COMPUTER SCIENCE AND CYBERSECURITY

ISSUE 1(1) 2016

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 1(1) 2016

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 (June 24, 2016, protocol No. 8)

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-pages: *http://periodicals.karazin.ua/cscs (Open Journal System)*

Published articles have been internally and externally peer reviewed

TABLE OF CONTENTS

Issue 1(1) 2016

UDC 004.421.5

A PSEUDORANDOM SEQUENCES GENERATOR BASED ON THE MULTIMODULO TRANSFORMATION

Yurii Gorbenko[1], Tetiana Grinenko[2], Oleksii Nariezhnii[3], Nikołay Karpinskiy[4]

[1,3] V.N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
narlexa69@mail.ru

[2] Kharkiv National University of Radio Electronics, Nauka Ave, 14, Kharkov, 61166, Ukraine
t_lame@mail.ru

[4] University of Bielsko-Biala, Willowa St., 2, 43-309 Bielsko-Biala, Poland
mkarpinski@ath.bielsko.pl

Reviewer: Victor Krasnobayev, Dr., Full Professor, V.N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
krasnobayev@karazin.ua

Received on January 2016

Abstract. *Main theoretical statements and practical research results of pseudorandom sequences over arbitrary alphabet generation based on multimodulo transformation in the finite field GF(p^n) are given, results of properties analysis on distinguishing, unpredictability, irreversibility, repetition period and complexity (performance) are brought.*

Keywords: *pseudorandom sequence, pseudorandom sequence generator, multimodulo transformation, Galois field, distinguishing, unpredictability, irreversibility, repetition period, complexity.*

1 Introduction

The keys management tools are important components of cryptography systems, which characteristics and properties on, depend their resistance and the level of security in whole. At the different stages of key management it is needed to generate key data, key information and different options, having quite complex properties requirements. In practice, depending on the requirements, two methods are applied for key generation, based on random and pseudorandom sequences (PRS), which are brought about in the form of corresponding cryptographic tools.

As main demands to such generators are set out requirements of direct and reverse unpredictability (structural security), irreversibility concerning the used key, distinguishing of sequences, promptitude and repetition period difficulties for pseudorandom sequences are set out [1]. Wherein the level of key generators warranty depends to a considerable extent on the key source entropy, which should be from 128 to 512 bits for now.

Nowadays was developed a range of methods and PRS generation means on its basis. Their peculiarity is that they are built, well researched and applied as a rule for alphabet with $m = 2$ basis. At the same time a range of updates needs PRS generation means that can be resumed in space and time with acceptable complexity and random basis beginning with $m = 2$. The studies have shown that this problem can be solved through the transformations known as multimodulo.

Some regulations of multimodulo transformations for prime field $GF(p)$ are published in the work [2]. PRS generation on basis of multimodulo transformation in Galois field $GF(p)$ is offered in the work [2]. Such a method really allows generating PRS with random alphabet *m*, specified period of repetition and certain but not researched enough distinguishing properties. The elaboration of PRS generation method with certain alphabet of *m* symbols on basis of multimodulo transformations using Galois field $GF(p)$ elements, besides results of irreversibility and distinguishing properties research are published in the work [3]. The work [3] consists of definition of the conditions of pseudorandom sequences existence with equally possible letter distribution of *m* alphabet in

the class of multimodulo transformations and valuating of lower limit of irreversibility.

But in the mentioned works [2,3] a range of theoretical grounds of properties doesn't have generalized character of unified theory, in addition to that there wasn`t undertaken enough field research, which would verify theoretical results as regard to distinguishing, irreversibility, unpredictability, repetition period and complexity. The results of studies in works [2,3] also have constrained character, as they were undertaken only for multimodulo transformations over prime Galois field $GF(p)$.

The aim of the work is development of theoretical basis of PRS generation method with arbitrary alphabet of *m* symbols based on multimodulo transformations using elements of arbitrary Galois field, which at the theoretical stage would allow providing properties of distinguishing, irreversibility, unpredictability, repletion period and complexity for the finite field $GF(p^n)$ [1,4-6]. As a regard to this method it is needed to undertake a range of theoretical and field studies concerning definition of necessary and sufficient conditions of providing of predetermined repetition period, alphabet basis, probability of appearance of alphabet symbols at repetition period, features of irreversibility, unpredictability and distinguishing considering guarantees [4-7].

2 Method of multimodulo transformation in the finite field

Let us consider PRS generation method with certain symbols alphabet, for example *m*, on based on arbitrary Galois field $GF(p^n)$. For general case we will think that there is made up *k* transformations of units of Galois field $GF(p^n)$ extension, corresponding to modules $(f(X), f_1(X)),(f_1(X), f_2(X)),\ldots,(f_{k-2}(X), f_{k-1}(X))$ and the last module *m*. General options which are enough to generate elements a_i of $GF(p^n)$ field is tuple $(f(X), p, n, \theta_j)$, where $f(X)$ – irreducible polynomial of degree *n* over finite field $GF(p)$, and θ_j – primary element chosen from magnitude $\{\theta\}$ of division $\varphi(p^n-1)$, where $\varphi(\ )$ – Euler's function [8]. In such a case generation of field elements is carried out according to the rule:

$$a_i = (\theta_j)^i (\mathrm{mod}(f(X), p, n)). \quad (1)$$

It is shown [9], that if the above-said requirements to tuple $(f(X), p, n, \theta_j)$ have been fulfilled, (1) would generate finite Galois field with repetition period p^n-1. Let us denote that above-said is true for $p = 2,3,5,7$ and subsequent prime numbers. When $p = 2$, there will be extension of Galois field $F(2)$.

In the following, let $(f_s(X), p_s, n_s)$ be tuple of general options, for example of polynomials (among them irreducible) $f_s(X), s = (1, k-1)$, and n_s – their degrees, from this point on we need irreducibility of polynomials to provide their coprimality when necessary [9].

Also let degrees of polynomials (among them irreducible) n_s fulfill requirements:

$$n_1 > n_2,\ n_2 > n_3,\ \ldots,\ n_{k-2} > n_{k-1}, \quad (2)$$

wherein basis of m alphabet is any number, besides ineqautions are fulfilled:

$$p^{n_1} >> p^{n_2},\ p^{n_2} >> p^{n_3},\ldots, p^{n_{k-2}} >> p^{n_{k-1}},\ p^{n_{k-1}} >> m. \quad (3)$$

The statement 1 is fair.

Statement 1.

Deterministic PRS generator, which is functioning according to algorithm of multimodulo transformations:

$$b_i = ((\theta_j)^i (\mathrm{mod}(f(X), p, n), (f_1(X), p_1, n_1), (f_2(X), p_2, n_2),\ldots \quad (4)$$

$$\ldots, (f_{k-1}(X), p_{k-1}, n_{k-1}), (f_m(X), m)),$$

where $(f_s(X), p_s, n_s)$ – tuple of general options, m – certain integer, k – degree of multi modulari-

ty, p_m – number (not necessarily prime), m – positive integer, provides generation of PRS (symbols) with repetition period $p^n - 1$, equally possible with a certain basis of m alphabet, under condition that:

1) (1)–(3) requirements are fulfilled;

2) modules (couple of polynomials)

$$\left(f(X), f_1(X)\right), \left(f_1(X), f_2(X)\right), \ldots, \left(f_{k-2}(X), f_{k-1}(X)\right) \tag{5}$$

are coprime and tuple $\left(f_m(x), m\right)$ is undefined.

In (4) $\left(f_m(x), m\right)$ means that module *m* is given as a polynomial.

Under fulfillment of (4)–(5) conditions PRS (symbols) generation is provided with following properties and characteristics:

– arbitrary alphabet *m* basis;

– $p^n - 1$ repetition period;

– symbols are generated equally possible or "almost" equally possible;

– by ensemble of isomorphism's $\varphi\left(p^n - 1\right)$.

The statement 2 is fair too.

Statement 2.

Deterministic PRS generator, which is functioning according to algorithm of multimodulo transformations:

$$b_i = \left(\left(\theta_j\right)^{K_0+i}\left(\mathrm{mod}\left(f(X), p, n\right), \left(f_1(X), p_1, n_1\right), \left(f_2(X), p_2, n_2\right), \ldots\right.\right. \tag{6}$$

$$\left.\left. \ldots, \left(f_{k-1}(X), p_{k-1}, n_{k-1}\right), \left(f_m(X), \overleftarrow{m}\right)\right)\right),$$

where $K_0 + i$ – current generator key, wherein K_0 is primary key and i is session key, which is noninvertible with complexity not less than $O(n)$ [10].

Let us further observe isolated case of statements 1 and 2 for three modulo transformation, when elements of Galois field extension are also generated according to (1), but (2)–(6) take the form of (7)–(10):

$$n_1 > m. \tag{7}$$

$$p^{n_1} >> p^m. \tag{8}$$

$$b_i = \left(\left(\theta_j\right)^i\left(\mathrm{mod}\left(f(X), p\right), \left(f_1(X), p_1, n_1\right), \left(f_m(X), \overleftarrow{m}\right)\right)\right). \tag{9}$$

$$b_i = \left(\left(\theta_j\right)^{K_0+i}\left(\mathrm{mod}\left(f(X), p\right), \left(f_1(X), p_1, n_1\right), \left(f_m(X), \overleftarrow{m}\right)\right)\right). \tag{10}$$

For conditions (7)–(10) let us present statement 1 for three modulo transformation in form of theorem 1.

Theorem 1. Deterministic PRS generator, which is functioning according to algorithm of multimodulo transformations on the basis (1) according to the rules:

$$b_i = \left(\left(\theta_j\right)^i\left(\mathrm{mod}\left(f(X), p, n\right), \left(f_1(X), p_1, n_1\right), \left(f_m(X), \overleftarrow{m}\right)\right)\right) \tag{11}$$

or

$$b_i = \left((\theta_j)^{k_0+i} \left(\mathrm{mod}\left(f(X), p, n \right), \left(f_1(X), p_1, n_1 \right), \left(f_m(X), \tilde{\tilde{m}} \right) \right) \right), \quad (12)$$

under fulfillment of conditions (2)–(8) provides generation of PRS (symbols) numbers with undefined basis of *m* alphabet, with repetition period $p^n - 1$, with equally possible appearance of symbols at the repetition period $p^n - 1$ and with ensemble of isomorphism $\varphi(p^n - 1)$.

Theorem 1 for three modulo transformation proving.

Regarding the last module *m* it can take arbitrary value and it will be presented as polynomial. Let us mark that $f(x)$ and $f_1(x)$ in (11) are irreducible polynomials, which can be presented over the field $F(2)$, i.e. as polynomial of n degree over $F(2)$.

In regard to repetition period, since $\{\theta_i\}$ – primary elements, for providing maximum period $p^n - 1$ it is necessary and enough for $f(x)$ to be irreducible over the field $GF(p^n)$ [9]. Since $f(x)$ is irreducible over the field $GF(p^n)$, according to (1) elements of Galois field are generated with period $p^n - 1$ and each element appears only one time.

Let us define m-symbols (finite alphabet) appearance equiprobability degree, i.e. define conditions, under which symbols of m alphabet appear equally possible. Symbols will be determined with the help of polynomials $f_m(x)$ not higher than n_m degree.

Let us present all elements of field $GF(p^n)$ as positive integers from $\theta^0 = 1$ to $p^n - 1$.

Then let us sort numbers $1 \div p^n - 1$ according to the ascending order

$$1, 2, 3, \ldots, |f(x)|, |f(x)|+1, \ldots, 2|f(x)|, 2|f(x)|+1, \ldots, 3|f(x)|, 3|f(x)|+1, \ldots \quad (13)$$

$$\ldots, p^n - 1 - f(x), p^n - f(x), \ldots, p^n - 1,$$

where $|f(x)|$ is element value of field $f(x)$.

Let us bring the row (13) according to module $|f_1(x)|$, as a result we will get:

$$1, 2, 3, \ldots, |f_1(x)|\text{-}1, 0, 1, 2, 3, \ldots, |f_1(x)|\text{-}1, 0, 1, 2, 3, \ldots, |f_1(x)|\text{-}1, 0, 1, \ldots, V, \quad (14)$$

where $0 \le V \le |f_1(x)| - 1$.

Let us present the array (14) as:

$$\overbrace{1,2,3,\ldots,|f_1(x)|-1,0;}^{1} \ \overbrace{1,2,3,\ldots,|f_1(x)|-1,0;}^{2} \ldots \quad (15)$$

$$\ldots; \overbrace{1,\ 2,\ 3,\ldots,\ |f_1(x)|-1,0;}^{z-1} \ \overbrace{1,\ 2,\ 3,\ldots,\ V}^{z},$$

where $V \le |f_1(x)| - 1$.

On the whole there will be sequence elements $((z-1)|f_1(x)| + V$ in the PRS (15). Besides in the last unit there will be no sequence elements beginning with $(V+1)$ to $|f_1(x)| - 1$ and 0.

