійні підстановки, таблиці замін, S-блоки), які виконують функції приховування статистичних зв'язків відкритого тексту і шифртекста, перемішування і розсіювання даних, внесення нелінійності в процедуру шифрування для протистояння різним криптоаналітичних і статистичними атакам. Від показників ефективності нелінійних вузлів (збалансованості, нелінійності, автокореляції, кореляційної імунності та ін.) безпосередньо залежить ефективність симетричного шифру, його стійкість до більшості відомих криптографічних атак і рівень забезпечуваної безпеки інформаційних технологій. У даній роботі розглядаються різні методи розрахунку алгебраїчного імунітету, вивчається їх взаємозв'язок і наводяться результати порівняльних досліджень алгебраїчної імунності нелінійних вузлів найбільш відомих сучасних симетричних шифрів.

Ключові слова: симетричні шифри, алгебраїчний імунітет, нелінійні блоки підстановки.

Рецензент: Антон Алексейчук, д.т.н., доцент, Институт специальной связи и защиты информации национального технического университета Украины «КПИ», пр. Победы, 37, г. Киев, 03056, Украина.
E-mail: alex-dtn@ukr.net

Поступила: Ноябрь 2017.

Авторы:
Александр Кузнецов, д.т.н., проф., академик Академии наук прикладной радиоэлектроники, Харьковский национальный университет им. В. Н. Каразина, пл. Свободы, 6, Харьков, 61022, Украина. E-mail: kuznetsov@karazin.ua

Роман Сергиенко, Национальная академия сухопутных войск имени гетмана Петра Сагайдачного, ул. Героев Майдана, 32, г. Львов, 79026, Украина. E-mail: romanserg69@gmail.com

Дмитрий Прокопович-Ткаченко, Университет таможенного дела и финансов, ул. Владимира Вернадского, 2/4, г. Днепр, 49000, Украина. E-mail: omega2@email.dp.ua

Юрий Тарасенко, Университет таможенного дела и финансов, ул. Владимира Вернадского, 2/4, г. Днепр, 49000, Украина.
E-mail: me_dnepr@ua.fm

Иван Белозерцев, студент, Харьковский национальный университет имени В.Н. Каразина, пл. Свободы, 6, Харьков, 61022, Украина. E-mail: ivanbelozersevv.jw@gmail.com

Алгебраический иммунитет симметричных шифров.

Аннотация. Ключевым компонентом современных симметричных шифров являются нелинейные узлы (нелинейные подстановки, таблицы замен, S-блоки), которые выполняют функции скрытия статистических связей открытого текста и шифртекста, перемешивания и рассеивания данных, внесения нелинейности в процедуру зашифрования для противостояния различным криптоаналитическим и статистическим атакам. От показателей эффективности нелинейных узлов (сбалансированности, нелинейности, автокорреляции, корреляционной иммунности и пр.) непосредственно зависят эффективность симметричного шифра, его устойчивость к большинству известных криптографических атак и уровень обеспечиваемой им безопасности информационных технологий. В данной работе рассматриваются различные методы расчета алгебраического иммунитета, изучается их взаимосвязь и приводятся результаты сравнительных исследований алгебраической иммунности нелинейных узлов наиболее известных современных симметричных шифров.

Ключевые слова: симметричные шифры, алгебраический иммунитет, нелинейные блоки подстановки.

UDC 004.9: 621.391.7

METHODS OF ENSURING ELECTROMAGNETIC COMPATIBILITY IN MODERN INFORMATION COMMUNICATION SYSTEMS

I. Gorbenko, V. Morozov, A. Zamula

V. N. Karazin Kharkiv National University, Svobody sq.,4, Kharkov, 61022, Ukraine
gorbenkoi@iit.kharkov.ua, morozov@boiko.com.ua, zamylaaa@gmail.com

Reviewer: Alexey Stakhov, Doctor of Sciences (Engineering), Full Prof., Academicians of the Academy of Engineering Sciences of Ukraine, International Club of the Golden Section, 6 McCreary Trail, Bolton, Ont., L7E 2C8, Canada
goldenmuseum@rogers.com

Received on September 2017

Abstract. *Requirements are formulated for the choice of complex signals systems – data carriers for use in multi-user broadband telecommunication systems (BTS), which are increased requirements for noise immunity, electromagnetic compatibility, stealth operation and information security data. Conceptual bases are presented of synthesis for a new class of complex signals – cryptographic signals (CS). The justified advisability of application of CS protected BTS, including the construction of derivative signal systems to improve the performance of noise immunity, interference immunity, electromagnetic compatibility transmission security and information security data in protected BTS.*

Keywords*: multi-user system; the Euclidean distance; the signal ensemble; cryptographic signal; orthogonal signal derivative signal system; the correlation function.*

1 Introduction

In the conditions of the development of modern technologies, the commissioning of new control and communication systems, as well as the development of computer and information technologies, a single information and telecommunication space is being created that covers many countries, a gradual transition of communication and automation systems to modern digital ways of transmitting and processing information, automation of management processes is carried out. Moreover, the requirements for electromagnetic compatibility of systems and facilities, integrity, reliability, confidentiality, data authenticity in the process of their storage, transmission and processing are constantly increasing, especially in critical systems of state and regional level. The fulfillment of these requirements is inextricably linked with the need to generalize the already accumulated world experience in the field of information communications and completely depends on the degree of deployment of advanced information technologies for the information transmission and processing.

The rapid growth of information communications and the continuous development of technical means for their provision contribute to the fact that setting the tasks of managing telecommunications networks, traffic, information security, services and quality of service are substantially changing. Meanwhile, such indicators of the effectiveness of information communications systems (ICS), such as electromagnetic compatibility, noise immunity, information security, depend to a significant extent on the properties of physical carriers of information – signals.

Electromagnetic compatibility (EMC) implies the conflict-free existence of various radio engineering systems. Obviously, it is impossible to completely exclude the mutual influence of different systems, the functioning of which is carried out in some relatively small area (*for example, frequency domain*). The task of the system's developer (user), e.g. telecommunications systems, is the elimination or reduction to an acceptable level of undesirable effects of the system, e.g. electromagnetic waves, on other systems. To the ICS, increasingly stringent requirements for ensuring the efficiency of operation in conditions of complex external influences: natural and deliberate interference, interference from other radio systems operating at close frequencies or in the general section of the frequency range.

Modern wireless ICS (*e.g. cellular and satellite systems*), refer to multi-user systems. In such systems, a plurality of channels is located within a common frequency-time resource, so that each

subscriber is able to transmit and receive information simultaneously with and independently of other subscribers. When designing such systems, the main problem is the choice of the multiple access method, i.e., the possibility of simultaneous use by many subscribers of the communication channel with minimal mutual influence. If it is necessary to service a large number of subscribers, the time-frequency resource should be significant. One of the problems of multi-user systems is the need to effectively use the frequency band, ensuring the maximum density of radio engineering means per unit bandwidth. This raises another problem of electromagnetic compatibility of radio equipment (subscribers) operating in the general frequency band allocated for the system. One of the methods for increasing the efficiency of using the frequency range in terms of electromagnetic compatibility is the use of code division of channels (subscribers) operating in the common frequency band, also known as code division multiple access (CDMA). With this method of information transfer, each subscriber is allocated in a wideband signal (signature) from a plurality of orthogonal signals, and each signal occupies the entire band and the entire time interval. In this case, when a user signal occupies both the entire available band and the entire time interval, that is, the need to apply an orthogonal multiple access scheme in which all user signals are broadband. Such a multi-user system will have all the advantages of broadband technology [1]. In an asynchronous multiple access method with CDMA, the delays of various signals at the input of the receiver can vary over a wide range. In this case, the procedure for synchronizing broadband signals (signatures) becomes problematic. This is due to the fact that the signatures of different subscribers, having overlapping spectrum, cannot remain orthogonal in a wide range of mutual delays. The consequence of this is the occurrence of an inter-user interference (*multiple-access interference*), the manifestation of which is the non-zero response of the receiver tuned to the i-th subscriber from the signals of other subscribers. For applications of telecommunication systems in which an asynchronous method with CDMA is used, the choice of signals must be made in such a way as to minimize mutual interference, i.e. ensure electromagnetic compatibility. In particular, such user signals (signatures) must have special properties of mutually correlating functions.

2 The problem of electromagnetic compatibility in information systems

When studying the EMC problem, we will assume that there are two parties involved in the information exchange process. The first of these is the system that carries out the data transfer (*let's call it the "radiating system"*). The second is the system adjacent to the first (the "interacting" system). For the radiating system, the signals of the interacting system can be interpreted as interference (*narrowband, broadband, structural, retransmitted, etc.*). We also assume that the most characteristic type of interference acts in the channel, described by a Gaussian random process whose spectrum coincides with the signal spectrum. With this approach, the error probability depends only on the ratio q^2 of the signal to the total interfering effect. The indicated parameter is found from the relation [1]:

$$q^2=2E/N_0+P_п/F, \quad (1)$$

where: E – signal energy; N_0 – spectral power density of thermal noise; $P_п$ – interference power; F – bandwidth.

The term $P_п/F$ – in fact, an additional white Gaussian noise with spectral density $P_п/F$.

As follows from the relation (1), the use of broadband technology (*broadband signals*) allows successfully solving the problems of EMC systems and withstanding interference effects. It is quite obvious that the wider the signal bandwidth F, the smaller the additional spectral density (*at a constant value of the interference power P_n*) and, thus, the ratio q^2 of the signal powers to the common interfering effect is greater. It is extremely important, from the EMC point of view, that the peak signal power may be limited by the relevant international and national regulatory documents, and the extension of the signal band is realized not by increasing the signal duration, resulting in a decrease in signal energy and value q^2.

Broadband (interference) interference affects the signal as an additional white Gaussian noise with a power spectral density $N_п=P_п/F$. In this case, the ratio $q^2_п$ the signal powers to the total inter-

fering effect at the output of the matched filter of the radiating system will be estimated from the relation

$$q^2_{п}=2E/N_0+N_{п}=2E/N_0+P_{п}/F. \quad (2)$$

The last relation coincides with the relation (1). The only difference is that the interacting system, the spectrum of which completely coincides with the signal spectrum of the radiating system, can realize a much greater suppression effect in comparison with white Gaussian noise. In the case where the ratio $P_{п}/F$ much bigger $N_{0,}$ expression (2) takes the form

$$q^2=2\cdot E\cdot F/P_{п}=2\cdot P\cdot F\cdot T/P_{п,} \quad (3)$$

where P, T – respectively, the power and duration of the signal of the radiating system.