Farther on symbols $1, 2, 3, \ldots, V$ appear z times $V+1, V+2, \ldots, |f_1(x)| - 1, 0$ – $(z-1)$ times.

Probabilities of elements $1, 2, 3, \ldots, V$ appearance will be correspondingly:

$$R_1 = \frac{z}{p^n - 1}, \quad (16)$$

and $V+1, V+2, \ldots, |f_1(x)| - 1, 0$

$$R_2 = \frac{z-1}{p^n - 1}. \quad (17)$$

Thus symbols $1,2,3,\ldots,|f_1(x)|-1,0$ appear almost with almost equal probability, i.e. equally possible at the period $p^n - 1$ as a result of conversion according to the second $|f_1(x)|$ module.

Let us observe the stage of conversion according to the third module, which is according to the theorem 1, can be undefined number $|f_m(x)|$.

While analyzing for frequency let us define an array $0,1,2,3,\ldots,|f_1(x)|-1$ as

$$1,2,3,\ldots,|f_1(x)|. \quad (18)$$

We will bring (18) together according to module $|f_m(x)|$ and get the row:

$$1,2,3,\ldots,|f_m(x)|-1,0,1,2,3,\ldots,|f_m(x)|-1,0,1,2,3,\ldots,|f_m(x)|-1,0,1,2,3,\ldots,V, \quad (19)$$

where $0 \le V \le |f_m(x)|-1$.

Analyzing in (19) $0,1,2,3,\ldots,|f_m(x)|-1$ symbols appearance probability we will get the same assed values as in (16) and (17).

It is also should be pointed out that in (16) V symbols appearance unequiprobability is no more than 1 in number of appearance of symbols $0,1,2,3,\ldots,V$, and also as an assessed value of probability for each symbol $\Delta p = \frac{1}{p^n - 1}$.

Thus theorem 1 for three modulo transformation is proved. Also it should be mentioned that above-described theorem 1 proving can be applied to *k*-modulo transformation, of course under condition when couples of polynomials $(f(X), f_1(X)),(f_1(X), f_2(X)),\ldots,(f_{k-2}(X), f_{k-1}(X))$ are coprime and tuple $f_m(X), m$ is undefined, module *m* value is meant.

On the whole the procedure of PRS generation based on multimodulo transformation can be brought to the following.

1. To set or generate system options – general options tuples $(f_s(X), p_s, n_s)$ according to the requirement of statement 1.

2. To set or install secret key of generator k, $k = 1 \div p^n - 1$.

3. Determine initial value of generator a_0 using the rule:

$$a_0 = \theta^k (\mathrm{mod}(f(x), n)),$$

where $(f(x), n)$ – basic transformation module.

4. Determine element a_i of generator using the rule:

$$a_i = a_{i-1}\theta(\mathrm{mod}(f(x), n)) = R_{(f(x),n_1)}(a_0\theta^i),$$

where $i \ge 1$ – number of PRS generating element, a_{i-1} – $(i-1)$ element of an array over a field of extension p^n.

5. Determine element b_i of PRSG using the rule:

$$b_i = a_i(\mathrm{mod}(f_1(x), n_1)) = R_{(f_1(x),n_1)}(a_i) = R_{(f_1(x),n_1)}\left(R_{(f(x),n)}(a_0\theta^i)\right),$$

where $1 < (f_1(x), n_1) < (f(x), n)$.

6. Determine element c_i of PRSG using the rule:

$$c_i = R_{(f_n(x),m_n)}\left(R_{(f_{n-1}(x),m_{n-1})}\left(\ldots\left(R_{(f_2(x),m_2)}\left(R_{(f_1(x),m_1)}(a_0\theta^i)\right)\right)\ldots\right)\right), 0 \le i \le \varphi(p),$$

where $i \ge 1$ – the number of PRS generating element, $(f_1(x), n_1),\ldots,(f_n(x), n_n)$ – intermediate modules.

7. If necessary determine hash-value number i from b_i and accept it as random word number i, i.e.:

$$y_i = H(b_i).$$

The scheme of algorithm (variant) that implements above-described method of determined random number generator (DRNG) is illustrated on fig. 1.

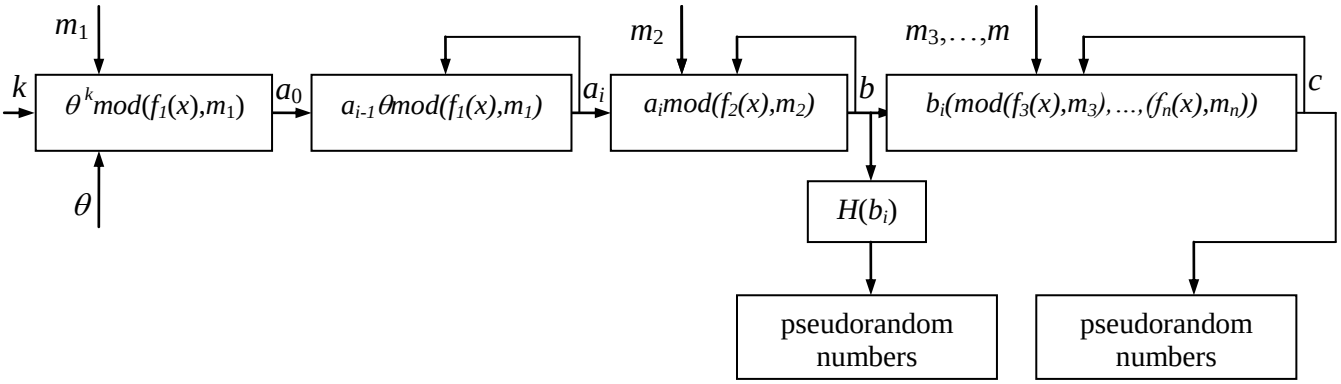

Fig.1 – The scheme of algorithm of determined random sequences generation in the finite field of $p^n - 1$ division by method of multimodulo transformation

3 Properties of PRS of multimodulo transformations

Let us farther observe the method of PRS generation with certain alphabet of symbols, e.g. m, based on multimodulo transformations in finite Galois field $GF(p^n)$, $n \geq 1$. It is considered that k transformations of Galois field $GF(p^n)$ extension elements are carried out according to modules $(f(X), f_1(X)), (f_1(X), f_2(X)), \ldots, (f_{k-2}(X), f_{k-1}(X))$ and the last module m. General options is tuple $(f(X), p, n, \theta_j)$, where $f(X)$ – irreducible polynomial of *n* degree over field $GF(p)$, and θ_j – primary element chosen from magnitude $\{\theta\}$ of division $\varphi(p^n - 1)$.

We will also observe special case of theorem 1 for three modulo transformation. In this case Galois field extension elements are also generated according to (1). And in such a case (2)–(6) look like:

$$n_1 > m \text{ i } p^{n_1} >> p^m;$$

$$b_i = \left((\theta_j)^{K_0+i} \left(\operatorname{mod}(f(X), p), (f_1(X), p_1, n_1), \left(f_m(X), \overline{m} \right) \right) \right),$$

where $K_0 + i$ is current generator key, $K_0 + i$ is primary key and i is session key as above.

Complexity assessment of PRS generator inversion.

Let us make complexity assessment of discrete logging for three modulo and multimodulo transformations.

In a case of finite Galois field $GF(p)$ we have:

$$b_i = \left((\theta_j)^X (\operatorname{mod}(P), (P_1), (m)) \right), \quad (20)$$

where $X = K_0 + i$ belongs to definition, under condition, that some array of symbols b_i is known, primary element θ_j and tuple of options (P, P_1, m).

While using «brute force» attack can be applied the following main methods: keys search, table attack and attack with dictionary [11,12].

While applying «brute force» attack it is considered that the length of key k is not more than the one of generated PRS and counterfeiter while searching key X, make an attempt to get a value

$$b_i^* = b_i . \quad (21)$$

Under condition fulfillment (21) generator key will be determined.

For assessment of possibility of applying «brute force» attack can be used such data as N_k – number of keys, safe time t_s, P_p – probability of successful cryptanalysis, etc [11,12,13]. Value t_s can be determined according to the formula [13]:

$$t_s = \frac{N_k}{\gamma K} P_p ,$$

where γ – capacity of cryptanalytic system, $K = 3.15 \cdot 10^7$ – the number of seconds in a year.

Table attack and attack with dictionary based on using mathematical tool called «birthday problem»: method of collisions creation [14]. For this method options: collisions probability P_k, cryptanalyst's attempts number k and exhaustive set of possible output values n are bounded with each other with parametric equation [14,15]:

$$1 - P_k = e^{-(k(k-1))/2n}$$

or of closed form :

$$k^2 - k + 2n \ln(1 - P_k) = 0 . \quad (22)$$

Correlation (22) allows assessing a number of experiments needed to carry out to implement collision with applying mathematical tool «birthday problem».

In some cases couple «generator key – PRS output unit» can be received with the help of a dictionary. In such a case couples «generator key – PRS output unit» are generated or collected in the special dictionary. And key search is implemented by method of PRS embedding searching that corresponds to generator output according to the dictionary.

Let us carry out an analysis of possibilities and conditions of implementation of attack like «brute force», which is carried out in regard to (20) with an aim of field $(\theta_j)^X \pmod p$ element determining. In a case of (20) for achieving (21) let us observe model of transformation of m-ary symbol into p-ary one.

Let the lengths of symbols in binary representation be l_p, l_{p_1} and l_m correspondingly to modules p, $p1$ and m. Let us define the possibility of guessing through b_i symbol of p-ary symbol, in essence definition of $\theta_j^{K_0+i}$.

Theorem 2. For conditions (20) possibility of correct (guessing) transformation of P_{CT} m-ary b_i symbol into p-ary $\theta_j^{K_0+i}$ is determined with correlation:

$$P_{\text{CT}} = 2^{l_m - l_p} , \quad (23)$$

where l_p and l_m – binary representation of lengths of symbols p and m.

Let us observe theorem 2 proving. When the length of m-ary b_i symbol in binary representation is l_m, the number of his possible modes is defined as 2^{l_m}. During transformation according to module p_1 the length of symbol in binary representation will be l_{p_1} and the number of possible modes will be defined as $2^{l_{p_1}}$. Where degree of alphabet extension can be assessed as

$$\mu_2 = 2^{l_{p_1}} \Big/ 2^{l_m} = 2^{l_{p_1} - l_m} .$$

During transformation according to module p the length of symbol in binary representation will be l_p, and the number of possible modes will be defined as 2^{l_p}. Degree of alphabet extension during switching to transformation according to p will be:

$$\mu_1 = 2^{l_p} \Big/ 2^{l_{p_1}} = 2^{l_p - l_{p_1}} .$$

Correspondingly the possibility of guessing an alphabet symbol according to module p_1 is defined as

$$P_{p_1} = 1/\mu_2 = 2^{l_m - l_{p_1}}. \quad (24)$$

The possibility of guessing an alphabet symbol according to module p is defined as

$$P_p = 1/\mu_1 = 2^{l_{p_1} - l_p}. \quad (25)$$

Thus theorem is proved. The general possibility of guessing an alphabet P_{G} symbol according to module p during switching from m-ary source to p-ary will be defined with multiplication of events P_{p_1} (24) and P_p (25), i.e.:

$$P_{\text{G}} = P_{p_1} \cdot P_p = 2^{l_m - l_{p_1}} \cdot 2^{l_{p_1} - l_p} = 2^{l_m - l_p}. \quad (26)$$

Using (26) the one can define complexity I_{G} of one alphabet symbol according to module p during switching from m-ary source to p-ary as

$$I_{\text{G}} = 1/P_{\text{в}} = 2^{l_p - l_m}.$$

Thus while applying of generator scheme without hashing the complexity I_{KR} of key reconstruction $X = K_0 + i$ is determined with a formula:

$$I_{\text{KR}} = I_{\text{G}} \cdot I_{\text{DL}} = 2^{l_p - l_m} \cdot \exp\left(\varepsilon \ln(p)^{\upsilon} \ln\ln(p)^{(1-\upsilon)}\right). \quad (27)$$

For a case of applying of generator schemes with guessing a field element, discrete logarithm solution and hashing the complexity I_{KRH} of key reconstruction $X = K_0 + i$ is determined with a formula:

$$I_{\text{KRH}} = I_{\text{G}} \cdot I_{\text{DL}} \cdot I_{\text{H}} = 2^{l_p - l_m} \cdot \exp\left(\varepsilon \ln(p)^{\upsilon} \ln\ln(p)^{(1-\upsilon)}\right) \cdot 2^{n/2}. \quad (28)$$

It is necessary to point out that formulae (27) and (28) received for a case, when PRS is produced by mean of applying only one m-ary symbol. If for producing of PRS μ of m-ary symbols is used and value of i is getting bigger according to a known rule, then (27) and (28) can be applied to assessment of cryptographic resistibility of offered PRS generator. If i is getting bigger according to an unknown rule, then besides it is necessary to solve a task of determination of rule of its changing. But as we consider that cryptanalyst knows the rule of i changing, (27) and (28) are recommended for assessment of PRS generators inversion complexity of a type that is observed. In the Table 1 are given assessments of PRS generator inversion complexity according to (27) and (28). Data analysis of Table 1 allows making a conclusion that PRS generator inversion complexity has an exponential character and it is bigger than complexity of «brutal force» method.

Table 1 – Complexity of generator inversion

Method		p , p_1 , m				
		2^{256}, 2^{128}, 2^{8}	2^{256}, 2^{128}, 2^{64}	2^{512}, 2^{256}, 2^{8}	2^{1024}, 2^{512}, 2^{256}	2^{2048}, 2^{1024}, 2^{512}
I_{KR}		$5.0543 \cdot 10^{089}$	$7.0143 \cdot 10^{072}$	$2.1618 \cdot 10^{172}$	$1.4827 \cdot 10^{259}$	$1.1867 \cdot 10^{500}$
I_{KRH}	n					
	160	$6.1103 \cdot 10^{113}$	$8.4798 \cdot 10^{096}$	$2.6135 \cdot 10^{196}$	$1.7925 \cdot 10^{283}$	$1.4346 \cdot 10^{524}$
	256	$1.7199 \cdot 10^{128}$	$2.3868 \cdot 10^{111}$	$7.3562 \cdot 10^{210}$	$5.0453 \cdot 10^{297}$	$4.0381 \cdot 10^{538}$
	384	$3.1726 \cdot 10^{147}$	$4.4029 \cdot 10^{130}$	$1.3570 \cdot 10^{230}$	$9.3071 \cdot 10^{316}$	$7.4490 \cdot 10^{557}$
	512	$5.8524 \cdot 10^{166}$	$8.1219 \cdot 10^{149}$	$2.5031 \cdot 10^{249}$	$1.7168 \cdot 10^{336}$	$1.3741 \cdot 10^{577}$

Let us observe one more way to solve a task of PRS generator inversion of the form (20), which is based on residue classes. For this aim let us give (20) of the following form:

$$\begin{aligned} & b_i = \Theta^{x_i} \pmod P \pmod{P_1} \pmod m, \\ & \Theta^{x_i} \pmod P \pmod{P_1} = q_i \cdot m + b_i,\ 0 \le q_i \cdot m + b_i < P_1, \\ & \Theta^{x_i} \pmod P = l_i \cdot P_1 + q_i \cdot m + b_i,\ 0 \le l_i \cdot P_1 + q_i \cdot m + b_i < P, \\ & \Theta^{x_i} \pmod P = l_i \cdot P_1 + q_i \cdot m + b_i \pmod P. \end{aligned} \tag{29}$$

Direct analysis (29) is showing that x_i, l_i, q_i are unknown and should be determined. Now let us take into account that rule of changing of x_i is known. On the basis of (29) it is possible to make equation system of the following form:

$$\begin{cases} \Theta^{x_i} \pmod P = l_i \cdot P_1 + q_i \cdot m + b_i \pmod P; \\ \Theta^{x_{i+1}} \pmod P = l_{i+1} \cdot P_1 + q_{i+1} \cdot m + b_{i+1} \pmod P; \\ \ldots\ldots\ldots\ldots \\ \Theta^{x_{i+k}} \pmod P = l_{i+k} \cdot P_1 + q_{i+k} \cdot m + b_{i+k} \pmod P. \end{cases} \tag{30}$$

The equation system (29) analysis is showing that each new equation in the system adds 2 variables, but there exists linear dependence between x_i and x_{i+1} etc. On the whole in a system of k division there will be $2k+1$ variables, even if we consider that only x_i is variable.

Thus an equation system of the form of (30) with $2k+1$ variables has no solution. Also it should be pointed out that by analogy with three modulo transformation, during multimodulo transformation every new additional modulo transformation adds two variables.

Thus properties of inconvertibility of PRS generator in essence are connected with solving of discrete logarithm equations, e.g. for three modulo transformations of the form of (6) as to i and $K_0 + i$.

For a successful cryptanalysis of generator, firstly, it is needed to solve a discrete logarithm equation and find element – operand. First of all in this case operand of correspondent element of A_i field should be found, and then a discrete logarithm equation with complexity I_{DL} should be solved.

For condition (20) a possibility of correct transformation (of guessing) of P_{CT} of m-ary b_i symbol into p-ary $\theta_j^{K_0+i}$ is determined with correlation (23).

The equation system analysis (29) is showing, that every new equation in the system adds 2 variables; in addition to this there exists linear dependence between x_i and x_{i+1} etc. In a system of k-division there will be $2k+1$ variables. That is why an equation system of the form of (30) with $2k+1$ variables has no solution.

4 Investigation of distinguishing properties of PRS generated on the basis of multimodulo transformations

Applying of PRS on the basis of multimodulo transformations in the finite fields $GF(p)$ and $GF(p^n)$ is possible only under condition of providing good distinguishing properties. Where by distinguishing is meant degree of resembling of PRS to physically random sequence. The main requirements to such sequences from the point of distinguishing are given in [4,6,7].

Below are given the results of assessments in regard to properties of distinguishing of PRS generation based on multimodulo transformations in finite Galois fields $GF(p)$ and $GF(p^n)$, which output values are hashed.

The four types of PRSG are considered. The first one is PRSG in the field $GF(p)$ without hashing; the second one is PRSG in $GF(p)$ with hashing, the third one is PRSG in the field $GF(p^n)$ without hashing, the fourth one is PRSG in $GF(p^n)$ with hashing according to [13,14].

4.1 PRSG with multimodulo transformation in the field $GF(p)$

Data used during PRSG implementation is given below. On the whole there were implemented 10 PRSGs with different output options (Table 2).

PRSG options without hashing.

The value of the first module p with the size of 1024 bytes was chosen from ISO/IEC 9796-3 standard [15], besides it was the same for all implementations:

p=ffffffffffffffffc90fdaa22168c234c4c6628b80dc1cd129024e088a67cc74020bbea63b139b22514a0 8798e3404ddef9519b3cd3a431b302b0a6df25f14374fe1356d6d51c245e485b576625e7ec6f44c42e9 a637ed6b0bff5cb6f406b7edee386bfb5a899fa5ae9f24117c4b1fe649286651ece65381ffffffffffffffff.

The value of the second module p_1 (160 bytes) was also chosen from ISO/IEC 9796-3 standard [15], the same for all implementations:

p_1 =ffd5d55fa9934410d3eb8bc04648779f13174945.

The value of the third module was chosen the same for all implementations, i.e. the alphabet basis $m = 2$.

The value of primary element θ (1023 bytes) was chosen from ISO/IEC 9796-3 standard [15], the same for all implementations:

θ =7fffffffffffffffe487ed5110b4611a62633145c06e0e68948127044533e63a0105df531d89cd912 8a5043cc71a026ef7ca8cd9e69d218d98158536f92f8a1ba7f09ab6b6a8e122f242dabb312f3f637a2 62174d31bf6b585ffae5b7a035bf6f71c35fdad44cfd2d74f9208be258ff324943328f67329c0fffffffffff fffff.

The value of generator k key for all implementations was generated at random under condition that $k = 1 \div p - 1$. The values of PRSG options are given in the table 2.

Table 2 – PRSG options in $GF(p)$ used during testing

PRSG implementation	Size p, bytes	Size p_1, bytes	Value m	Size θ, bytes	k, 128 bytes
1	1024	160	2	1023	e6894898f9976ba42761f201cc2ff016
2	1024	160	2	1023	84b1c668a99815a269eb15fc87315efc
3	1024	160	2	1023	f4bf155fa99f25a259ebf5f1f73f5ef1
4	1024	160	2	1023	44b4554a541473419942eb45a2595e41
5-SHA-1 (3)	1024	160	–	1023	f4bf155fa99f25a259ebf5f1f73f5ef1
6-SHA-1 (4)	1024	160	–	1023	44b4554a541473419942eb45a2595e41
7-SHA-256 (1)	1024	160	–	1023	e6894898f9976ba42761f201cc2ff016
8-SHA-384(1)	1024	160	–	1023	e6894898f9976ba42761f201cc2ff016
9-SHA-384 (2)	1024	160	–	1023	84b1c668a99815a269eb15fc87315efc
10-SHA-512 (1)	1024	160	–	1023	e6894898f9976ba42761f201cc2ff016

The results of experimental research of theses generators are given in the tables 3 and 4.

4.2 PRSG with transformations in the field $GF(p^n)$

The research of such a PRSG was carried out without hashing. On the whole 5 PRSGs with different output options were implemented.

The value of the first module $f_1(x)$ was chosen from DSTU 4145 [16] the same for all implementations:

$$f_1(x)=x431+x5+x3+x+1.$$

The value of the second module $f_2(x)$ was chosen from DSTU 4145 the same for all implementations:

$$f_2(x)=x163+x7+x6+x3+x+1.$$

The value of the third module $f_3(x)$ was chosen from DSTU 4145 the same for all implementations:

$$f_3(x)=28.$$

The value of primary element θ was chosen from DSTU 4145 the same for all implementations:

θ = x425 + x424 + x423 + x422 + x419 + x418 + x417 + x412 + x406 + x403 + x400 + x395 + x394 + x393 + x392 + x390 + x389 + x387 + x385 + x382 + x381 + x380 + x375 + x371 + x370 + x369 + x368 + x367 + x366 + x361 + x358 + x357 + x355 + x354 + x352 + x351 + x350 + x349 + x348 + x347 + x346 + x345 + x343 + x339 + x338 + x333 + x332 + x331 + x330 + x328 + x325 + x322 + x321 + x320 + x319 + x318 + x314 + x311 + x310 + x309 + x308 + x307 + x304 + x302 + x299 + x298 + x297 + x294 + x293 + x291 + x288 + x280 + x277 + x276 + x274 + x271 + x270 + x268 + x266 + x264 + x263 + x261 + x260 + x259 + x258 + x257 + x256 + x255 + x254 + x253 + x252 + x251 + x248 + x247 + x243 + x239 + x238 + x236 + x235 + x231 + x230 + x228 + x225 + x223 + x219 + x217 + x215 + x213 + x211 + x210 + x209 + x207 + x205 + x203 + x202 + x201 + x199 + x198 + x196 + x195 + x194 + x193 + x191 + x188 + x186 + x185 + x184 + x182 + x180 + x179 + x176 + x173 + x172 + x170 + x169 + x167 + x166 + x162 + x161 + x158 + x157 + x155 + x153 + x152 + x151 + x149 + x147 + x146 + x142 + x140 + x137 + x136 + x134 + x133 + x131 + x129 + x128 + x124 + x123 + x119 + x117 + x115 + x114 + x113 + x109 + x107 + x106 + x104 + x103 + x102 + x97 + x96 + x92 + x89 + x87 + x86 + x83 + x81 + x78 + x75 + x72 + x69 + x68 + x64 + x60 + x58 + x57 + x56 + x55 + x54 + x52 + x51 + x49 + x47 + x45 + x42 + x38 + x37 + x35 + x32 + x31 + x30 + x26 + x25 + x22 + x15 + x14 + x11 + x9 + x7 + x6 + x5 + x4 + x + 1.

The value of generator k key was generated at random under condition that $k = 1 \div p^n - 1$.

1 – DRNG in $GF(p^n)$: k =x207 + x206 + x205 + x204 + x203 + x202 + x201 + x200 + x199 + x198 + x197 + x196 + x195 + x194 + x193 + x192 + x187 + x186 + x185 + x183 + x182 + x181 + x179 + x177 + x174 + x173 + x172 + x171 + x165 + x160 + x129 + x128 + x122 + x120 + x119 + x117 + x116 + x115 + x114 + x113 + x112 + x111 + x109 + x104 + x101 + x98 + x82 + x81 + x80 + x77 + x75 + x74 + x73 + x72 + x71 + x70 + x69 + x68 + x67 + x65 + x64 + x4 + x2 + 1;

2 – DRNG in $GF(p^n)$: k =0xFFFF 0EEA7821 00000003 05bfa124 00072FFB 00000007 00000015;

3 – DRNG in $GF(p^n)$: k =0x151 1596FBBC 47F9B44C ADBC8541 9841BACD FF841632 001F589F 0EEA7821 0034814F 05BFA124 02F846FB 07894ABC 05519584;

4 – DRNG in $GF(p^n)$: k =0x3CE 10490F6A 708FC26D FE8C3D27 C4F94E69 0134D5BF F988D8D2 8AAEAEDE 975936C6 6BAC536B 18AE2DC3 12CA4931 17DAA469 C640CAF3;

5 – the implementation 2 of DRNG in $GF(p^n)$ with hashing with the help of SHA-384.