It follows from (3) that when limiting the peak power of the radiating and interacting systems, the only method of ensuring EMC and noise immunity of data reception is the use of broadband signals, i.e. signals having a large value of the product F·T, the so-called processing gain. The task of the designer of ICS is to select such a processing gain that would provide a sufficiently low level of the power spectral density of the applied signals with respect to the noise spectral density at the input of the receiver of the neighboring system.

The above results are valid for the case when the noise is a normal random process and has a uniform spectral density. The neighboring system can use in the process of information exchange signals similar to those used by the radiating system, from the point of view of the law of manipulation, creating so-called structural interference with an uneven spectrum. Under such conditions of functioning of the ICS, noise immunity is largely determined by the similarity (difference) in signal structures and interference, i.e. the way in which individual elements of a signal are suppressed.

Let the signal power of the radiating system - P_c, and the power of the interfering component produced by the interacting system - $P_{п}$. The power of the signal component at the output of the matched filter at the time of making the decision (reference) is proportional P_c, and the power of the interfering component $P_{П}R^2_{jk}(\tau)$, where $R^2_{jk}(\tau)$ – the cross-correlation function (CCF) of the useful k-th signal and the j-th interfering signal. Value τ is determined by the shift of the CCF relative to the reference time. The signal-to-noise ratio at the output of the optimum reception device will be [2]:

$$q^2(\tau)=\frac{P_c}{P_{п}R^2_{jk}(\tau)}. \quad (4)$$

The smallest signal-to-interference ratio will be

$$q^2(\tau)=\frac{P_c}{P_{п}R^2_{max}(\tau)}, \quad (5)$$

where R_{max} – is a maximum value $R_{jk}(\tau)$.

As follows from (5), in order to ensure a satisfactory EMC and in order to increase the noise immunity of receiving data in multi-user ICS, it is necessary to select signals for which the maximum CCF peaks are minimal.

If the maximum peaks of CCF are reduced to the root-mean-square level $\sigma_{j,k}=\sigma^2$, then the signal-to-interference ratio will be

$$q^2(\tau)=\frac{P_c}{P_{п}}\ \sigma^2\cdot \quad (6)$$

For example, if: $\sigma^2=\frac{1}{2FT}$, then

$$q^2 = \frac{P_c}{P_п} 2FT, \tag{7}$$

where FT=B – signal base.

For discrete phase-shifted signals $\sigma^2 = \frac{l}{2N}$ (N – number of signal elements). For such signals

$$q^2 = \frac{P_c}{P_п} 2N. \tag{8}$$

It follows from formulas (7), (8) that the increase in the signal base increases q^2 (*and hence the noise immunity of the system*). In addition, these expressions indicate the way of ensuring EMC of systems operating in a sufficiently close region. This decrease in the ratio $\frac{P_c}{P_П}$ (*in the case of an increase in the radiation power of the station* ($P_п$)) by increasing the signal base of the radiating system.

Typical for communication theory is the approach of developing an optimal receiver that will restore the information contained in the observed oscillation with the best quality. The determination of the optimal processing algorithm based on the account of the specific properties of the transmitted signal allows one to synthesize, in an optimal way, the signal itself, i.e. choose the best way of its coding and modulation [1-4].

In communication theory, the most common model is a channel with additive white Gaussian noise, in which the probability of a channel transforming a given input signal into an output observation $y(t)$ (transition probability - $P\left[y(t)|S(t)\right]$) exponentially decreases with increasing square of the Euclidean distance between the transmitted signal and the output observation [1]:

$$P\left[y(t)\,|\,S(t)\right] = k\exp\left(-\frac{1}{N_0} d(s,y)\right), \tag{9}$$

where k – constant independent of S(t) and y(t), N_0 – single-sided white noise spectral density.

The Euclidean distance between S(t) and y(t) is defined as

$$d(S,y) = \sqrt{\int_0^T [y(t) - S(t)]^2 dt}. \tag{10}$$

According to relations (9) and (10), the similarity of the signal (the probability that it is converted by the channel into observation y(t)) decreases with increasing Euclidean distance between S(t) and y(t). In the case of equal probability of all source messages, the maximum likelihood criterion (MLE) is the optimal strategy of the observer providing the minimum error in making a decision on the actually transmitted signal. According to this rule, after the y(t) oscillation is accepted, the decision is made in favor of the signal for which the probability of its channel transformation into the received observation y (t) is the largest *(in comparison with the probabilities for other signals*).

In view of the foregoing, the MP solution for the Gaussian channel can be transformed into a minimum distance rule

$$d(S_j, y) = \min d(S_i, y) \Rightarrow H_j, \tag{11}$$

i.e. the decision is made in favor of the signal $S_j(t)$, since it is closest (in the sense of the Euclidean distance) to the observation of y (t) among all possible signals.

Expanding the brackets in (10), we arrive at the relation

$$d^2(S_i, y) = \int_0^T y^2(t)dt - 2\int_0^T y(t)\cdot S(t) + \int_0^T S^2(t)dt = \|y\|^2 - 2Z_i + \|S_i\|^2, \quad (12)$$

where Z_i - correlation between observation of $y(t)$ and i-th signal $S_j(t)$

$$Z_i = (y_i, S_i) = \int_0^T y_i(t)S_i(t)dt. \quad (13)$$

The first term on the right-hand side of relation (12) is fixed for this observation and does not affect the decision which of the signals was adopted. The last term is the energy of the i-th signal E_i. Then, the minimum distance rule (11) can be formulated as a rule of maximum correlation:

$$Z_j - \frac{E_i}{2} = \max(Z_i - \frac{E_i}{2}). \quad (14)$$

which means, in particular, that of M possible signals with the same energy, the one that has the maximum correlation with the observation $y(t)$.

One of the limitations in the synthesis of signals is the dimension of the signal space within which their packaging is carried out. The physical essence of this limitation is due to the practical resource, for example, the bandwidth of the frequency band. If the time-frequency resource in which the M signals can be located is limited by the parameters ΔF a T, accordingly, one of the limitations takes into account the bandwidth savings, while the second reflects the desire to transmit data at an acceptable rate $R=\log M|T$. Then, according to the counting theorem, there is about ΔFT independent samples that can be used in the synthesis of M signals, and each of the signals is treated as a vector in a space of dimensionality $n_S=\Delta FT$.

The problem of selecting a set of signals can be formulated as follows: find in a space of a given dimension n_s a constellation of M vectors satisfying energy constraints and having the maximum possible minimum distance between vectors $dmin=max$. With allowance for expressions (13)–(14), signals with the smallest value of the maximum side lobe are preferred. Thus, the requirements for the best signal can be formulated in the form of the following optimization problem: on the set of all possible sequences of length N with symbols from a pre-selected alphabet, find a sequence or sequences with the minimum value of the maximum lateral lobe of the correlation function.

3 Discrete signals synthesis methods

At present, there are no regular methods for synthesizing discrete sequences (DS) optimal by the minimax criterion. Moreover, it is not possible to answer the question: how well-known signals with a large number of N positions are close to optimal. Therefore, it is urgent to find effective methods for synthesizing DS with good minimax properties.

One of these methods is based on the use of iterative algorithms [2]. With an appropriate choice of the initial approximation and the use of integer optimization with respect to the minimax or medium-level criteria, it is possible to obtain comparatively good signals in this sense. However, the lack of iterative methods is a dependence on the initial approximation, a sharp increase in the calculation time of the signal with increasing N, and the fact that they lead only to a local extremum.

The method of synthesizing DP by means of a homomorphic map of the multiplicative groups of the simple and extended Galois fields with the aid of the K-valued character [3] deserves attention. Studies have shown that with the increase in the field characteristics and the number of classes, the volume of calculations for directional search sharply increases.

Other methods assume the search for the necessary conditions for the existence of a DP with given parameters. An example of such an approach is the following. It is known [1-5] that sequences with a good aperiodic autocorrelation function (ACF) can be found only among sequences with good periodic ACF. At the first stage, a set of candidate sequences with a good periodic ACF is

formed. At the second stage, an exhaustive search is performed by the criterion of the lowest level of the side lobe maximum of aperiodic ACF among all cyclic shifts of one-period segments of candidate sequences. The result of the search is a sequence with a minimum value of the side lobes of aperiodic ACF.

The known methods of synthesis of DP with given correlation functions are almost always based on conducting operations to search through a variety of options for selecting the best result, and for a significant period of DP, the application of such methods becomes problematic.

In multi-user systems with code division, families of discrete signals with special mutual correlation properties are necessary. Synthesis of families of signals with the necessary cross-correlation properties consists in the search for a family of sequences with corresponding mutually correlating functions. In this paper, we present methods that allow the synthesis of systems of nonlinear discrete complex signals with given, for certain ICS applications, correlation, ensemble, and structural properties.

Since the code division is based on the difference in signals, the construction of multi-user systems and their characteristics are determined by the choice of signals and their properties. Usually the number of subscribers is large enough, so the choice of signals for ICS applications (*mobile communication systems, space communication systems, etc.*) is reduced to the synthesis of signal systems with given ensemble, correlation and other properties. The development of multi-user ICS based on code division of signals and led to research in the theory of signal systems.

The appearance in recent years of new areas of use of pseudorandom sequences required an additional and more thorough study of their ensemble, correlation, structural, and other properties. For example, the increased interest in broadband has stimulated the study of aperiodic correlation functions, and not just periodic ones. The application of code division multiplexing methods in systems with multiple access and, as a consequence, the problems of EMC of various systems, required a deeper analysis of the mutual-correlation properties. The necessity to counteract the mutual interfering influence of ICS led to the search (synthesis) of signals with specified correlation, structural, ensemble, technological and other properties.

For most applications, in particular for broadband systems with multiple access, interesting are not pairs, but large sets of sequences with good cross-correlation properties, improved ensemble and structural properties. In some systems, the number of concurrent sequences can exceed several hundred. There are large sets of periodic sequences (Kasami, Gold, etc.), which have comparatively small side lobes of mutual-correlation functions [6-10]. To generate such sequences, shift registers with linear feedback are used. The rules for constructing these classes of sequences indicate a low structural concealment of the generated sequences, and, consequently, signals-physical carriers of information in the ICS.

The need to use protected radio channels forces researchers to look at the modes of functioning of the protected radio channels and the aspects of the formation and application of complex signals in a new way. Therefore, in our opinion, today new approaches and new views are needed on the application processes and functions of complex signals in order to create secure ISS. Fundamental here, in our opinion, is a new understanding of the methods of ensuring information stealth and imitation resistance, that is, functions that are implemented in traditional systems with the use of systems and means of cryptographic information protection [11]. A productive step, from the point of view of a new direction in the use of complex signal systems, is the synthesis of so-called cryptographic signal systems. Synthesis of such signals is based on the use of key data, and at the same time, the signals must possess: absolute structural concealment with respect to the laws of their formation and signal change in a dynamic mode; improved ensemble properties (*exist for almost any period value, have a significant amount of signal system*); necessary to ensure the required value of noise immunity, correlation properties.

The authors formulated and solved the problem of synthesis of nonlinear cryptographic discrete signals (CS) providing the required values of noise immunity, information and structural stealth of the ICS operation [12-13]. In conditions of intensive information counteraction of the parties, interests and competition of which can manifest themselves in various spheres, including, as recent

events have shown, in the sphere of information and hybrid wars, the availability and use of secure ICS is of particular importance. To a significant extent, such systems are based on the use of protected radio channels. At the same time, under the security of systems, it is necessary to understand in a broad sense, first of all, their ability to provide the necessary EMC, noise immunity, imitating, information, energy and structural stealth. Increased requirements for the effectiveness of the operation of ICS in the context of internal and external influences are largely ignored by existing information technologies. There is a contradiction between the stringent requirements for the provision of EMC systems and facilities, reliability, secrecy, confidentiality, integrity of data transmitted via the ICS communication lines, on the one hand, and existing models, methods and technologies of control over ICS, information security (IS), services and quality of service, on the other hand. The main ways to solve this contradiction is to provide EMS systems and tools, increase noise immunity and ISS IR by improving the methodological foundations of ICS construction by creating new models, methods and technologies for managing telecommunications networks, information security, services and quality of service, developing information exchange methods, synthesis methods new classes of nonlinear complex discrete signals – data carriers with the necessary ensemble, correlation and structural properties.

By cryptographic discrete signals (CS) it is proposed to understand a set of sequences (vectors) of symbols of a certain alphabet, which necessarily have the necessary structural, ensemble and correlation properties, temporal and spatial complexity, and the possibility of forming on the basis of keys [12]. Rules for constructing the CS are based on the use of random or pseudo-random processes, which must meet the requirements of randomness, irreversibility, unpredictability, etc. [14].

4 Discrete cryptographic signals model

Let us formulate in general form the problem of synthesis of CS.

The task of constructing (synthesizing) the CS will be understood as the problem of constructing subsets of discrete sequences $(W_l^q), q=\overline{1,N}, l=\overline{1,L}$, the set of which forms a system of discrete signals of a given alphabet of dimension $M_k = N \times L$, such that in each of the subsets (the dictionary) the conditions imposed on the subsets of the CS in terms of structural, ensemble, correlation properties, the spatial and temporal complexity of their generation.

The construction of the CS is based on the analysis and use of periodic and aperiodic correlation functions and reduces to the following stages.

1. Ensuring the conditions for meeting the requirements for structural and ensemble properties, the ability to form a subset of the COP with allowable temporal and spatial complexity, including using keys.

2. Constructing a CS W^q, periodic autocorrelation function (PFAC) of each of which satisfies the system of nonlinear parametric inequalities (NPI):

$$R_{a_1}^q(l) \le \sum_{i=1}^{L} W_i^q (W_{i+l}^q)^* \le R_{a_2}^q(l), \quad l=\overline{1,L-1}, \quad q=\overline{1,N}, \tag{15}$$

where $R_{a_1}^q(l)$ and $R_{a_2}^q(l)$ – given PFAC implementations, and the indices are calculated modulo (*i*+*l*) *mod L*.

If $l=L$ for all $q=\overline{1,N}$ (15) gives convolution with value L:

$$\sum_{i=1}^{L} W_i^q W_{i+L}{}^q = \sum_{i=1}^{L} W_i^q W_i^q = L, q=\overline{1,N}, \tag{16}$$

3. Construction of pairs KC W^q and W^p, the cross-correlation functions (CCF) which satisfy the requirements, which are determined by the set of NPI systems (16), and also meet the requirements for the cross-correlation joint function (CCJF) W^q and W^p concordant discrete words W^{qp} and W^{pq} (17-21):

$$R_{b_{1,1}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^p)^* \le R_{b_{2,1}}^{qp}(l); \quad (17)$$

$$R_{b_{1,2}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^q)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^p)^* \le R_{b_{2,2}}^{qp}(l); \quad (18)$$

$$R_{b_{1,3}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^q)^* \le R_{b_{2,3}}^{qp}(l); \quad (19)$$

$$R_{b_{1,4}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^p \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^p \times (W_{i-l+K}^q)^* \le R_{b_{2,4}}^{qp}(l); \quad (20)$$

$$R_{b_{1,5}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^p \times (W_{i+l}^q)^* + \sum_{i=L-K+1}^{L-1} W_i^p \times (W_{i-l+K}^p)^* \le R_{b_{2,5}}^{qp}(l); \quad (21)$$

Besides, $l=\overline{1,L-1}$ for all kinds of combinations q and p, $q=\overline{1,N}$, $p=\overline{1,N}$, $q \ne p$, where $R_{b_{1,j}}^{qp}(l)$ and $R_{b_{2,j}}^{qp}(l)$, - specified (necessary) implementations PCCF and CCCF respectively ($j=\overline{1,5}$).

In systems NPI (15), (16) and (17–21) W_i^q and W_i^p are unknown values of random or pseudo-random CS symbols W^q and W^p, $q=\overline{1,N}$, which are subject to determination in the process of their construction. In what follows, the systems (15–16) and (17–21) will be called the model of the subset (dictionary) of the CS.

We analyze systems of nonlinear parametric quadratic inequalities (hereinafter systems) (15), (16) and (17)–(21) using the introduced model.

The systems (18) and (20) with l=L for all $q=\overline{1,N}$ must give a complete convolution with the value of L, that is (18):

$$\sum_{i=1}^{L} W_i^q W_i^q = L, q=\overline{1,N} \quad (22)$$

and (20) gives

$$\sum_{i=1}^{L} W_i^p W_i^p = L, p=\overline{1,N}. \quad (23)$$

The systems (17), (19) and (21) with $l=L$ for all pairs W^q and W^p give the values of the cross-correlation function with zero shift:

$$\sum_{i=1}^{L} W_i^q W_i^p = R^{qp}(0); q, p=\overline{1,N}, \quad (24)$$

$$\sum_{i=1}^{L} W_i^q W_i^p = R^{qp}(0), q, p=\overline{1,N}, \quad (25)$$

$$\sum_{i=1}^{L} W_i^p W_i^q = R^{pq}(0), p, q=\overline{1,N}. \quad (26)$$

In what follows, the systems (15–16), (17–21) and the quadratic equation (24) will be called the model of the subset (dictionary) of the CS.

We will analyze systems (15–16) for the existence of solutions and independence. It follows directly from (15) that for each of q CS W^q there are L unknowns $W_1^q, W_2^q \cdots W_L^q$. To find them, ac-

cording to (15), we can construct a system of L–1 independent NPI. Further, using (16), we obtain one more expression, but an equation. The peculiarity of the system (15) is that it gives a convolution of each of the CS with the value L. On the basis of (15) and (16) in the construction of each N subset of the CS, one can compile N independent systems of quadratic NPIs, each of which will contain L–1 quadratic inequalities of the form (15) and formally one equation, so that there will be only L.

We also analyze the set of systems of parametric inequalities (17–21), taking into account (22), (26), for the existence of solutions and the independence of systems and individual equations. The systems (17–21) determine the permissible mutual properties relative to PCCF and CCCF of each pair of CS - W^q and W^p. They define the requirements for PCCF and CCCF specifically for only two CS W^q and W^p. When constructing three CS, we have 3!/2, and for N CS, respectively, N!/2 of such systems.

Thus, with increasing N, the number of systems of the form (17–21) increases exponentially (by factorial).

For N=2, among the (22)–(26) systems of NPI there are redundant nonlinear quadratic equations. Equation (16) coincides with (22) and (23) because the last two already enter the system (16), are dependent, and therefore cannot be used. Further, equation (24) and (25) coincide, and equation (26) is symmetric, in part of the correlation function, with respect to equations (23) and (25). Therefore, for each pair of p and q, (24) is independent.

On the basis of detailed analysis, we have that all (17–21) NPI systems determine the different implementations of PCCF and CCCF specifically for only two CS - W^q and W^p. Therefore, the mathematical model for constructing two CS W^q and W^p is uniquely determined by the five NPI systems in the form (17–21) and, as already justified, by the equation (24).

The above analysis results allow to determine the complexity of the model and on its basis the complexity of constructing a subset of N CS.

1. When constructing one CS, it is necessary, depending on the allowable values $R^q_{a_1}(l)$ and $R^q_{a_2}(l)$, defined by the limits of dense packaging, consider v ≥ k systems of the form (15-16).

2. When constructing two CS, it is necessary to consider $v_2 \geq k_2$ systems of the form (17-21), where k_2 is determined from $R^{qp}_{b_{1,j}}(l)$ and $R^{qp}_{b_{2,j}}(l)$.

3. When constructing N CS, it is necessary to consider $v_N \geq k_N$ systems of the form (17-21), where k_N is determined $R^q_{a_1}(l)$ and $R^q_{a_2}(l)$, and also $R^{qp}_{b_{1,j}}(l)$, and $R^{qp}_{b_{2,j}}(l)$ allowed values.

Thus, on the basis of accounting for the boundaries of the physical packing of the subset of CS [1], there are possibilities to construct subsets of the CS according to (15–16) and (17–21), using aperiodic autocorrelation functions (AACF). In this case, simplifications are possible. So the system (15–16) by analogy can be represented in the form of an NPI system on the basis of aperiodic correlation functions, that is,

$$r^q_{a_1}(l) \leq \sum_{i=1}^{L-m} W_i^q \left(W_{i+1}^q\right)^* \leq r^q_{a_2}(l),\ l=\overline{1,L},\ m=\overline{1,L}, \tag{27}$$

where $r^q_{a_1}(l)$ and $r^q_{a_2}(l)$ – prescribed, but feasible, implementations in terms of tight packaging. Further, the systems (15–16) and (17–21) can also be represented in terms of aperiodic mutual correlation functions (ACCF) in the form of a system of nonlinear parametric inequalities

$$r^{qp}_{b_{1,1}}(l) \leq \frac{1}{L-m} \sum_{i=0}^{L-m} W_i^q \left(W_{i+1}^q\right)^* \leq r^{qp}_{b_{1,2}}(l); \tag{28}$$

$$l=\overline{1,L},\ m=\overline{1,L},$$

$$r_{b_{2,1}}^{qp}(l) \le \frac{1}{L-m} \sum_{i=0}^{L-m} W_i^p \left(W_{i+1}^q\right)^* \le r_{b_{2,2}}^{pq}(l); \quad (29)$$

$$l = \overline{1, L},\ m = \overline{1, L},$$

where $r_{b1,1}{}^{qp}, r_{b1,2}, {}^{qp}\, r_{b2,1}, {}^{qp}\, r_{b2,2}{}^{qp}$ - permissible from the point of view of close packing AACF and ACCF.