The data of experimental research of theses generators are given in the tables 3 and 4.

For testing of developed PRSG was applied NIST STS method, recommended by the National Institute of Standards and Technology USA [6]. NIST STS packet consists of 16 static tests. These

tests are applied for checking of the hypothesis about randomness of binary arrays of undefined length have generated by RSG or PRSG. Taking into consideration the results of all the tests the decision about, whether array of zeros and units will be set at random or not, is made.

With application of NIST STS method was carried out a testing of pseudorandom sequences and also properties comparison of these sequences with properties of PRS generator of pseudorandom bytes BBS (test sample, recommended by NIST). The data about PRS tests pass according to the rule 1 [6] is given in the table 3. And the data about BBS generator was taken for reference.

Table 3 – The results of PRS testing on distinguishing according to the rule 1

Generator	Tests quantity, which passed more than 99% arrays	Tests quantity, which passed more than 96% arrays
BBS	134 (70,8%)	189 (100%)
1 - DRNG $GF(p)$	136 (71,95%)	189 (100%)
2 - DRNG $GF(p)$	124 (65,6%)	189 (100%)
3 - DRNG $GF(p)$	140 (74,07%)	187 (98,94%)
4 - DRNG $GF(p)$	130 (68,78%)	187 (98,94%)
5 - SHA-1 (3)	128 (67,72%)	189 (100%)
6 - SHA-1 (4)	129 (68,25%)	189 (100%)
7 - SHA-256 (1)	129 (68,25%)	189 (100%)
8 - SHA-384 (1)	143 (75,66%)	189 (100%)
9 - SHA-384 (2)	130 (68,78%)	188 (100%)
10 - SHA-512 (1)	122 (64,55%)	189 (100%)
1 - DRNG $GF(p^n)$	138 (73%)	189 (100%)
2 - DRNG $GF(p^n)$	132 (69,84%)	187 (98,94%)
3 - DRNG $GF(p^n)$	126 (66,67%)	189 (100%)
4- DRNG $GF(p^n)$	134 (70,8%)	187 (98,94%)
5-SHA-384 2- DRNG $GF(p^n)$	139 (73,5%)	189 (100%)

In the table 4 is given the summary data about tests passes by generators according to the rule 2 [6].

Table 4 – The results of PRS testing on distinguishing according to the rule 2

Generator	Tests quantity, in which possibility value is $P \le 0{,}01$	Tests quantity, in which possibility value is $P \le 0{,}001$
1	**2**	**3**
BBS	0	0
1 - DRNG $GF(p)$	4	0
2 - DRNG $GF(p)$	3	0
3 - DRNG $GF(p)$	4	0
4 - DRNG $GF(p)$	0	0
5 - SHA-1 (3)	2	0
6 - SHA-1 (4)	2	0
7 - SHA-256 (1)	2	0
8 - SHA-380 (1)	1	0
9 - SHA-380 (2)	0	0
10 - SHA-512 (1)	2	0

Continuation of Table 4

1	2	3
1 - DRNG $GF(p^n)$	0	0
2 - DRNG $GF(p^n)$	4	0
3 - DRNG $GF(p^n)$	2	0
4 - DRNG $GF(p^n)$	1	0
5-SHA-384 2- DRNG $GF(p^n)$	1	0

In the fig. 2 and 3 as examples are given phase portraits of distinguishing received with the application of NIST STS [6] test method. Their analysis allows making a conclusion about high quality of distinguishing (randomness).

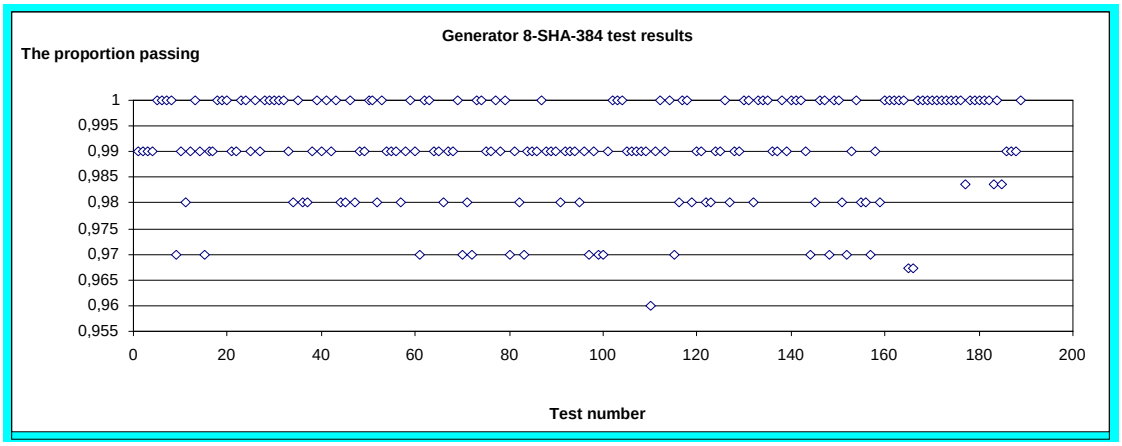

Fig. 2 – The results of experimental research of DRNG 8-SHA-384

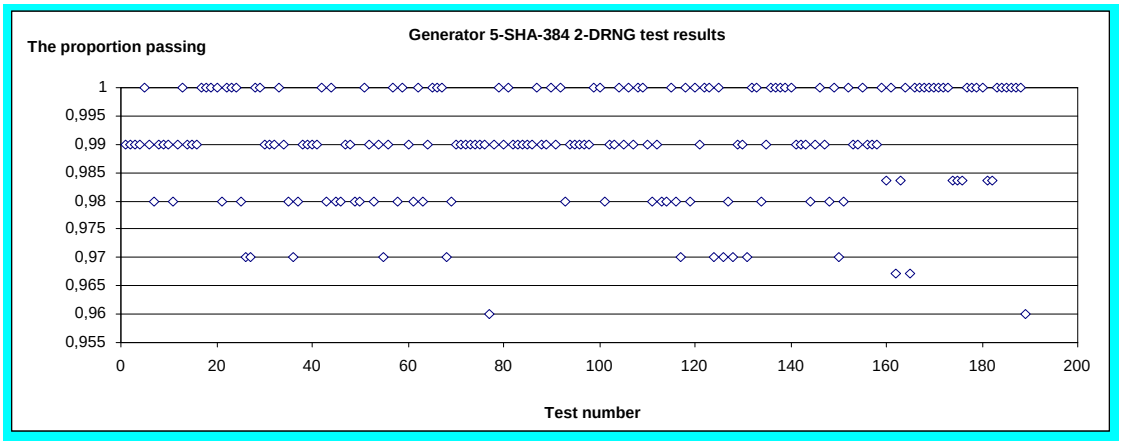

Fig. 3 – The results of experimental research of DRNG 5-SHA-384 2-DRNG $GF(p^n)$

The PRS analysis was carried out according to rating K1 – K4 AIS 20 [4] requirements, which are summarized in the table 5.

Also let us point out that ratings are hierarchically dependent, i.e. each following rating completely includes the previous one and adds its new requirements. Above-given results of research allow making a conclusion that PRS of multimodulo transformations can be applied almost for most of the cryptographic applications. Restrictions can occur only because of complexity of transformation (performance).

Aforementioned requirements are setting up all the level of security from the lowest (an application of DRNG as a counter) to the highest (analyst even knowing certain internal states of generator cannot compromise the whole array).

Table 5 – Comparison of functional ratings К1–К4

Functional rating	Requirements to DRNG	Cryptographic systems, which DRNG of this rating is applied for
К1	К1(i)	Interactive protocols
К2	К1(i) + К2(ii)	Steam ciphers
К3	К1(i) + К2(ii) + К3(iii) + К3(iv)	Key generation, Generation of digital DSS (secret key x or random number k), Password generation
К4	К1(i) + К2(ii) + К3(iii) + К3(iv) + К4(v)	Key generation, Generation of digital DSS (secret key x or random number k), Session key for symmetric cryptographic mechanisms, Password generation

Besides AIS 20 testing method can be applied either in actual time, during the process of research or technological testing.

5 Conclusions

Currently a number of methods and on its basis means of PRS formation have been developed. Their peculiarity includes the fact that they are built as a rule for binary basis $m = 2$. The aim to develop PRS generation methods and means with necessary properties of probability and undefined (certain) alphabet basis is important and necessary. From our point of view the rating of multimodulo transformations should be called the most promising among ratings of such transformations.

Determined PRS generator, which is functioning according to three modulo transformation on the basis (11) or (12) under conditions (2)–(8) fulfillment, provides generation of PRS (symbols) numbers with certain basis of m alphabet, repetition period $p^n - 1$, equally possible appearance of symbols at the repetition period $p^n - 1$ and ensemble of isomorphisms $\varphi\left(p^n - 1\right)$.

On the whole the method and directly PRS generator based on multimodulo transformation can be applied in a number of cryptographic and other applications, in which are set conditions of the high equiprobability and the necessity of undefined basis of PRS symbols appearance.

For through study of PRS generation complexity additional studies are needed. As rough assessments can be used the ones given in [10] concerning the complexity of cryptographic transformations in the finite field $GF\left(p^n\right)$.

References

[1] Methods and means of pseudorandom sequences generation /Y. Gorbenko, T. Grinenko, N. Shapochka, A. Neyvanov, R. Mordvinov// Applied Radio Electronics . - 2011. - Vol. 10. - №2. - P. 141-152. (in Ukrainian).

[2] Potiy A.V. Method of multimodulo transformation of numbers / A.V. Potiy // Information processing and control of managing systems reliability: collection of the science papers. – Kh., 1997. – P.63-68. (in Ukrainian).

[3] Grinenko T.O. Properties of determined random sequences generated on the basis is of multimodulo transformation in Galois fields/ T.O. Grinenko, Y.I. Gorbenko // Collection of the science papers of Kharkiv University of the Science Force. – 2011. – Pub. 1(27). – P.136–139. (in Ukrainian).

[4] Application Notes and Interpretation of the Scheme (AIS) 20. Functionality classes and evaluation methodology for Deterministic random number generators. Certification body of the BSI in context of certification scheme. BSI, 1999.

[5] Information technology. Security techniques. Random bit generation: ISO/IEC 18031. - 2005.

[6] Potiy A.V. Static testing of random and pseudorandom numbers generators with the use of NIST STS static test collection/ A.V.Potiy, S.Y.Orlova, T.A Grinenko // Legal, regulatory and metrological support of information security in Ukraine. – 2001. – Pub. 2. – P.206–214. (in Ukranian).

[7] NIST SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. April 2000. http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf.

[8] Vinogradov I.M . Main theories of numbers/ I.M Vinogradov. – M.: Science, 1981. – 177 p. (in Russian).

[9] Lidl R. The finite fields: In 2 vol. / R. Lidl, G. Niderrayter. – M.: Mir, 1988. – Vol.2. – 822 p.(in Russian).

[10] Gorbenko Y.I. Methods of pseudorandom sequences generator assessment based on multimodulo transformations in the finite fields/ Y.I. Gorbenko // Radio technique: All-Ukranian. Mezhved. Scien-Tech. Col. – 2011. – Pub. 165. – P.249-253. (in Russian).

[11] Shnayer B. Applied Cryptography. Protocols, algorithms, reference texts in SI language/ B. Shnayer. – M.: Triumph, 2002. – 797 p. (in Russian).

[12] Stollings V. Cryptography and nets security / V. Stollings. – M. :Wiliams, 2001. – 669 p. (in Russian).
[13] Information technology. Security techniques. Hash-functions. Part 2. Hash-functions using an n-bit block cipher: ISO/IEC 10118-2.
[14] Information technology. Security techniques. Hash-functions. Part 3. Dedicated hash-functions: ISO/IEC 10118-3.
[15] Information technology. Security techniques. Digital signature schemes giving message recovery. Part 3. Discrete logarithm based mechanisms: ISO/IEC 9796-3:2006.
[16] Information technologies. Cryptographic information security. Digital signature based on elliptic curves. Forming and Checking: DSTU (State Standards of Ukraine) 4145-2002.

Рецензент: Віктор Краснобаєв, д.т.н., проф., Харківський національний університет імені В.Н. Каразіна, Харків, Україна. E-mail: krasnobayev@karazin.ua

Надійшло: січень 2016.

Автори:
Юрій Горбенко, к.т.н., Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: YuGorbenko@iit.kharkov.ua
Тетяна Гріненко, к.т.н., доцент, Харківський національний університет радіоелектроніки, Харків, Україна.
E-mail: t_lame@mail.ru
Олексій Нарєжній, к.т.н., Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: narlexa69@mail.ru
Микола Карпінський, д.т.н., проф., університет Бельсько-Бяла, Польща. E-mail: mkarpinski@ath.bielsko.pl

Генератор псевдовипадкових послідовностей на основі багатомодульних перетворень.