5 Problem solution for synthesis of a system of nonlinear discrete complex cryptographic signals

The use of CS will improve the performance of ICS, in particular: EMS, noise immunity (noise immunity of receiving signals under the influence of structural, obstructive, retransmitted and other types of interference, stealth operation) and information security. Such discrete signals have the necessary but limited ("tight packing" values), correlation and ensemble properties. With this approach, the structural concealment of the signal is provided by randomness or pseudo randomness, and noise immunity is provided by the correlation properties of the synthesized system of signals. Information security of ICS is provided on the basis of the fact that the statistical properties of CS are close to the properties of random sequences, as well as the use of cryptographic keys. It is necessary to note the special property of CS systems: the possibility of their recovery in space and time with the use of keys and a number of other parameters that are used in the synthesis of signals.

The authors proposed a method for synthesizing systems of complex nonlinear cryptographic signals, including the following stages [13].

1. Formation of random or pseudorandom discrete sequences using key data.
2. Estimation of statistical properties of potential CS.
3. Building the required number of potential CS W^q in accordance with the system of inequalities (15) and key data.
4. Finding pairs or subsets of the CS W^q and W^p, which satisfy the requirements (17–21).
5. The construction of the matrix of states of the mutually correlated functions of all possible pairs of potential CS, which were selected by the results of the previous step and have all the necessary properties.
6. The analysis of the matrix of states and the formation of the necessary number of subsets or pairs of CS according to (15–16) and (17–21) and selection in the subset of only those pairs that satisfy the requirements.

Examples of pairs and subsets of CS are given in [13].

Taking into account the need to ensure the cryptographic stability and structural concealment (complexity) of the cryptographic signal, the choice of the algorithm of symmetric block encryption with the counter is justified as a source of pseudorandom sequences of symbols (*the first stage of the method*): The national cryptographic standard of the block symmetric transformation of DSTU 7624:2014, "Kalyna" and its modes of operation to ensure confidentiality and integrity of information [15]. Alternatively, a source based on the AES algorithm (international standard ISO/IEC 18033) may be proposed. Preference in the selection is given to DSTU 7624:2014, taking into account the following factors.

Block symmetric ciphers (BSC) are one of the most common cryptographic primitives [16-18]. In addition to securing the confidentiality (*encryption*) of the main volumes of information transmitted over the network or stored locally, they are used as a constructive element of other primitives (hashing functions, message authentication codes, pseudorandom sequence generators, etc.). The importance of this cryptographic transformation is underscored by a number of international competitions, such as AES, NESSIE, CRYPTRACK, which were focused on the development of block cipher (*as the main goal or as part of a set of promising solutions*).

The national standard supports the block size and encryption key length of 128, 256 and 512 bits (*the key length is equal to the block size or twice as large*), providing a normal, high and ultra high

level of durability (*now it is the only block encryption standard in the world supporting 512- bit symmetric keys*). Different variants of the standard provide flexibility of choice of parameters for developers of cryptographic protection systems, which makes it possible to obtain both the highest level of performance and the largest margin of conversion stability. The high-level design uses a well-researched Square-like SPN structure used in the algorithms of AES/Rijndael, Whirlpool, Stribog and many others. The cycle transformation is constructed on the basis of tables of substitution (S-blocks) and multiplication by an MDS-matrix over a finite field, providing necessary cryptographic properties. The use of such a design makes it possible to provide provable stability with respect to differential, linear and other types of cryptanalysis, while simultaneously providing an effective implementation for a wide range of software and hardware/software platforms. When choosing the size of the MDR-matrix, the size of the L1 cache of modern and promising processors was taken into account, which made it possible to optimize the performance of the software implementation of the cipher [19-22]. The standard of Ukraine provides the greatest nonlinearity of Boolean functions, which gives an additional margin of stability in relation to linear cryptanalysis. In addition, in our opinion, the standard of block symmetric transformation of DSTU 7624: 2014 refers to post-quantum algorithms, i.e. it will ensure (*when selecting the appropriate parameters*) cryptographic resistance against attacks with the use of quantum computers [11].

6 Nonlinear discrete complex cryptographic signals properties

Tables 1 and 2 show the results of studies that illustrate the possibility of applying the above method of signal synthesis for a number of applications of ICS.

Table 1 – Correlation properties of cryptographic discrete sequences

CS segment size	Limit values of the uncertainty function	PACF			AACF	PCCF		
		The number of CS satisfying the boundary	The smallest value R_{6max}	The number of CS with the least R_{6max}	The number of CS that satisfy the boundary	Total number of pairs	Number of pairs satisfying the boundary	The smallest value R_{6max}
64	17	9 545	8	14	4 931	45 553 512	5 451 589	10
1 024	90	2 209	72	3	1 149	2 439 840	26 638	82
30	9	2 479	2	2	973	3 072 720	95 722	6
31	9	7 743	5	155	3 622	29 977 024	1 465 137	5
63	17	10 868	9	14	7 166	59 056 712	12 214 869	11
127	25	6 798	17	51	3 636	23 106 402	1 266 098	19
127	27	10 006	17	51	6 491	50 060 018	9 006 648	19
511	63	7 662	45	6	4 783	29 353 122	2 666 671	51
1 023	100	8 513	70	4	6 194	36 235 584	5 293 538	81

So, in Table 1, in accordance with the method described above, the results of synthesis of discrete sequences for some values of the sequence period are presented, in particular, the following are given: boundary values for maximum emissions of correlation functions satisfying the "tight packing" boundaries [1-3]; the number of pairs of sequences constituting a complete ensemble of signals (*for estimating the cross-correlation properties of signals*); the number of signals satisfying the boundary values for different correlation functions. Table 2 gives estimates of the number of pairs of sequences of different classes (*M-sequences, sequences with a three-level cross-correlation function – PCCFT, cryptographic sequences (CP))* that satisfy the "close packing" boundary for the corresponding period [5,13].

Table 2 – The ensemble properties of various complex signal systems

Type of signals	Sequence Period	"Dense packing" border value	Sequences pairs number satisfying the boundary
M-sequences	31	9	3
PCCFT	31	9	495
CS	31	9	1465137
M-sequences	127	27	36
PCCFT	127	17	11610
CS	127	23	47 053
M-sequences	255	36	28
PCCFT	–	–	–
CS	255	36	17599
M-sequences	511	63	276
PCCFT	511	33	147500
CS	511	63	2666671
M-sequences	1023	100	435
PCCFT	1023	65	338000
CS	1023	100	5293538

The analysis of the data in Table 1-2 shows that the proposed method for synthesizing complex nonlinear discrete cryptographic signals using random or pseudorandom processes allows the formation of large ensembles of discrete sequences of almost any period with given, but physically realizable, side lobes of auto-mutual and butt correlation functions in periodic and aperiodic modes of operation, as well as statistical characteristics of correlation functions that are not inferior to anal tech characteristics of the best classes of linear signals. Thus, for the period of the sequence N=63, the number of pairs of cryptographic discrete sequences satisfying the established limit value of the maximum side lobes PCCF-17 is 12,214,869. For a representative of a class of linear sequences – sequences with a three-level cross-correlation function (*Gold sets that are optimal from the point of view functions of cross-correlation signals* [6]), the number of pairs of signals satisfying this boundary is -975. Exceeding the volume of cryptographic signals over the ensemble composed of M-sequences is more than 10^7 times. For the period of the sequence 1023, the number of pairs of cryptographic discrete sequences satisfying the established boundary value for the side lobes of the cross-correlation functions (CCF) -100 is 5293538, whereas for a representative of the class of linear sequences of M-sequences, the number of pairs satisfying this boundary is -43 i.e. exceeding the volume of the signal system is more than 105 times. It should be emphasized that the law for the formation of each of the cryptographic signals is determined by the key, and the length of the key can be substantially smaller than the period (length) of the signal itself. With a slight decrease in the requirements for the maximum peak side peak CCF, according to which signals are selected (*in fact, decrease in noise immunity of reception*), the indicators of imitating resistance of IKS operation can be significantly improved. Thus, for the period of the sequence N=127, an increase in the boundary value by 1.2 dB, will increase the volume of the ensemble with M=11610 at the boundary R_{bmax}=17, to 9,006,648 signals, with a boundary value of 27, i.e. in 776 times.

The performed calculations and simulated simulation indicate that the maximum lateral emissions of the correlation functions of the CS, as well as the statistical characteristics of this class of signals, are not inferior to the corresponding characteristics of linear M-sequences [8].

Thus, varying the boundary values of the level of the side lobes of the corresponding correlation function, depending on the requirements imposed on the ICS from the point of view of noise immunity of receiving signals, the system can be solved to achieve the required noise immunity of signal reception, imitating and information stealth ICS.

In Table 3 shows examples of calculating the statistical characteristics of various correlation functions for discrete signals widely used in communication systems and, in particular, the characteristics of cryptographic DS These characteristics were obtained using the developed special software. Calculations were carried out for different values of the DS period. As statistical characteristics of the correlation functions:

- greatest lateral emissions values R_{max};
- mathematical expectation value of the emission module $m_{|R|}$;
- standard deviation value of the emission module $D_{|R|}^{1/2}$ and emission values $D_{R}^{1/2}$.

Table 3 – Statistical characteristics of the correlation functions of discrete signals

Type of signals	Characteristics	$\frac{R_{макс}}{\sqrt{N}}$	$\frac{m_{\|R\|}}{\sqrt{N}}$	$\frac{D_{\|R\|}^{1/2}}{\sqrt{N}}$	$\frac{D_{(R)}^{1/2}}{\sqrt{N}}$
Characteristic discrete signals	AACF	1,0 – 1,8	0,5	0,4	0,5
	PACF	0,1 – 1,9	0,2	0,1	0,2
	ACCF	1,9 - 3,2	1,0	0,8	1,0
	PCCF	2,5 – 3,6	1,0	0,8	1,2
	CCCF	2.1 – 5,0	0,9	0,7	1,1
M-sequences	AACF	0,7...1,25	0,32	0,26	0,41
	PACF	$1/\sqrt{N}$	$1/\sqrt{N}$	0	0
	ACCF	1,4...5,0	0,54	0,48	0,73
	PCCF	1,9...6,0	0,8	0,62	1,0
	CCCF	2,0...5,1	0,83	0,62	1
Cryptographic signals	AACF	1,2 – 1,9	0,5	1	1,1
	PACF	0,2 – 1,9	0,6	0,4	0,7
	ACCF	1,4 – 3,4	0,5	0,4	0,6
	PCCF	1,9 – 5,2	0,7	0,5	0,8

Analysis of the data given in Table 3, indicates that the values of the maximum lateral emissions of the CS, as well as the statistical characteristics of this class of signals, are not inferior to the corresponding characteristics of signals constructed using M-sequences and characteristic discrete signals [3]. As illustrations in Fig. 1 to 3, various correlation functions for the cryptographic DS synthesized according to the method described above.