Анотація. Викладаються основні теоретичні положення та практичні результати дослідження методу генерування псевдовипадкових послідовностей з довільним алфавітом на основі багатомодульних перетворень в скінченному полі $GF(p^n)$, наводяться результати аналізу властивостей нерозрізнюваності, непередбачуваності, необоротності, періодів повторення та складності (швидкодії).

Ключові слова: псевдовипадкова послідовність, генератор псевдовипадкової послідовності, багатомодульне перетворення, поле Галуа, нерозрізнюваність, непередбачуваність, необоротність, період повторення.

Рецензент: Виктор Краснобаев, д.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина. E-mail: krasnobayev@karazin.ua

Поступила: январь 2016.

Авторы:
Ю. Горбенко, к.т.н., Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
E-mail: YuGorbenko@iit.kharkov.ua
Т. Гриненко, к.т.н., доцент, Харьковский национальный университет радиоэлектроники, Харьков, Украина.
E-mail: t_lame@mail.ru
А. Нарежний, к.т.н., Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
E-mail: narlexa69@mail.ru
Николай Карпинский д.т.н., проф., университет Бельсько-Бяла, Польша.
E-mail: mkarpinski@ath.bielsko.pl

Генератор псевдослучайных последовательностей на основе многомодульных преобразований.

Аннотация. Излагаются основные теоретические положения и практические результаты исследования метода генерации псевдослучайных последовательностей с произвольным алфавитом на основе многомодульных преобразований в конечном поле $GF(p^n)$, приводятся результаты анализа свойств неотличимости, непредсказуемости, необратимости, периодов повторения и сложности (скорости).

Ключевые слова: псевдослучайная последовательность, генератор псевдослучайной последовательности, многомодульное преобразование, поле Галуа, неотличимость, непредсказуемость, необратимость, период повторения.

УДК 004.94:53.01.07

КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ КАК ИНСТРУМЕНТ ФИЗИЧЕСКИХ ИССЛЕДОВАНИЙ

А.Г. Загородний[1], В.М. Куклин[2]

[1] Институт теоретической физики имени Н.Н. Боголюбова, ул. Метрологическая, 14-б; г. Киев, 03680, Украина

[2] Харьковский национальный университет имени В.Н. Каразина, пл. Свободы, 4, г. Харьков, 61022, Украина
kuklinvm1@gmail.com

Рецензент: Николай Карпинский, доктор технических наук, профессор, университет Бельсько-Бяла, ул. Виллова 2, Польша.
mkarpinski@ath.bielsko.pl

Поступила в феврале 2016

Аннотация. *Анонсированы новые описания физических явлений и новые физические эффекты, которые удалось обнаружить в последнее время, создавая и анализируя компьютерные модели процессов. Это выяснение условий появления океанских волн аномально большой амплитуды. Обнаружены структурно-фазовые переходы в пространственной картине тонкой облачности. Выявлены количественные и качественные характеристики распределения ионов по энергиям при модуляционной неустойчивости интенсивных легмюровских волн в плазме. Выяснена природа преимущественного излучения и поглощения тяжелых квантов осциллятором на его собственной частоте, захваченным в потенциальную яму в условиях отдачи. Обнаружен новый порог индуцированного излучения и представлено пояснение природы появления импульсов когерентного излучения вблизи этого порога.*

Ключевые слова: *компьютерные модели, имитационное моделирование, физические явления, физические эффекты.*

1 Введение

Традиционное представление о моделировании связано с необходимостью иллюстрации и визуализации процессов для создания технологий и отработки процедур реагирования. Однако в практике исследования природы, моделирование становится действенным методом обнаружения новых физических явлений и эффективным способом выявления новых закономерностей. Полезным для создания эффективных имитационных моделей является использование эвристических, основанных на эмпирических данных подходов к описанию процессов, внесение в известные универсальные уравнения и описания полезных изменений. Ибо по мнению А. Пуанкаре «главным образом уравнения нас должны учить тому, что можно и что следует в них изменить». Рационально применять приближенные методы, основанные на малых параметрах и активно применять численное моделирование для выяснения основных механизмов изучаемых процессов. Не ограничиваясь исследованием пусть даже весьма важных, но частных решений для формулирования нужных подсказок практикам.

Ниже анонсированы новые описания физических явлений и новые физические эффекты, которые удалось обнаружить, создавая и анализируя математические модели процессов.

Программы, реализующие математические модели обсуждаемых ниже задач с очень большим числом уравнений созданы с использованием технологии JCUDA. JCUDA обеспечивает взаимодействие с технологией CUDA из Java-программы. Созданные JCUDA-программы обеспечивают выполнение программного кода, написанного на языке программирования ”C” со вставками кода, характерными для технологии CUDA.

2 Математические модели описания модуляционных неустойчивостей океанского волнения

Рассмотрены процессы развития модуляционной неустойчивости волн большой амплитуды. Обсуждается математическая модель, которая **описывает появление волн аномальной амплитуды на поверхности океана** в условиях существования волнения конечной ампли-

туды. Отмечается, что амплитуда аномально больших волн в начале нелинейного режима неустойчивости почти в три раза превосходит их средние значения. Показано, что частоты появления аномальных волн в статистике по ансамблю и по времени в моделях описания океанского волнения практически не отличаются.

На начальной стадии нелинейного режима неустойчивости возможно появление волн и всплесков огибающей с весьма большой амплитудой значительно чаще, чем это следует из статистически обоснованных оценок.

При наличии источника и стока (распределенного вывода, поглощения и диссипации) энергии волны уравнение Лайтхилла (разновидность нелинейного уравнения Шредингера) принимает вид

$$\frac{\partial A}{\partial t} = -\delta A - i\hat{f}A - i\hat{h}A|A|^2 + g, \qquad (1)$$

где δ - декремент поглощения;

g - внешний источник волновой энергии;

$\hat{f}$ и $\hat{h}$ - пространственные операторы.

Неустойчивость понимают как возбуждение спектра

$$\sum_{n\neq 0} u_n(t)\cdot\exp\{i\varphi_{k_n}(t)\}\cdot\exp\{i\omega_0 t - ik_n x\},$$

где $u_n(t)\cdot\exp\{i\varphi_{k_n}(t)\}$ - медленно меняющаяся комплексная амплитуда n-ной моды спектра.

Аномально большие волны и волны-убийцы в океане. Представляет особый интерес случай модуляционной неустойчивости гравитационных поверхностных волн на глубокой воде для судоходства в районах с высоким уровнем океанского волнения. Для частоты волн большой амплитуды справедливо следующее выражение

$$\omega = kW = \sqrt{gk}\cdot\{1 + \frac{A^2k^2}{2} + ...\}, \qquad (2)$$

где A - отклонение поверхности, W - фазовая скорость волны, g – ускорение свободного падения, $f(K) = \sqrt{g(k_0+K)} - \sqrt{gk_0}$, $h(K) = \sqrt{g(k_0+K)}\,\frac{(k_0+K)^2}{2}$.

Для анализа размахов волн (т.е. расстояния между верхней точкой гребня волны и нижней точкой впадины) выделим из них треть наибольших. Критерий, по которому выделяют аномально большие волны обычно $U_{AG} > 2U_{SWH}$, где U_{AG} - аномальная волна, а U_{SWH} - среднее значения трети самых больших размахов.

Методы описания.

1. На линейной по амплитудам возмущений стадии модуляционной неустойчивости возбуждается спектр колебаний, волновые числа которых располагаются симметрично относительно волнового числа k_0 основной моды конечной амплитуды $k_n + k_{-n} = 2k_0$.

2. Основываясь на этой особенности модуляционной неустойчивости, была построена так называемая S-теория, которая учитывала взаимодействие только «спаренных» мод спектра $2k_0 = k_S + k_{-S} = k_n + k_{-n}$. Этот вариант был детально исследован в работах [1-3].

3. Более общее описание позволяет в выражении для нелинейного слагаемого вида $\{A|A|^2\}$ в уравнении (1) удерживать все слагаемые, не ограничиваясь симметричными (в пространстве волновых векторов) по отношению к накачке модами спектра.

Результаты моделирования.

На рисунке 1.а кружками отмечено появление волн аномальной амплитуды U_{AG} в рамках S-теории и в общем случае рассмотрения, без приближений (рис.1.b). Посредине (рис.1.*в*)-характерный вид аномальной волны. Справа (рис.1.*г*) - трехмерная реализация океанского волнения.

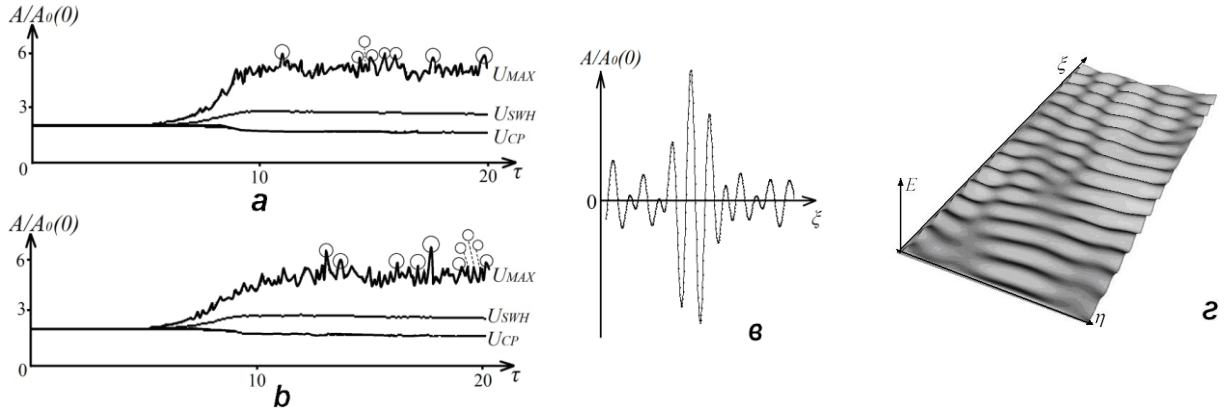

Рис.1 - Средняя амплитуда U_{CP} , средняя амплитуда трети наибольших мод U_{SWH} и самый большой размах волны из ансамбля U_{Max} , как функции времени

Статистика. В работах [2,3] была проведена статистическая обработка множества расчетов на основе **S**- теории и набрана статистика по ансамблям, которая показала хорошее соответствие с данными наблюдения из космоса. Позднее [4] была набрана статистика по текущим изменениям (по времени): Анализ пространственного волнения поверхности проводился через интервалы времени, заведомо превышающие время жизни аномальных волн. Одновременно была проведена верификация результатов S-теории, которая показала качественное соответствие этих двух моделей.

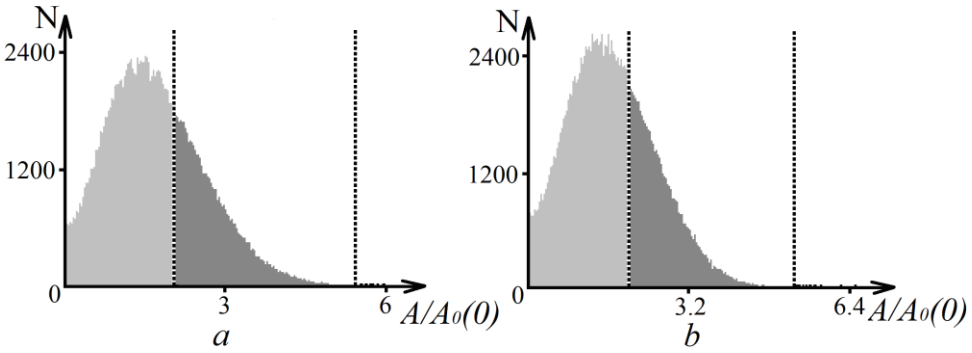

Рис.2 - Распределение амплитуд размахов за все время расчетов в случае описания в рамках S-теории (a) и в общем случае рассмотрения без приближений (b)

На рис. 2 пунктирные линии определяют границу между модами малой амплитуды и третью самых больших мод и величиной, в два раза превышающей среднее значение от трети самых больших мод:

a) - всего размахов 173526, треть наибольших размахов 57842, размахов в 2 раза больше среднего трети наибольших размахов 8;

b) - всего размахов 176386, треть наибольших размахов 58795, размахов в 2 раза больше среднего трети наибольших размахов 10.