For many applications of ICS, a situation is typical where individual stations intentionally have a negative effect on the functioning of the radiating system. In such cases, the electromagnetic compatibility, information security and noise immunity of ICS is largely determined by the structural or statistical properties of the data-sending signals in the system. In the face of EMC countermeasures, the radio channels interference immunity of ICS depends on the secretiveness of the selection and use of the system parameters. The interference will only be effective the case where the countermeasure station establishes the fact of the presence of the opposing system in the air and assesses its parameters frequency band occupied band, the law of modulation of the signal, and others.

Under the covertness of radio channels in general and the hiddenness of the parameters used in them, we will understand their ability to withstand the measures of the radio-electronic countermeasure aimed at detecting the fact of the system operation (*energy concealment*) and determining the signal parameters necessary for radio counteraction (*structural and information concealment*).

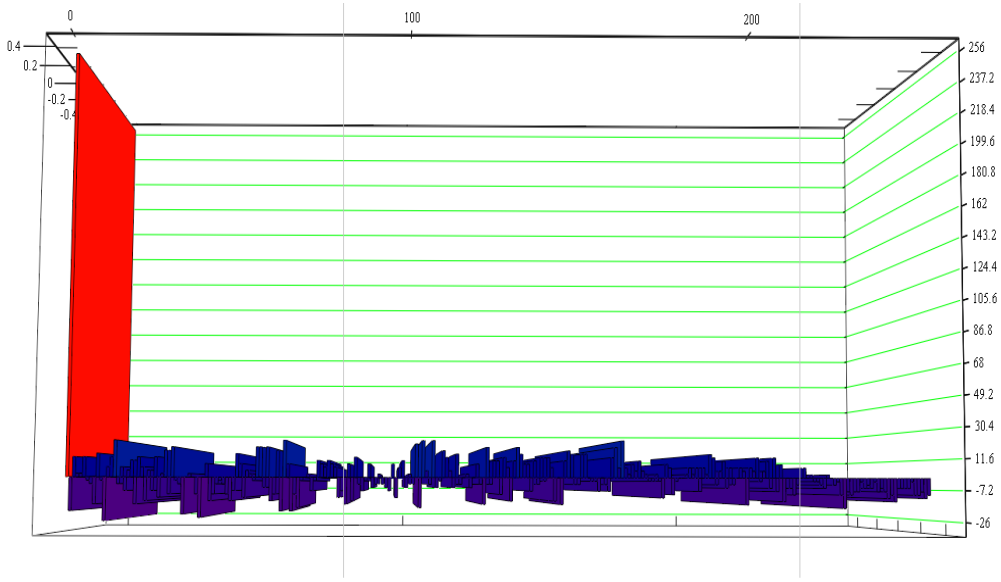

Fig. 1 – AACF for CS period L=256

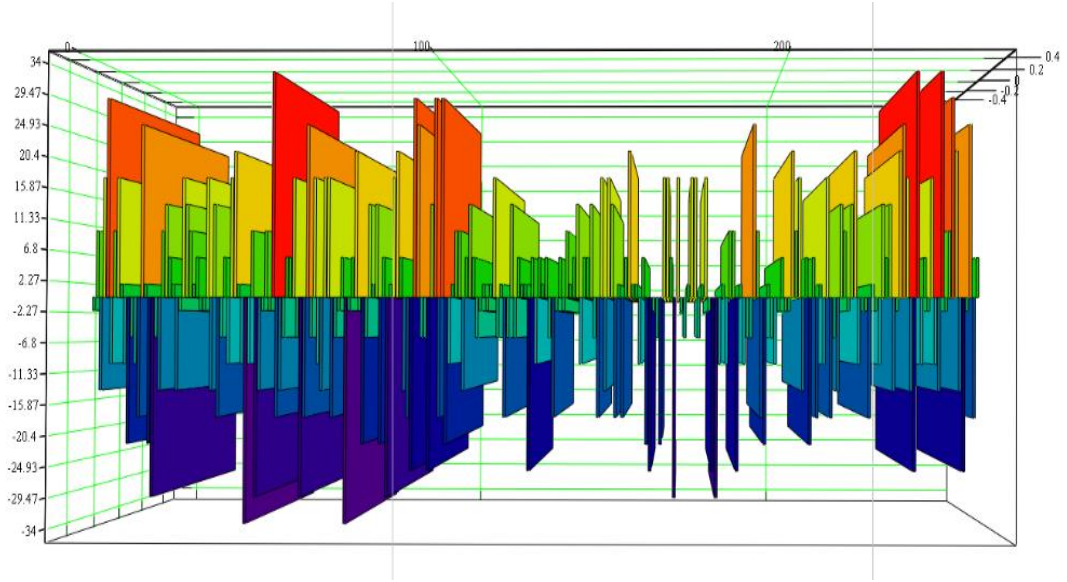

Fig. 2 – PCCF for CS period L=256

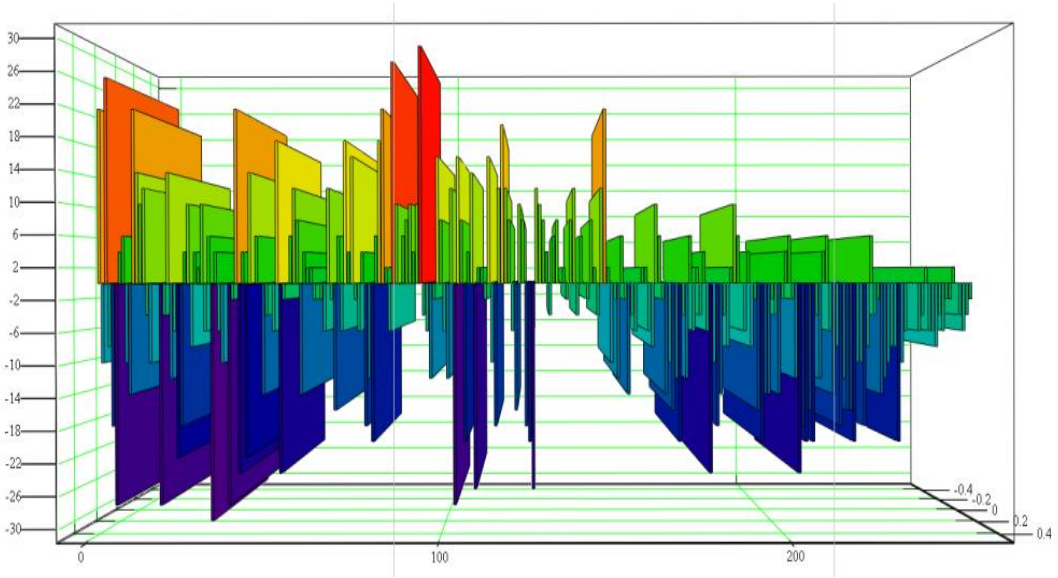

Fig. 3 – ACCF for CS period L=256

Energy concealment characterizes the ability of the system to withstand measures aimed at detecting by the station the counteraction to the fact of the functioning of the system. Structural concealment of used signals characterizes the complexity of reliable prediction of signals or their symbols (*according to known previous ones*). Information concealment (*difficulties in identifying received signals with a message that is transmitted*) predisposes the system's ability to conceal the semantic content of messages, the ways of generating messages (signals), the very fact of signal transmission.

If the radiating system uses a signal with a nontrivial modulation law whose parameters are unknown to the counter, the latter is unable to use a correlator or a matched filter to detect the signal. The only strategy of the opposing side in this case is the use of an energy detector [1], which is optimal from the point of view of detecting a band-limited noise signal against the background of Abelian white Gaussian noise. To prevent the station from detecting counteracting the signal, the radiating system should use signals with a distributed or wide spectrum, which have the highest possible value of the processing gain, and a practically undiscovered structure.

The ideal structural concealment of the signal means that the signal synthesis methods must implement signals that meet certain requirements. It is quite obvious that such requirements meet the requirements for generators, which form random (pseudo-random) sequences. In addition, there should be an opportunity to perform an assessment of the correspondence of the properties of the synthesized signals to certain requirements. Investigations of statistical properties are carried out within the framework of statistical tests based on statistical tests. The most acceptable (from the point of view of practical use) testing techniques are: NIST STS, FIPS PUB 140-1, AIS 20 and AIS 31, NIST 800-90b, NIST 800-22.

To investigate the structural properties of CS, we used the random number (pseudo-random) generator testing methodology defined by NIST 800-22 [23]. NIST 800-22 includes 16 statistical tests, and 188 probability values are computed. All tests are aimed at identifying various randomness defects (not meeting the requirements of randomness).

Testing procedure:

1. A null hypothesis is advanced H_0 – the assumption that the test binary sequence is random.

2. For the sequence generated by the generator, the test statistics are calculated.

3. Using the special function and test statistics, the probability value $P \in [0,1]$.

4. Probability value P is compared with the level of significance α, $\alpha \in [0,001; 0,01]$. If $P \geq \alpha$, then the hypothesis H_0 is accepted. Otherwise, an alternative hypothesis is adopted.

As a result of testing the memory bandwidth, a vector of probability values is generated $P = \{P_1, P_2, ..., P_{188}\}$. In the standard, the recommended length is the input data block – 106 binary symbols; one test uses 100 blocks of this length (*the input data length for one test cycle is 108 characters*). In NIST, two thresholds are used to decide the test results: 0.96 and 0.99, that is, for different significance levels it is established that out of 100 blocks cannot pass four and one test respectively.

With the use of NIST SP 800-22, the implementation of the cryptographic symbol sequence was tested. The test results are shown in the Table 4.

The results of testing showed that the statistical properties of nonlinear KS in terms of the values of the probabilities of this method are within the limits of acceptable values. And this, in turn, means that the CS satisfy the requirements for pseudo-random sequences [23-24]: - the unpredictability of the sequence of symbols, irreversibility, randomness, equal probability, independence, unpredictability, indistinguishability, etc. In essence, CS are indistinguishable from random sequences. Thus, the use of CS as a physical data carrier will increase the structural and information security (*cryptographic strength*) of the ICS.