Выводы: Аномально большие волны (U_{AG} > 15-20 метров, возникающие в результате интерференции сильного волнения моря *(средняя высота-размах волн 4-6 м, период 10-12 сек, фазовая скорость – более 20 м/сек, групповая – в два раза меньше, длины затухания волнения - тысячи километров)* с непременным учетом нелинейного взаимодействия, представляют собой цуг (группу) обычно из 3-х волн, одна из которых наибольшая, частота появления (статистика по ансамблю и по времени) – одна такая волновая группа на 10-20

тысяч волн. Для таких длинных волн *(200-250 м)* максимально достижимая амплитуда до обрушения - около 30 м. Наиболее вероятно их появление в начале развития модуляционной неустойчивости *(в интервале сотни километров от границы зоны ветрового возбуждения волн, время развития неустойчивости - 10 обратных инкрементов – около 2,5-3 часов*). Кроме таких цугов волн возможно весьма редкое появление уединенных волн (с размахом до 30 м) даже при небольшом волнении - результат обычной интерференции на больших расстояниях уже ослабленных таких длинноволновых ветровых волн.

2 Изменения в структуре тонкой облачности

Рассматривается развитие пространственных структур конвекции и структурно-фазовые переходы в тонких слоях газа и жидкости между состояниями, обладающими разной топологией в отсутствии или при наличии температурной зависимости вязкости. Изучены процессы формирования долгоживущих пространственных структур и структурных трансформаций. Данная модель способна описывать подобные состояния и структурные переходы конвекции тонкого облачного слоя.

Если число Релея (*Ra*) превышает критическое значение Ra_{thr}, то есть $Ra=Ra_{thr}(1+\varepsilon)$, в слое газа или жидкости между плохо проводящими тепло горизонтальными поверхностями (вдоль оси z) возникает трехмерная конвекция, описываемая уравнением Проктора – Сивашинского, которое определяет динамику температурного поля этого процесса в горизонтальной плоскости *(x,y)*:

$$\dot{\Phi} = \varepsilon^2\Phi + \gamma\cdot\nabla(\Phi\nabla\Phi) - (1-\nabla^2)^2\Phi + \frac{1}{3}\nabla\left(\nabla\Phi|\Phi|^2\right) + \varepsilon^2 f\,, \qquad (3)$$

где f - внешний аддитивный шум; ε - определяющая превышение порога развития конвекции, считается достаточно малой и положительно определенной величиной. Слагаемое вида $\gamma\nabla(\Phi\nabla\Phi)$ отвечает за температурную зависимость вязкости. Решение можно искать в форме $\Phi = \varepsilon\sum_j a_j \exp(i\vec{k}_j\vec{r})$ с $|\vec{k}_j| = 1$.

1. В условиях ***пренебрежения зависимостью вязкости от температуры*** динамика функции состояния $I = \sum_i a_i^2$ от времени имеет вид [5-7], изображенный на рис.3.

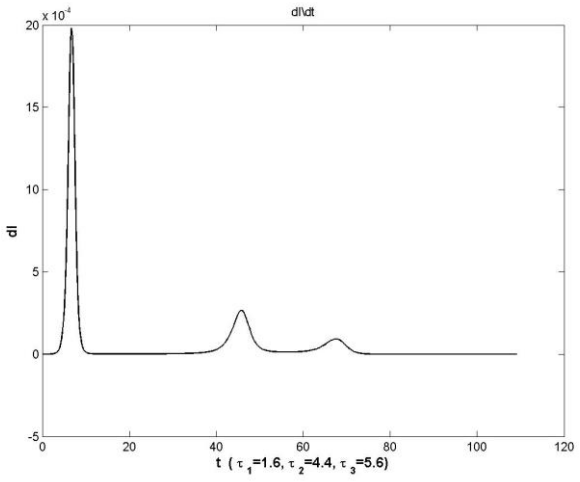

Рис.3 - Поведение производной $\partial I/\partial t$ интегральной квадратичной формы $I = \sum_j a_j^2$ со временем

Характерные времена переходных процессов (рис.3): $\tau_1 = 1.6$, время возникновения «аморфного» состояния; $\tau_2 = 4.4$ - время формирования выраженных валообразных струк-

тур; $\tau_3 \approx 5.6$ - время формирования системы ячеек для одной из реализаций процесса установления конвективного движения.

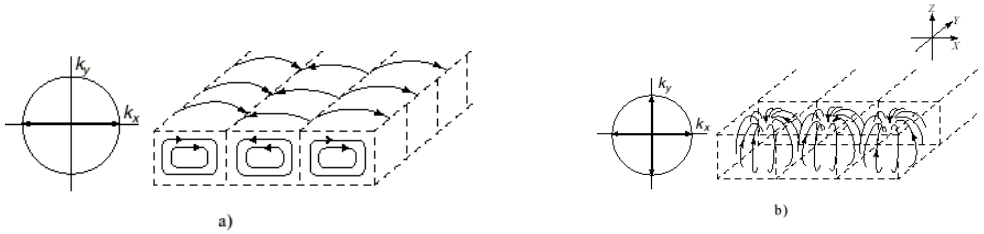

Рис. 4 - Конвективные структуры: валы (a) и квадратные ячейки (b)

Можно убедиться в том, что времена формирования состояний τ_n обратно пропорциональны разности между значениями $I = \sum_i A^2{}_i$ после структурно-фазового перехода $I_n^{(+)} = (\sum_i A^2{}_i)_n^{(+)}$ и до этого перехода $I_n^{(-)} = (\sum_i A^2{}_i)_n^{(-)}$.

То есть, $\tau_n \sim \{(\sum_i A^2{}_i)_n^{(+)} - \sum_i A^2{}_i)_n^{(-)}\}^{-1} = \Delta I_n^{-1}$. Легко видеть, что $\tau_3 / \tau_2 \approx \Delta I_2 / \Delta I_3$.

Таким образом, на основе численного исследования модели Проктора-Сивашинского показано, что функцией состояния, обладающего определенной топологией, является сумма квадратов амплитуд мод

$$I = \sum_i A^2{}_i .$$

Кроме того, более быстрые релаксационные процессы, то есть структурно-фазовые переходы предшествуют более медленным [8,9].

Рис.5 - Фрагмент тонкой облачности – несовершенные конвективные валы
(окружная дорога в р-не города Харьков 12.09.2012)

На интервале между вторым и третьим всплеском производной квадратичной формы (см. рис.3) изучим динамику «спектральной дефектности» структуры

$$D = \sum_{j \neq 1,2} a_j^2 \,/\, \sum_j a_j^2 ,$$

основанной на отношении квадратов амплитуд мод спектра, не отвечающего системе квадратных ячеек к полной сумме квадратов мод, а также так называемую «визуальную дефектность» $d = N_{def} / N$, где N_{def} - число дефектных пространственных ячеек (площадь структуры, занятая нерегулярными ячейками) и N - число ячеек в идеальной регулярной структуре (полная площадь структуры).

На рис.6 представлен фрагмент пространственной структуры конвекции тонкого облачного слоя *(р-н «Белое озеро», г. Змиев, 06.10.2012 г.)*. На рис. 7 представлена пространственная короткоживущая конвективная структура, обладающая дальним порядком, но нарушенным ближним порядком

$$I = \sum_j a_j^2 = 15/14 .$$

Рис.6 - Пространственная структура конвекции тонкого облачного слоя

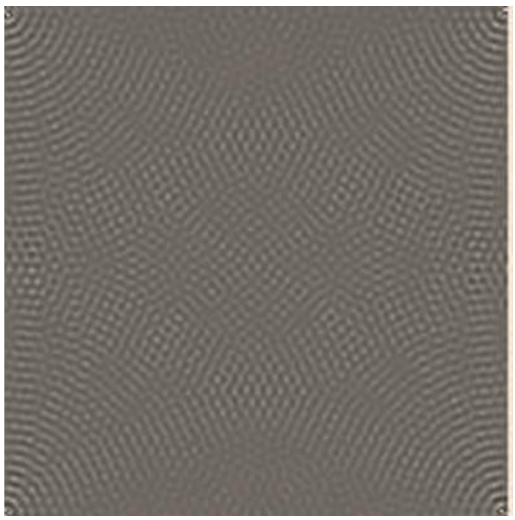

Рис.7 - Пространственная короткоживущая конвективная структура

При приближении к стабильному состоянию пространственная структура избавляется от множества дефектов, причем наблюдается корреляция между относительной долей наблюдаемых визуально (геометрически) дефектов структуры и величиной спектральной дефектности (см. рис.8).

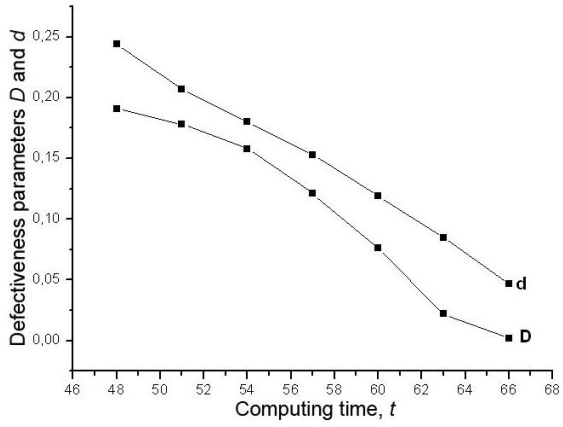

Рис.8 - Сравнительный анализ спектральной (**D**) и визуальной (**d**) дефектности *(число мод - 50)*

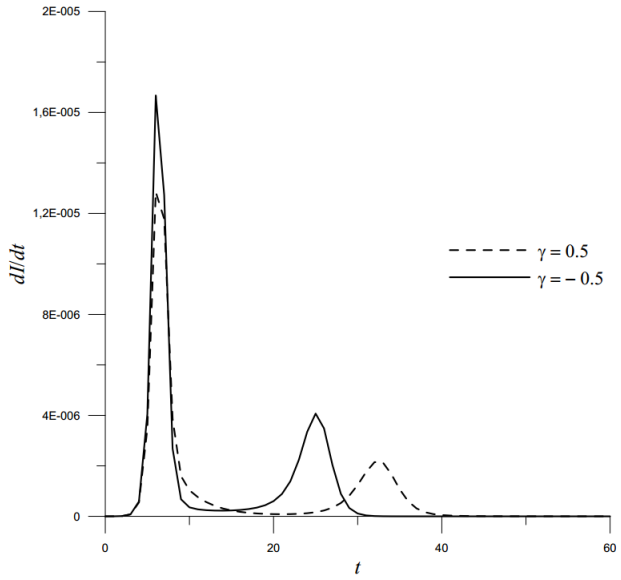

Рис.9 - Изменение производной $\partial I/\partial t$ при развитии процесса, $|\gamma| = 0{,}5$

2. ***Конвекция при учете температурной зависимости вязкости.*** Учет зависимости вязкости от температуры определяется слагаемым вида $\gamma\nabla(\Phi\nabla\Phi)$ в (3), пропорциональным γ. Причем $\gamma > 0$, соответствует случаю газа, а $\gamma < 0$ - жидкости. При $|\gamma| << 1$ влияние этого слагаемого на характер процесса невелико. Процесс конвекции происходит по сценарию, обсуждаемому выше. Но при приближении величины γ к единице, дополнительный механизм обмена энергии между каждой тройкой мод ориентированных по сторонам равностороннего треугольника, вписанной в окружность единичного радиуса $|\vec{k}_j| = 1$, разрушает механизм многоволнового взаимодействия кубической векторной нелинейности. Причем последствия

этого разрушения в случае разного знака γ оказываются практически одинаковыми. Прежде всего, быстрый рост мод спектра на линейной стадии формирует «аморфное» состояние. Однако спустя небольшое время происходит второй структурный переход (см. рис.9) в результате которого формируются устойчивые протяженные и четко выраженные валы, пространственное распределение температурного поля которых представлено на рис.10.

В природе подобные структуры тонкой облачности не редкость (см. рис.11). Таким образом, заметная зависимость вязкости от температуры способна формировать устойчивые конвективные валы. Некоторые отличия для газа и жидкости меняют лишь амплитуду конечной структуры конвективных валов, не изменяя характера структурно-фазовых переходов [7-9].

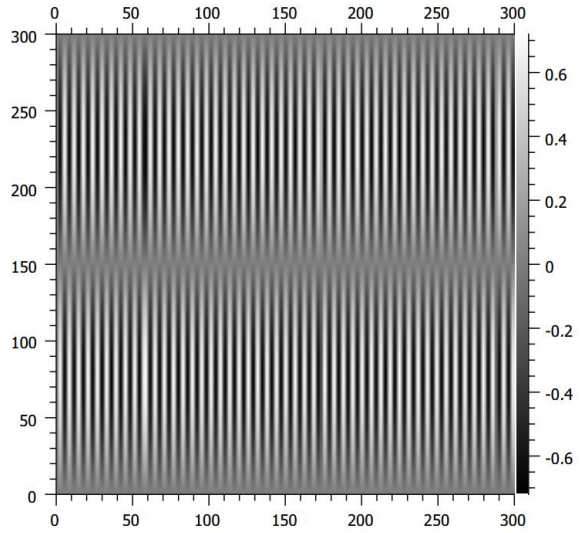

Рис.10 - Температурное поле, отвечающее формированию конвективных валов при |γ| = 0,5

Рис.11 - Формирование конвективных валов, длиной в сотни км *(север Австралии, начало периода дождей)*

3 Нагрев ионов при распаде интенсивного ленгмюровского поля в плазме

Рассмотрено развитие 1D параметрических неустойчивостей интенсивных длинноволновых ленгмюровских волн. Ионы описываются модельными частицами в обоих случаях, когда средняя энергия поля меньше (гибридная модель Захарова) и больше (гибридная модель Силина) тепловой энергии плазмы. Подобные модели позволяют учесть воздействие нерезонансных, захваченных потенциальными ямами колебаний частиц, влияние пересечения их траекторий на развитие неустойчивости и ***детально описать процессы нагрева ионов***. Показано, что энергия ионов при насыщении неустойчивостей оказывается порядка отношения линейного инкремента к частоте в случае, когда начальная энергия поля заметно превышает тепловую энергию плазмы. В этом случае распределение существенно отличается от Максвелловского и характеризуется наличием группы быстрых частиц. В условиях горячей плазмы, ионам передается доля энергии интенсивных ленгмюровских колебаний порядка отношения начальной энергии поля к тепловой энергии плазмы. При этом, так как распределение ионов близко Максвелловскому, можно говорить о температуре ионов.

Корректный аппарат описания параметрической неустойчивости длинноволновых ленгмюровских колебаний фактически был создан в основополагающих работах В.П. Силина и В.Е. Захарова Первые численные 1D эксперименты по параметрическому распаду ленгмюровских колебаний подтвердили теоретические представления (детально ссылки на эти работы представлены, например, в [10,11]).

Рассмотрим модуляционную неустойчивость интенсивных ленгмюровских колебаний в случаях, когда средняя энергия поля меньше (модель Захарова) и больше (модель Силина) тепловой энергии плазмы. Для этого используем гидродинамические уравнения для электронов плазмы и метод крупных частиц для представления ионов плазмы. Такое описание можно считать гибридным. Ограничимся одномерным описанием, так как одномерные модели процессов, как отметил Дж. Даусон, часто сохраняет основные черты процессов, существенно упрощая описание и понимание физических явлений. Кроме того, использованное ниже число частиц *N=20.000*, в трехмерном случае $N^3 \approx 10^{13}$ соответствовало числу частиц реальной плазмы. Это позволяло считать моделирующие частицы фактически отдельными ионами. Гибридное описание позволяет учесть нерезонансное взаимодействие захваченных частиц-ионов с модами низкочастотной составляющей спектра неустойчивости, пересечение траекторий ионов потенциальными полями возникающих каверн плотности плазмы, что приводило к нестабильности последних и к появлению групп быстрых частиц. Эти эффекты остаются вне рассмотрения в традиционном гидродинамическом описании и в кинетическом описании с использованием уравнений для функции распределения частиц.

К преимуществу гибридного описания следует отнести прежде всего ***возможность количественного и качественного описания распределения ионов по энергиям*** [11,12] в режиме насыщения неустойчивости.

Системы уравнений для двух моделей и их сравнение приведены, например, в [10].

Высокотемпературная плазма $n_0 T_e >> |E_0|^2/4\pi$:

$$\frac{\partial E_n}{\partial t} - i\frac{k_0^2 n^2 v_{Te}^2}{2\omega_{pe}} E_n - i\frac{\omega_{pe}}{2n_0}\cdot\sum_m n_{in-m}E_m = 0; \qquad \frac{\partial E_0}{\partial t} - i\frac{\omega_0}{2n_0}\cdot\sum_m n_{i,-m}E_m = 0;$$

$$\frac{d^2 x_s}{dt^2} = \frac{e}{M}\sum_n \bar{E}_n \cdot \exp\{ik_0 n x_s\};\ , \qquad \bar{E}_n = \frac{-ik_0 ne}{4m\omega_{pe}^2}(E_n E_0^* + E_0 E_{-n}^* + \sum_{m\neq 0,n} E_{n-m}E_{-m}^*)\cdot \tag{4}$$

Низкотемпературная плазма $n_0 T_e << |E_0|^2/4\pi$:

$$\frac{\partial E_n}{\partial t} - \frac{4\pi\omega_{pe}\nu_{in}}{k_0 n} J_1(a_n)\cdot\exp(i\phi_0) - i\frac{\omega_0}{2en_0}\sum_m \nu_{in-m}\cdot[E_{-m}{}^*\cdot J_2(a_{n-m})\exp[2i\phi_0] + E_m\cdot J_0(a_{n-m})] = 0;$$

$$\bar{E}_n = (-\frac{4\pi i}{k_0 n})\nu_{in}[1 - J_0^2(a_n) + \frac{2}{3}J_2{}^2(a_n)] + \frac{1}{2}J_1(a_n)[E_n\cdot e^{-i\phi_0} - E_{-n}^*\cdot e^{i\phi_0}] -$$

$$-\frac{ink_0}{16\pi en_0}J_0(a_n)\sum_m E_{n-m}\cdot E_{-m}^* - \frac{ik_0}{16\pi en_0}J_2(a_n)\cdot\sum_m (n-m)[E_{n-m}\cdot E_m\cdot e^{-2i\phi_0} + E_{m-n}^*\cdot E_{-m}^*\cdot e^{2i\phi_0}]; \tag{5}$$

$$\frac{d^2 x_s}{dt^2} = \frac{e}{M}\sum_n \bar{E}_n\cdot\exp\{ik_0 n x_s\};\ \ \frac{\partial E_0}{\partial t} - i\Delta E_0 = -\frac{\omega_0}{2en_0}\sum_m \nu_{i,-m}\cdot[E_m{}^{(-1)}\cdot J_2(a_m)\exp[2i\phi_0] + E_m{}^{(+1)}\cdot J_0(a_m)];$$

где $v_{Te}^2 = T_e/m_e$, $-e, m_e, T_e, n_0$ - заряд, масса, температура и плотность электронов $\omega_0 \approx \omega_{pe} = [4\pi e^2 n_0/m_e]^{1/2}$, $\nu_{im} = en_{im} = en_0\cdot\frac{k_0}{2\pi}\int_{-\pi/k_0}^{\pi/k_0}\exp[-imk_0\cdot x_s(x_0,t)]\cdot dx_{s0}$, E_m - компонент электрического поля коротковолнового спектра: $E = \sum_m E_m\exp\{ik_m x\} = \sum_m E_m\exp\{imk_0 x\}$, $J_s(a_m)$ - функция Бесселя, аргумент которой $a_m = m\cdot a_0 = ek_0|E_0|/m_e\omega_{pe}^2$; $E_0 = |E_0|\exp\{i\phi_0\}$ и $E_n = |E_n|\exp\{i\psi_n\}$ медленно меняющиеся амплитуды длинноволновой и коротковолновой ленгмюровских волн.

Максимальные относительные инкременты неустойчивостей в модели Захарова $\delta/\omega_{pe} = (\frac{1}{2}\frac{|E_0|^2}{4\pi n_0 T_e}\frac{m_e}{M})^{1/2}$ и в модели Силина $\delta/\omega_{pe} = 0,44\cdot(\frac{m_e}{M})^{1/3}$.

Для числа частиц, моделирующих ионы S=$2\cdot10^4$, отношение массы электрона к массе иона выбиралось $m_e / M = 0{,}5\cdot10^{-3}$(легкие ионы) и $m_e / M = 10^{-6}/8$(тяжелые ионы). Крупные частицы равномерно распределены на интервале $-1/2<\xi<1/2$, начальные условия для частиц $d\xi_s / d\tau|_{\tau=0} = v_s|_{\tau=0} = 0$, число мод спектра $-N<n<N$, $N = S/100$. Начальная нормированная амплитуда интенсивных колебаний $a_0(0) = ek_0|E_0(0)|/m_e\omega_{pe}^2 = 0.06$. Начальные амплитуды ВЧ мод задаются выражением $e_n|_{\tau=0} = ek_0|E_n(0)|/m_e\omega_{pe}^2 = (2+g)\cdot10^{-3}$ в модели Силина и $e_n|_{\tau=0} = ek_0E_n(0)/m_e\omega_{pe}^2 = (0.5+g)\cdot10^{-4}$ в модели Захарова, где $g\in[0;1]$ - случайное число, $\psi_n|_{\tau=0}$ также случайным образом распределялись в интервале $0\div2\pi$. Величина $I = \sum_s(\frac{d\xi_s}{d\tau})^2 = \sum_s(\frac{k_0dx_s}{2\pi\delta dt})^2$ и распределение частиц по энергиям являлись целью исследований и основным результатом расчетов.

Результаты моделирования. В процессе развития неустойчивости при прекращении роста энергии ионов в Силинской модели достигнуты значения $I_s \approx 0{,}08$ (легкие ионы), $I_s \approx 0{,}005$ (тяжелые ионы) и в Захаровской $I_s \approx 4{,}58$ (легкие ионы), $I_s \approx 0{,}8$ (тяжелые ионы).

Отношение кинетической энергии ионов к начальной энергии поля [11,12]

$$\frac{E_{kin}}{W_0} \approx 0.27\cdot I\cdot(\frac{M}{m})\cdot\delta^2/\omega_{pe}^2. \qquad (6)$$

и для холодной плазмы (модель Силина) оказывается порядка относительного инкремента для выбранного соотношения масс. В случае высокотемпературной плазмы для легких ионов это соотношение порядка $|E_0(0)|^2/4\pi n_0T_e = W_0/n_0T_e$, а для тяжелых - почти в 6 раз меньше.

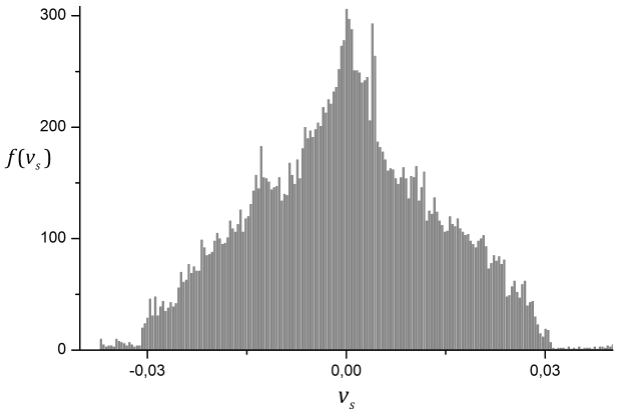

Рис.12 - Распределение ионов по скоростям для случая высокотемпературной плазмы с легкими ионами $v_s = k_0v/2\pi\delta$

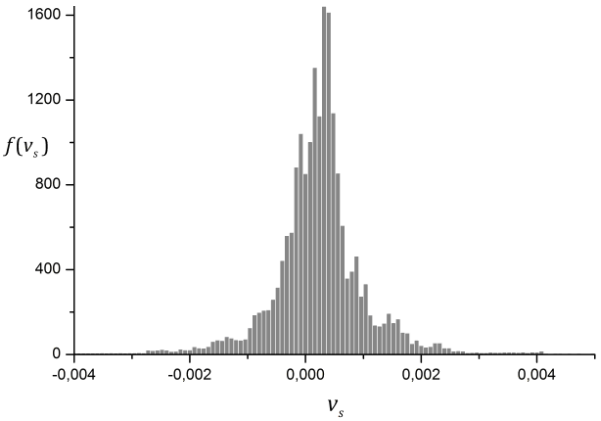

Рис.13 - Распределение ионов по скоростям для случая холодной плазмы с легкими ионами $v_s = k_0v/2\pi\delta$

В случае высокотемпературной плазмы только 10-14% частиц–ионов находятся вне контура функции от энергии частиц, отвечающей Максвелловскому распределению. Для случая холодной плазмы явно выражена группа быстрых частиц. То есть, для высокотемпературной плазмы распределение частиц-ионов по энергиям близко к Максвелловскому, то есть можно говорить о температуре легких ионов $T_i \approx (|E_0(0)|^2/4\pi)^2n_0^2T_e$, однако для более тяжелых ионов их температура оказывается несколько меньше.

Распределение ионов по энергиям в гибридной модели Силина существенно отличается от Максвелловского и характеризуется наличием большой доли быстрых частиц. Различие в распределении ионов по энергиям могут быть пояснены тем, что в модели Захарова было об-

наружено формирование многочисленных каверн плотности, причем в модели Силина каверн оказалось заметно меньше, и они были глубже.

Следует отметить, что масштабы возмущений ионной плотности меньшие дебаевского радиуса ионов $r_{Di} = v_{Ti} / \omega_{pi}$ не дают вклада в формирование низкочастотных электрических полей из-за эффекта экранировки. В терминах $r_{Di} k_0 / 2\pi$ - ионный дебаевский радиус можно оценить как

$$r_{Di} k_0 / 2\pi = R_{Di} \approx < \frac{v_i k_0}{2\pi\gamma_L} > \left(\frac{\delta}{\omega_{pe}} \right) \left(\frac{M}{m_e} \right)^{1/2} = < v_s > \left(\frac{\delta}{\omega_{pe}} \right) \left(\frac{M}{m_e} \right)^{1/2} \quad (7)$$

В режиме развитой неустойчивости эта величина оказывается порядка $R_{Di} \leq 10\text{-}3$, а число мод спектра ионной плотности не превышает величины $1/R_{Di}$, что не противоречит проведенному анализу.