Table 4 – Estimation of statistical properties of cryptographic discrete sequences using NIST SP 800-22

№	c1	c2	c3	c4	c5	c6	c7	c8	c9	c10	Probability	Test result	Test title
1	14	5	11	10	10	12	7	14	8	9	0,574903	0,99	Frequency
2	10	8	10	11	12	5	6	13	14	11	0,574903	0,99	BlockFrequency
3	13	6	5	14	18	10	9	5	12	8	0,058984	0,99	CumulativeSums
4	14	9	4	10	8	8	15	15	12	5	0,122325	1	CumulativeSums
5	9	8	8	12	10	10	14	7	8	14	0,759756	1	Runs
6	8	14	15	8	8	7	9	12	10	9	0,657933	1	LongestRun
7	12	10	11	7	11	7	6	15	11	10	0,678686	1	Rank
8	10	7	9	12	9	11	14	10	8	10	0,935716	1	FFT
9	10	10	6	10	7	10	11	9	9	18	0,419021	1	NonOverlappingTemplate
10	11	7	9	12	9	14	9	8	11	10	0,924076	0,98	NonOverlappingTemplate
11	17	11	14	10	10	6	10	7	7	8	0,319084	1	NonOverlappingTemplate
12	16	9	7	8	6	7	10	13	9	15	0,275709	0,98	NonOverlappingTemplate
13	12	6	7	8	11	7	12	10	13	14	0,616305	0,99	NonOverlappingTemplate
14	15	15	10	9	7	11	6	9	7	11	0,455937	0,98	NonOverlappingTemplate
15	11	9	13	7	11	14	9	12	8	6	0,719747	1	NonOverlappingTemplate
16	13	12	12	9	12	12	7	8	8	7	0,816537	0,97	NonOverlappingTemplate
17	11	11	14	8	10	8	10	10	9	9	0,971699	1	NonOverlappingTemplate
18	8	12	11	11	12	7	12	12	6	9	0,851383	1	NonOverlappingTemplate
19	9	11	10	12	7	11	8	16	7	9	0,678686	1	NonOverlappingTemplate
20	14	10	13	10	12	12	6	7	11	5	0,494392	0,98	NonOverlappingTemplate
21	15	11	10	8	12	9	13	9	5	8	0,595549	0,95	NonOverlappingTemplate
22	9	5	14	10	7	6	14	9	13	13	0,334538	1	NonOverlappingTemplate
23	12	7	7	11	11	5	14	12	11	10	0,637119	0,99	NonOverlappingTemplate
24	10	12	12	11	15	10	7	10	6	7	0,657933	1	NonOverlappingTemplate
25	12	8	14	9	12	12	6	8	11	8	0,759756	0,98	NonOverlappingTemplate
26	6	7	7	10	14	7	8	15	15	11	0,249284	0,99	NonOverlappingTemplate
27	12	7	13	6	11	10	10	16	7	8	0,455937	0,98	NonOverlappingTemplate
28	12	9	9	12	9	10	6	7	17	9	0,474986	0,98	NonOverlappingTemplate
... 184	7	7	11	7	6	11	5	6	4	7	0,666838	0,9859	RandomExcursionsVariant
185	7	6	10	11	4	5	11	8	4	5	0,362174	1	RandomExcursionsVariant
186	6	11	11	1	9	11	4	4	6	8	0,076389	1	RandomExcursionsVariant
187	14	7	6	9	13	7	14	6	14	10	0,289667	1	Serial
188	11	8	13	5	6	11	14	8	14	10	0,419021	1	Serial
189	9	6	13	9	11	11	10	6	13	12	0,759756	0,99	LinearComplexity
											84,82113	186,0039	

7 Synthesis of derived signal systems based on cryptographic discrete sequences of symbols

Various signal systems (sets of linear recurrence sequences, Kasami, Gold, Kamaletdinov sets, etc.) that have relatively small values of the side lobes of auto and mutually correlated functions are found in the IKS as a physical carrier of information [1-3]. However, these signals have low structural latency, limited ensemble properties, and also exist only for a limited number of signal period values. In the case of truncation (increase) of the period of such signals, their correlation properties deteriorate. Therefore, the actual task is to develop the theory and practice of synthesis and analysis of discrete signal systems with the required correlation, structural, ensemble properties. Studies have shown [12] that the required (in various conditions) performance indicators of the system can be realized, including through the use of broadband radio systems, for which the expansion of the spectrum is carried out using nonlinear discrete sequences. In [13], the problem of synthesizing nonlinear cryptographic discrete signals (CS) that provide the required values of noise immunity, information and structural stealth of the TKS operation, is formulated and solved. In general, the problem of synthesis of optimal binary cryptographic signals of a given period is formulated as follows. It is necessary to find a lot of discrete binary sequences - cryptographic sequences (CS) with a given number of symbols possessing the permissible level of maximum side lobes of the periodic autocorrelation function (PACF). Further, the solution of the synthesis problem is reduced to the preliminary selection of a certain limited set of discrete sequences, which seems promising in terms of providing the necessary cross-correlation properties.

Among the systems of phase-shifted signals, many are formed on the basis of Walsh systems [1-4]. It is known that auto - and mutually correlated functions of Walsh sequences have large lateral peaks. To improve the correlation properties of the signals, the signal system derivatives (DSS) are generated by multiplying the Walsh sequences (source sequences) by a signal that has certain properties (the signal generator), in particular, has small side peaks of the autocorrelation function. The authors formulated a hypothesis about the possibility of using non-linear cryptographic sequences (CS) as generators, the theoretical bases of their synthesis are given in [12-13]. The method of synthesizing derived signal systems based on the use of CS includes the following steps.

1. A selection is made of M cryptographic sequences (CS) of a fixed period L having minimum values of maximum side lobes (Rmax.) PACF.

2. A set of Walsh codes (the matrix N · N) is formed in which each line corresponds to a separate code.

3. The sequences (each of the Walsh code lines of the original sequences) are multiplied by a cryptographic signal, forming N DSS.

4. Investigate the correlation properties of the DSS formed (in particular, PACF, AACF). To investigate the cross-correlation functions, they form a matrix of dimension N · N. The number of such matrices is L · N.

As an illustration of this method of DSS synthesis, consider the Walsh code (Table 5).

Table 5 - The Walsh code *(of dimension N = 64)*

N = 64	1111111111111111111111111111111111111111111111111111111111111111 1010101010101010101010101010101010101010101010101010101010101010 1100110011001100110011001100110011001100110011001100110011001100 1001100110011001100110011001100110011001100110011001100110011001 1111000011110000111100001111000011110000111100001111000011110000 1010010110100101101001011010010110100101101001011010010110100101 1100001111000011110000111100001111000011110000111100001111000011 1001011010010110100101101001011010010110100101101001011010010110 1111111100000000111111110000000011111111000000001111111100000000 1010101001010101100101010010101011010101001010101101010100101010 1100110000110011110011000011001111001100001100111100110000110011 1001100101100110100110010110011010011001011001101001100101100110 1111000000001111111100000000111111110000000011111111000000001111 1010010101011010010101101001011010101001011010010101011010010110 1100001100111100110000110011110011000011001111001100001100111100 1001011001101001100101100110100110010110011010011001011001101001 1111111111111111000000000000000011111111111111110000000000000000 1010101010101010010101010101010110101010101010100101010101010101 1100110011001100110011001100110000110011001100110011001100110011 1001100110011001100110011001100101100110011001100110011001100110 1111000011110000111100001111000000001111000011110000111100001111 1010010110100101101001011010010101011010010110100101101001011010 1100001111000011110000111100001100111100001111000011110000111100 1001011001101001011010011001011001101001100101101001011001101001

Table 6 shows the CS (M=14), selected from the set of sequences, according to the criterion of

the minimum value of the maximum side lobes PACF (R_{max}<10). The calculations of the statistical characteristics of the correlation functions (PACF) of the selected CS are also presented here.

Table 6 – Cryptographic sequences with minimum values of side peaks PACF

1	1110001111101000011111011100110011000101000110101101001001100101
2	1000010010000100101110011010000000110010010000010111001110011101
3	0000100100001001011100110100000001100100100000101110011100111011
4	0000100100001001011100110100000001100100100000101110011100111011
5	0001001000010010111001101000000011001001000001011100111001110110
6	0100100001001011100110100000001100100100000101110011100111011000
7	0000100101110011010000000110010010000010111001110011101100010110
8	0001001011100110100000001100100100000101110011100111011000101101
9	0010010111001101000000011001001000001011100111001110110001011010
10	0100101110011010000000110010010000010111001110011101100010110100
11	0000000010100010011000001111100001101101110001101000010111100101
12	0000000101000100110000011111000011011011100011010000101111001010
13	0000001010001001100000111110000110110111000110100001011110010100
14	0100011110001100000100110010000000011011111011100101011000010110

The results of the PCCF DSS based on CS show that the number of pairs of signals for a sequence of 64 symbols for which the R_{max} values do not exceed 17 (*this, the so-called "close packing" boundary, achieved in the best CCF series from the CCF viewpoint three-level PCCF*) is 604 pairs (*about 30% of the total number of possible combinations of pairs of signals*). The number of pairs of signals for which the values of R_{max} do not exceed 20 – 1577, which is 77% of the total number of pairs of signals. At the boundary R_{max}<25, the maximum number of selected pairs of signals is 1984 (96.8 %). The values of the maximum side peaks of PCCF R_{max}<25 occur for the sequences most widely used in modern M-sequences.

Calculation of statistical characteristics of correlation functions (PACF) CS

1)64 0 -8 -4 -4 0 -8 0 0 4 0 4 4 -8 -4 8 -4 -4 0 4 4 -4 4 -4 0 8 4 4 -4 -8 -4 0 -8 0 -4 -8 -4 4 4 8 0 -4 4 -4 4 4 0 -4 -4 8 -4 -8 4 4 0 4 0 0 -8 0 -4 -4 -8 0
PFAKmin: -4 PFAKmax: -8 MO: -0.09375 |MO|: 0.46875 DISP: 0.5763694553724894 |DISP|: 0.3384787011890674

2)64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 4 8 4 4 8 -8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4
PFAKmin: 4 PFAKmax: -8 MO: 0.15625 |MO|: 0.59375 DISP: 0.6774495430488349 |DISP|: 0.3469815618916576

3)64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 4 8 4 4 8 -8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4
PFAKmin: 4 PFAKmax: -8 MO: 0.15625 |MO|: 0.59375 DISP: 0.6774495430488349 |DISP|:
0.3469815618916576

4)64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 8 4 4 8 -8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4
PFAKmin: 4 PFAKmax: -8MO: 0.15625 |MO|: 0.59375 DISP: 0.6774495430488349 |DISP|:
0.3469815618916576

5)64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 8 4 4 8 -8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4
PFAKmin: 4 PFAKmax: -8MO: 0.15625 |MO|: 0.59375 DISP: 0.6774495430488349 |DISP|:
0.3469815618916576

6)64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 8 4 4 8 -8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4
PFAKmin: 4 PFAKmax: -8 MO: 0.15625 |MO|: 0.59375 DISP: 0.6774495430488349 |DISP|:
0.3469815618916576

7)64 4 -8 4 4 0 0 4 -4 4 0 -8 4 0 4 0 4 0 -8 0 0 8 0 0 -8 -4 -4 4 8 4 4 4 -4 4 4 4 8 4 -4 -4 -8 0 0 8 0 0 -8 0 4 0 4 0 4 -8 0 4 -4 4 0 0 4 4 -8 4
PFAKmin: 4 PFAKmax: -8 MO: 0.0703125 |MO|: 0.4296875 DISP: 0.5553298776598447 |DISP|:
0.350712702793093

8)64 0 -8 4 4 0 -4 4 -8 8 4 -8 4 0 8 0 0 4 -8 0 -4 4 0 0 -8 -4 0 0 4 4 0 0 0 0 0 4 4 0 0 -4 -8 0 0 4 -4 0 -8 4 0 0 8 0 4 -8 4 8 -8 4 -4 0 4 4 -8 0
PFAKmin: 4 PFAKmax: -8 MO: 0.0 |MO|: 0.40625 DISP: 0.5634361794742422 |DISP|:
0.3836429502240921

9)64 0 -8 4 4 0 -4 4 -8 8 4 -8 4 0 8 0 0 4 -8 0 -4 4 0 0 -8 -4 0 0 4 4 0 0 0 0 0 4 4 0 0 -4 -8 0 0 4 -4 0 -8 4 0 0 8 0 4 -8 4 8 -8 4 -4 0 4 4 -8 0
PFAKmin: 4 PFAKmax: -8 MO: 0.0 |MO|: 0.40625 DISP: 0.5634361794742422 |DISP|:
0.3836429502240921

10)64 0 -8 4 4 0 -4 4 -8 8 4 -8 4 0 8 0 0 4 -8 0 -4 4 0 0 -8 -4 0 0 4 4 0 0 0 0 0 4 4 0 0 -4 -8 0 0 4 -4 0 -8 4 0 0 8 0 4 -8 4 8 -8 4 -4 0 4 4 -8 0
PFAKmin: 4 PFAKmax: -8MO: 0.0 |MO|: 0.40625 DISP: 0.5634361794742422 |DISP|:
0.3836429502240921

11)64 8 4 0 -8 -8 -4 4 8 8 4 0 0 -4 -8 4 8 8 0 8 4 0 0 -4 -4 -8 -4 0 0 4 -4 4 -4 -4 -4 4 0 0 -4 -8 -4 -4 0 0 4 8 0 8 8 4 -8 -4 0 0 4 8 8 4 -4 -8 -8 0 4 8
PFAKmin: 4 PFAKmax: 8 MO: 0.0703125 |MO|: 0.5234375 DISP: 0.6476900319675074 |DISP|: 0.3767205345969094

12)64 8 4 0 -8 -8 -4 4 8 8 4 0 0 -4 -8 4 8 8 0 8 4 0 0 -4 -4 -8 -4 0 0 4 -4 4 -4 -4 -4 4 0 0 -4 -8 -4 -4 0 0 4 8 0 8 8 4 -8 -4 0 0 4 8 8 4 -4 -8 -8 0 4 8
PFAKmin: 4 PFAKmax: 8 MO: 0.0703125 |MO|: 0.5234375 DISP: 0.6476900319675074 |DISP|: 0.3767205345969094

13)64 8 4 0 -8 -8 -4 4 8 8 4 0 0 -4 -8 4 8 8 0 8 4 0 0 -4 -4 -8 -4 0 0 4 -4 4 -4 -4 -4 4 0 0 -4 -8 -4 -4 0 0 4 8 0 8 8 4 -8 -4 0 0 4 8 8 4 -4 -8 -8 0 4 8
PFAKmin: 4 PFAKmax: 8 MO: 0.0703125 |MO|: 0.5234375 DISP: 0.6476900319675074 |DISP|: 0.3767205345969094

14)64 8 -4 4 4 0 0 4 -4 -4 4 -4 -8 0 -4 0 8 0 8 -4 -8 -4 -8 8 -8 0 0 4 0 -4 4 4 8 4 4 -4 0 4 0 0 -8 8 -8 -4 -8 -4 8 0 8 0 -4 0 -8 -4 4 -4 -4 4 0 0 4 4 -4 8
PFAKmin: -4 PFAKmax: 8 MO: 0.0 |MO|: 0.5 DISP: 0.6236095697723273 |DISP|: 0.3618734420321171

Table 7 shows the results of studies of the statistical characteristics of the correlation functions of various classes of signals, including DSS when used as generating cryptographic signals. Calculations were carried out for different values of the sequence periods (from 30 to 2052).

Table7 – Statistical characteristics of correlation functions DSS

Type of signals	**Characteristics**	$\frac{R_{макс}}{\sqrt{N}}$	$\frac{m_{\lvert R\rvert}}{\sqrt{N}}$	$\frac{D_{\lvert R\rvert}^{1/2}}{\sqrt{N}}$	$\frac{D_{(R)}^{1/2}}{\sqrt{N}}$
DSS	AACF	0,8 – 2,4	0,4 – 0,5	0,9 – 1	1 – 1,1
	PACF	0,7 – 2,5	0,2 – 0,7	0,2 – 0,5	0,3 – 0,9
	ACCF	1 – 2,5	0,2 – 0,7	0,2 – 0,5	0,3 – 0,7
	PCCF	1,4 – 2,8	0,2 – 0,7	0,4 – 0,5	0,6 – 0,9
Linear M-sequences	AACF	0,7 – 1,25	0,32	0,26	0,41
	PACF	1/√N	1/√N	0	0
	ACCF	1,4 – 5,0	0,54	0,48	0,73
	PCCF	1,9 – 6,0	0,8	0,62	1

Analysis of the data in Table 7 shows that the statistical characteristics of the DSS are close to the corresponding characteristics of linear signal classes. In this case, the values of the maximum lateral peaks of the DSS cross-correlation functions are less than for the linear M sequences used in modern ICS.

8 Conclusions

The methods of information exchange used in the ICS, based on a fixed correspondence: the message bit (m bit) - signal (2^m signals) in the information channel, and the use (*for a long time*) of the same broadband signal in the synchronization channel (*the signals used are constructed using linear laws*), do not allow to provide the required electromagnetic compatibility (EMC) of systems and facilities operating in a relatively small to achieve the necessary values of noise immunity and information security of the operation of the ICS. Studies have shown [5,11,12-13,25] that the required (*in some or other conditions*) indicators of the efficiency of the operation of the ICS can be realized, including by using broadband radio systems for which the spreading of the spectrum is carried out using nonlinear discrete sequences.

A comprehensive solution to the problem of ensuring electromagnetic compatibility, noise immunity and information security of the operation of ICS can be achieved, including on the basis of the implementation of a dynamic information transfer mode, in which correspondence: the message bit - the signal changes over time according to a law whose prediction is possible with probability not exceeding the permissible value in the system, and applying signals with the necessary correlation, ensemble, statistical, structural properties. In this case, the signal systems must be based on nonlinear construction rules.

The proposed nonlinear discrete cryptographic signals, in contrast to the known signal classes used in various ICS applications, can be synthesized for any values of the period of discrete signals. The synthesis of this class of signals is based on the limitations associated with the boundary values of the auto and cross correlation functions of signals in the periodic and aperiodic modes of information transmission. The volume of the system of nonlinear cryptographic signals (*coding power*) is determined, first, by the requirements caused by the use of this class of signals (*detection and measurement of signal parameters, user data transfer mode, etc.*), and secondly, the requirements for the system with point of view of such indicators of the efficiency of the functioning of the telecommunications system, such as EMC noise immunity of signals reception, information concealment and imitation resistance of the system. The problem of synthesis of nonlinear discrete signals is formulated in general form. Under the cryptographic discrete signal, it is proposed to understand a sequence of symbols of an arbitrary alphabet and an arbitrary period, the only rule of construction

of which is randomness or pseudo-randomness. Such a discrete signal possesses the necessary but limited values of "tight packing", correlation and ensemble properties. With this approach, the structural concealment of the signal is provided through randomness or pseudo randomness. It is also necessary to note the special property of such signal systems - the possibility of their recovery in space and time with the use of keys and a number of other parameters that are used in the synthesis of signals. Taking into account the requirements of cryptographic stability and the complexity of generating a cryptographic signal as a signal generator, the choice of a symmetric block encryption algorithm with a counter is justified. As a block cipher it was proposed to use the national standard DSTU 7624: 2014. Alternatively, we can use the AES algorithm from the international standard ISO / IEC 18033. The preference is given to DSTU 7624: 2014, since in our opinion it refers to post-quantum algorithms, i.e. will provide (*when selecting the appropriate parameters*) cryptographic resistance against attacks with the use of quantum computers. CS are self-synchronized, and also have an ideal (absolute) structural concealment. The absolute structural concealment of such signals is that no subsequent bit, even the last, of such a signal can be uniquely determined with the prior symbols. It should be emphasized that the law for the formation of each of the cryptographic signals is determined by the key, and the length of the key can be substantially smaller than the period (length) of the signal itself.

The developed method for synthesizing a new class of nonlinear discrete signals allows changing the boundary values of the level of the side lobes of the corresponding correlation function, depending on the interference situation, as well as the requirements for the IRS, to achieve the necessary noise immunity of signal reception, imitating and information stealth of the system subscribers.

Synthesized systems complex signals possess, on the one hand, structural properties analogous to the properties of random (*pseudo-random*) sequences, and, on the other hand, the required ensemble and correlation properties, while improving the performance of ICS, in particular, EMC, noise immunity, information and structural stealth.

The characteristics of the auto- and mutual correlation functions of such signals are not inferior to those of the best ones from the point of view of the correlation properties of discrete sequences (*M-sequences, Gold and Kasami sets, Kamaletdinov ensembles, etc.).* In addition, cryptographic signal systems (CS) exist and possess the above properties, for a wide range of sequence period values. It is also necessary to note the special property of such signal systems – the possibility of their recovery in space and time with the use of keys and a number of other parameters that are used in the synthesis of signals. The improvement of the above mentioned indicators of the IKS operation is achieved, in particular, due to the possibility of forming, with the use of the obtained method, large discrete sequence ensembles of virtually any period with the necessary side-lobe values of the auto-mutual and butt-function correlation functions for various system applications periodic and aperiodic modes of operation, as well as statistical characteristics of correlation functions (CF), not inferior to similar characteristics of the best, in terms of CF, linear classes of signals. This makes it possible to improve the noise immunity of signal reception. The mathematical and software providing the proposed method and computational algorithms for the synthesis of systems of complex nonlinear discrete cryptographic signals, as well as derivatives of signal systems for which the coprocessors are used as the producing ones, are developed. During the research, an imitation (*software*) model was developed that implements the proposed method for synthesizing discrete cryptographic sequences. The obtained model allows: generating cryptographic signals of almost any period; to obtain minimum and maximum values of lateral emissions of periodic and aperiodic functions of auto- and cross-correlation of sequences; compare the values obtained with the known "close packing" boundaries; read selected, satisfying boundaries, sequences; assign unique identifiers to selected sequences for optimal signal processing in various applications of broadband systems. In addition, the proposed synthesis method makes it possible to synthesize pseudo-random sequences with zero values of the side peaks of the periodic auto and cross-correlation functions near the main peak, which is an important factor in maintaining stable synchronism in the system.

Software and mathematical support obtained in the course of research, realizing the methods of synthesis and research of the properties of nonlinear signal systems, including DSS, is practically

ready for possible use in the composition of prototypes and elements of modern digital communication means.

An improved method for synthesizing nonlinear discrete cryptographic signal systems is developed, based on the optimization of the synthesis of the signal system using the branch and boundary method, which makes it possible to reduce, in comparison with a full search, the volume of computational procedures for synthesizing signal systems and, consequently, necessary, for those or other applications of telecommunication systems, properties.

References

[1] Ipatov Valery P. Spread Spectrum and CDMA.Principles and Applications / Valery P. Ipatov. University of Turku, Finland and St. Petersburg Electrotechnical University 'LETI', Russia. – John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England. – 2005. – 385 p.

[2] Varakin L. E. Sistemy svyazi s shumopodobnymi signalami / Varakin L. E. – 1985. – 384 s.

[3] Sverdlik M. B. Optimal'nye diskretnye signaly / Sverdlik M. B. - M: Radio i svyaz', 1975. – 200 s.

[4] Sarvate, D.V. Crosleration Properties of Pseudorandom and Related Sequences / D.V. Sarvate, M.V. Pursley // IEEE Trans. Commun, 1980. – Vol. Com 68 – P. 59–90.

[5] Gorbenko I.D., Zamula A.A., Semenko Ye.A. Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications // Telecommunications and Radio Engineering. - Volume 75, 2016 Issue 2. pages 169-178.

[6] Gold, R. Optimal binary sequences for spread spectrum multiplexing // IEEE Trans. Inform. Theory.– 1967. Vol. 13. – P. 619–621.

[7] Karpenko O., Kuznetsov A., Sai V., Stasev Yu. Discrete Signals with Multi-Level Correlation Function // Telecommunications and Radio Engineering. – Volume 71, 2012 Issue 1. pages 91-98.

[8] Naumenko N.I., Stasev Yu.V., Kuznetsov A.A. Methods of synthesis of signals with prescribed properties // Cybernetics and Systems Analysis, Volume 43, Issue 3, May 2007, Pages 321-326.

[9] Stasev Yu.V., Kuznetsov A.A., Nosik A.M. Formation of pseudorandom sequences with improved autocorrelation properties // Cybernetics and Systems Analysis, Volume 43, Issue 1, January 2007, Pages 1–11.

[10] Lavrovska, T., Rassomahin, S. Physical model of pseudorandom codes in multidimensional Euclidean space. // 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, pp. 67-70.

[11] Gorbenko I.D., Gorbenko Ju.I. Prykladna kryptologija. Teorija. Praktyka. Zastosuvannja: monografija – Harkiv.: Vydavnyctvo «Fort», 2012. – 880 s. (in Ukrainian).

[12] Zamula A.A., Semenko E.A Perspektivy primeneniya nelineinykh diskretnykh signalov v sovremennykh telekommunikatsionnykh sistemakh i setyakh // Sistemi obrobki informatsiï:– Kh.: KhUPS, 2015. – Vip. 5 (130).– S. 129 - 134. (in Russian).

[13] Gorbenko I.D., Zamula A.A. Kriptograficheskie signaly: trebovaniya, metody sinteza, svoistva, primenenie v telekommunikatsionnykh sistemakh // Radiotekhnika: Vseukrainskii mezhvedomstvennyi nauchno – tekhnichneskii sbornik - 2016 g. - Vyp. 186. – S. 7–23. (in Russian).

[14] Application Notes and Interpretation of the Scheme (AIS) 31. Functionality classes and evaluation methodology for physical random number generators. Certification body of the BSI in context of certification scheme. BSI, 2001.

[15] DSTU 7624:2014. Informacijni tehnologii'. Kryptografichnyj zahyst informacii'. Algorytm symetrychnogo blokovogo peretvorennja. – Vved. 01–07–2015. – K.: Minekonomrozvytku Ukrai'ny, 2015. (in Ukrainian).

[16] Kuznetsov O., Gorbenko Y., Kolovanova I. Combinatorial properties of block symmetric ciphers key schedule. // 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, pp. 55-58.

[17] Kuznetsov O., Lutsenko M., Ivanenko D. Strumok stream cipher: Specification and basic properties // 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, pp. 59-62.

[18] ISCI'2017: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov. ASC Academic Publishing, USA, 2017. – 207 p.

[19] Kaidalov D., Oliynykov R., Kazymyrov O. A method for security estimation of the SPN-based block cipher against related-key attacks // Tatra Mountains Mathematical Publications. – Volume 60, Issue 1, Pages 25–45.

[20] Ruzhentsev V., Oliynykov R. Properties of Linear Transformations for Symmetric Block Ciphers on the basis of MDS-codes // Proceedings of the 6th International Conference on Network Architecture and Information System Security SAR-SSI 2011, pp. 193-196.

[21] Rodinko M., Oliynykov R.,Gorbenko Y. Improvement of the high nonlinear S-boxes generation method. // 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, pp. 63-66.

[22] Krasnobayev V.A., Yanko A.S., Koshman S.A. A Method for arithmetic comparison of data represented in a residue number system // Cybernetics and Systems Analysis. – January 2016. – Volume 52, Issue 1, pp. 145-150.

[23] NIST 800-90 b Recommendation for the Entropy Sources Used for Random Bit Generation, 2012.

[24] Potii A.V., Pesterev A.K. A System Approach to Certification of Pseudorandom Numbers Generators Used in Information Protection Systems // Telecommunications and Radio Engineering. – Volume 52, 1998 Issue 4. pages 97-102.

[25] I. D. Gorbenko, A. A. Zamula, A. E. Semenko, V. L. Morozov Method for complex improvement of characteristics of orthogonal ensembles based on multiplicative combining of signals of different classes// Telecommunications and Radio Engineering Volume 76, 2017 Issue 18, pages 1581-1594 .

Рецензент: Олексій Стахов, д.т.н., проф., академік Академії інженерних наук України, Міжнародний Клуб Золотого Перетину, Онтаріо, Канада. E-mail: goldenmuseum@rogers.com

Надійшло: Вересень 2017.

Автори:
Іван Горбенко, доктор технічних наук, професор, лауреат Державної премії України, професор кафедри безпеки інформаційних систем і технологій, ХНУ імені В.Н. Каразіна, майдан Свободи 4, м. Харків, 61022, Україна.
E-mail: gorbenkoi@iit.kharkov.ua

Владислав Морозов, аспірант кафедри безпеки інформаційних систем і технологій, ХНУ імені В.Н. Каразіна, майдан Свободи 4, м. Харків, 61022, Україна.
E-mail: morozov@boiko.com.ua

Олександр Замула, доктор технічних наук, професор кафедри безпеки інформаційних систем і технологій, Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, м. Харків, 61022, Україна.
E-mail: zamylaaa@gmail.com

Методи забезпечення електромагнітної сумісності у сучасних інформаційно-комунікаційних системах.

Анотація. Сформульовано вимоги до вибору систем складних сигналів – переносників даних для використання в багатокористувачевих широкосмугових телекомунікаційних системах (ШТС), в яких пред'являються підвищені вимоги до завадостійкості, електромагнітної сумісності, скритності і безпеки інформації. Наводяться концептуальні основи синтезу нового класу складних сигналів – криптографічні сигнали (КС). Обґрунтовується доцільність застосування в захищених широкосмугових телекомунікаційних системах похідних систем сигналів для підвищення ефективності, електромагнітної сумісності, завадостійкості прийому, скритності і інформаційної безпеки захищених ШТС.

Ключові слова: багатокористувачева система; евклідова відстань; ансамбль сигналів; криптографічний сигнал; система похідних ортогональних сигналів; кореляційна функція.

Рецензент: Алексей Стахов, д.т.н., проф., академик Академии инженерных наук Украины, Международный Клуб Золотого Сечения, Онтарио, Канада. E-mail: goldenmuseum@rogers.com

Поступила: Сентябрь 2017.

Авторы:
Иван Горбенко, доктор технических наук, профессор, лауреат Государственной премии Украины, профессор кафедры безопасности информационных систем и технологий, ХНУ имени В. Н. Каразина, площадь Свободы 4, г. Харьков, 61022, Украина.
E-mail: gorbenkoi@iit.kharkov.ua

Владислав Морозов, аспирант кафедры безопасности информационных систем и технологий, ХНУ имени В. Н. Каразина, площадь Свободы 4, г. Харьков, 61022, Украина.
E-mail: morozov@boiko.com.ua

Олександр Замула, доктор технических наук, профессор кафедры безопасности информационных систем и технологий, ХНУ имени В. Н. Каразина, площадь Свободы 4, г. Харьков, 61022, Украина.
E-mail: zamylaaa@gmail.com

Методы обеспечения электромагнитной совместимости в современных информационно-коммуникационных системах.

Аннотация. Сформулированы требования к выбору систем сложных сигналов – переносчиков данных для использования в многопользовательских широкополосных телекоммуникационных системах (ШТС), в которых предъявляются повышенные требования к помехоустойчивости, электромагнитной совместимости, скрытности и безопасности информации. Приводятся концептуальные основы синтеза нового класса сложных сигналов - криптографические сигналы (КС). Обосновывается целесообразность применения в защищенных широкополосных телекоммуникационных системах производных систем сигналов для повышения эффективности, электромагнитной совместимости, помехоустойчивости приема, скрытности и информационной безопасности защищенных ШТС.

Ключевые слова: многопользовательская система; евклидово расстояние; ансамбль сигналов; криптографический сигнал; система производных ортогональных сигналов; корреляционная функция.

Статті пройшли внутрішнє та зовнішнє рецензування.

Наукове видання

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА

Випуск 4(8) 2017

Міжнародний електронний науково-теоретичний журнал

Англійською, українською, російською мовами

Комп'ютерне верстання – Федоренко В.В., Єсіна М.В.

61022, Харків, майдан Свободи, 6
Харківський національний університет імені В.Н. Каразіна

V. N. Karazin Kharkiv National University Publishing