4 Излучение и поглощение тяжелых квантов осциллятором, захваченным в потенциальную яму *(природа эффекта Мессбауэра)*

Рассматривается характер излучения захваченного во внешнюю потенциальную яму осциллятора. Собственная частота осциллятора значительно превосходит частоту его колебаний в потенциальной яме. Изучена ***модель излучения такого осциллятора в случае отличной от нуля энергии отдачи***. В том случае, если энергия отдачи равна энергии кванта низкочастотных колебаний в потенциальной яме, ***наблюдается наибольшая интенсивность линий поглощения и излучения на собственной частоте*** осциллятора. Отмечается некоторое снижение амплитуды линий излучения и поглощения из-за дрожания потенциальной ямы, обусловленных, например, наличием фононного спектра. Оценены времена релаксации низкочастотных движений в потенциальной яме из-за излучения фононов в окружающую среду. Делается вывод, что эти процессы не способны повлиять на обнаруженные особенности процессов излучения и поглощения высокочастотных квантов. Применение данной модели для описания излучения и поглощения гамма квантов в кристаллических структурах возможно даже при наличии фононного спектра, если время релаксации низкочастотных движений в потенциальной яме превышает время жизни ВЧ осциллятора [13,14].

Расположим в начале координат ВЧ осциллятор, скорость которого $v_x = v_{x0} cos\omega_0 t = a\omega_0 cos\omega_0 t$. Медленные колебания такого осциллятора в потенциальной яме происходят со скоростью $v_z = b\Omega\cos(\Omega t)$, причем $\Omega << \omega_0$. Законы сохранения при поглощении кванта внешнего поля $E_\nu = \hbar(\omega_0 + \Omega)$ осциллятором с массой покоя m_0 и зарядом e имеют вид

$$\hbar(\omega_0 + \Omega)/c = m_0 V_Q, \qquad \hbar\Omega = m_0 V_Q^2 / 2. \quad (8)$$

В условиях $\alpha = \hbar\omega_0 / m_0 c^2 < 1$ движение осциллятора вдоль оси OZ описывается уравнением $z = b\sin\Omega t$, где $\Omega = V_Q / b$, откуда следует [15] соотношение $\omega_0 b / c = kb = 2$.

Векторный потенциал в точке, где находится частица - осциллятор,

$$A_x = \sqrt{2} \cdot q_0 \exp\{i(\omega \pm \Omega)t + ikb\sin\Omega t\} \cdot Cos\{\delta\} = \sqrt{2} \cdot q_0 Cos\{\delta\} \sum_m J_m(kb) \exp\{i(\omega \pm \Omega)t + im\Omega t\}$$

$v_x = v_{x0} \cdot cos\omega_0 t$ - скорость осциллятора. Таким образом, в системе существует m энергетических уровней, переходы на каждый из которых могут осуществляться независимо. При этом следует обратить внимание на изменение частоты при отдаче $k \cdot t^{-1} \int t dt \cdot (dV_Q / dt) \approx \pm k V_Q / 2 = \pm\Omega$ в системе покоя частицы-осциллятора.

В классической модели интервал времени передачи импульса и энергии частице- осциллятору достаточно длительный, в квантовом случае этот процесс мгновенный.

Добиваясь выполнения требований временного синхронизма, убедимся в том, что только при значениях частоты внешнего поля $\omega = (m \mp 1)\Omega + \omega_0$ выражение для энергии взаимодействия осциллятора с полем оказывается отличным от нуля и может быть представлено в виде

$$\mathrm{H}' = -e \cdot v_x A_x / c = -\frac{e \cdot v_{x0}}{c} q_0 \sqrt{2} \cdot \sum_m J_m(kb) \cdot \cos\delta . \qquad (9)$$

Вероятность перехода (ρ - плотность состояний) на собственной частоте ВЧ осциллятора ω_0 равна

$$P_{if} = \frac{4\pi^2}{h^2} |\mathrm{H}_{if}|^2 \rho = \frac{8\pi e^2}{hc^3} \omega_0^2 (|x_{ab}|^2 + |y_{ab}|^2) \cdot J_1^2(kb) \cdot Cos^2\delta , \qquad (10)$$

причем, излучение на частоте $\omega = \omega_0 - \Omega$ и поглощение $\omega = \omega_0 + \Omega$ описывается подобным выражением, где $m = 0$ и $J_{\pm 1}(kb)$ следует заменить на $J_0(kb)$.

Нетрудно видеть, что в случае колеблющегося в потенциальной яме осциллятора с частотой Ω и амплитудой колебаний b (так как $J_1^2(2) >> J_0^2(2)$), интенсивность линий поглощения и излучения на собственной частоте осциллятора ω_0 почти на порядок превосходит интенсивность линий излучения на частоте $\omega_0 - \Omega$, и поглощения на частоте $\omega_0 + \Omega$. Заметим также, что природа ВЧ осциллятора, энергия колебаний которого в потенциальной яме равна энергии отдачи, не влияет на обсуждаемый характер излучения и поглощения на его собственной частоте.

Если время релаксации НЧ движения в потенциальной яме значительно превышает время жизни ВЧ возбуждения, то процесс НЧ релаксации не влияет на характер обсуждаемого выше излучения и поглощения ВЧ квантов.

Отметим, что в трехмерном случае характерное время релаксации НЧ движения порядка $\tau_{LF} \approx 3(\rho_0 \lambda_s^3 / m_0)(\omega_0 / \pi^2 \Omega^2)$ пропорциональное весьма большому параметру $\rho_0 \lambda_s^3 / m_0$ (здесь ρ_0 - плотность среды v_s - скорость звука, $\lambda_s = 2\pi v_s / \Omega$ - длина излучаемой звуковой волны). Учет быстрых осцилляций потенциальной ямы приводит к снижению амплитуды векторного потенциала A_x и энергии взаимодействия H' уменьшает вероятность перехода в $\exp\{-W\}$ раз, где $\exp\{-W\} = (1 - b^{-2} \sum_{i=1} b_i^2)$, при выполнении условий на энергию $b^2\Omega^2 << \sum_{i=1} b_i^2 \omega_i^2$ и амплитуды отклонений $b^2 > \sum_{i=1} b_i^2$.

Так например, поглощение ядрами атомов 57Fe и 119Sn гамма-квантов 14,4 кэВ и 23,8 кэВ соответственно, согласно выражению $\omega_0 b / c \approx 2$, приводит к колебаниям атомов в потенциальной яме кристалла с размахами (удвоенной амплитудой) равными $0{,}55 \times 10^{-8}$ см и $0{,}33 \times 10^{-8}$ см. Время релаксации такого колебательного движения атомов железа и олова из-за генерации звука порядка 0,1 и 0,01 сек соответственно, что на много порядков больше времени жизни возбужденного ядра атома. Приведенные оценки ослабления интенсивности линий $\exp\{-W\}$ остаются справедливыми даже для температур Дебая θ_D (например, для железа $\theta_D = 467^0 K$, $\omega_{SMAX} \sim k\theta_D / \hbar \sim 10^{14}$). Процесс излучения и поглощения на собственной частоте ядра ω_0 определяется наличием значительного числа атомов, колеблющихся в потенциальных ямах кристалла, как с возбужденными, так и с не возбужденными ядрами.

5 Новый порог индуцированного излучения

Показано существование нового порога индуцированного излучения. Обнаружено изменение характера процесса генерации излучения в двухуровневой системе при ***превышении начальной инверсии заселенностей величины, равной корню квадратному из полного числа состояний***. При превышении этого порога число квантов начинает расти экспоненци-

ально со временем, возникает генерация в значительной степени когерентного излучения в виде импульсов с коротким передним фронтом и протяженным задним фронтом.

Индуцированным или вынужденным называют излучение, возникающее вследствие воздействия внешнего поля на источник излучения на той же самой частоте. Существовали трудности интерпретация индуцированного излучения как излучения когерентного. Ибо в квантовом описании, где в отличие от классического случая нельзя было ничего сказать о фазах полей, излучаемых отдельными атомами и молекулами, представление о когерентности излучения практически не используется. Тем не менее, Ч. Таунс, опираясь на многочисленные экспериментальные факты полагал, что «…энергия, излучаемая молекулярными системами, имеет то же самое распределение поля и ту же самую частоту, что и индуцирующее излучение, а следовательно и постоянную (возможно нулевую) разность фаз».

Согласно представлениям А. Эйнштейна, описание 1D двухуровневой системы при наличии излучения на частоте перехода $\varepsilon_2 - \varepsilon_1 = \hbar\omega_{12}$ следующее

$$\partial n_2/\partial t = -(u_{21} + w_{21}\cdot N_k)\cdot n_2 + w_{12}\cdot N_k \cdot n_1, \quad \partial n_1/\partial t = -w_{12}\cdot N_k\cdot n_1 + (u_{21} + w_{21}\cdot N_k)\cdot n_2,$$
$$\partial N_k/\partial t = (u_{21} + w_{21}\cdot N_k)\cdot n_2 - (w_{12}\cdot N_k)\cdot n_1 \qquad (11)$$

причем полное число частиц системы на первом и на втором уровне постоянно $n_1 + n_2 = Const$, $u_{21}\cdot n_2$ - скорость изменения количества квантов второго возбужденного уровня за счет спонтанных процессов излучения. Скорость изменения количества квантов (частиц) на этих уровнях за счет индуцированных процессов излучения $w_{21}\cdot N_k \cdot n_2$ и поглощения $w_{12}\cdot N_k\cdot n_1$, N_k - число квантов излучения на частоте перехода. Можно, на качественном уровне предположить, что слагаемые в правых частях уравнений (11) пропорциональные N_k, отвечают индуцированным процессам, также как и число квантов N_k, записанное там же. Рационально представить $N_k = N_k^{(incoh)} + N_k^{(coh)}$, где $N_k^{(incoh)}$ и $N_k^{(coh)}$ - соответственно числа квантов спонтанного и индуцированного излучения. То есть можно рассмотреть две модели описания - традиционную и качественную - модифицированную.

Традиционная система уравнений:

$$\partial \mathrm{M}_1/\partial T = -2N_0 - 2\mathrm{M}_1\cdot \mathrm{N}_1; \qquad \partial \mathrm{N}_1/\partial T = N_0 + \mathrm{M}_1\cdot\mathrm{N}_1 - \theta\cdot\mathrm{N}_1 . \qquad (12)$$

Качественная система уравнений с разделением квантов по их происхождению

$$\partial \mathrm{M}/\partial T = -2N_0 - 2\mathrm{M}\cdot\mathrm{N}_c; \quad \partial \mathrm{N}_{inc}/\partial T = N_0 - \theta\cdot\mathrm{N}_{inc};$$
$$\partial \mathrm{N}_c/\partial T = \mathrm{M}\cdot\mathrm{N}_c - \theta\cdot\mathrm{N}_c . \qquad (13)$$

где $\mathrm{N}_{inc} = N_k^{(incoh)}/\mu_0$, $\mathrm{N}_c = N_k^{(coh)}/\mu_0$, $\mathrm{M} = \mu/\mu_0$, $\mathrm{M} = \mathrm{M}_1 = \mu/\mu_0$ $T = w_{21}\cdot\mu_0\cdot t = \mu_0\cdot\tau$, $\mathrm{N}_1 = N_k/\mu_0$, единственным удобным для анализа свободным параметром является $N_0 = N/2\mu_0^2$.

Для корректности сравнения будем считать, что общее число реальных состояний $N = n_1 + n_2 = 10^{12}$, а пороговая инверсия $\mu_{0th} = \sqrt{N} = 10^6$. Переход к единой шкале времени будем оценивать согласно соотношению $T = \tau\cdot\mu_0$, где T - время в каждом отдельном случае.

Начальные значения определим следующим образом $\mathrm{M}(T=0) = \mathrm{M}_1(T=0) = 1$, $\mathrm{N}_{inc}(T=0) = \mathrm{N}_{inc}/\mu_0 = 3\cdot10^4/\mu_0$; $\mathrm{N}_c(T=0) = \mathrm{N}_c/\mu_0 = 3\cdot10^4/\mu_0$; $\mathrm{N}_1(T=0) = \mathrm{N}_k/\mu_0 = 3\cdot10^4/\mu_0$.

Поглощение энергии поля учитывается значением $\theta = \delta/\mu_0$.

Изменение характера процесса для традиционной системы (12) представлено на рис.14, Данный рисунок отображает динамику развития процесса при изменении параметра $N_0 \subset (30 \div 0.01)$, где: 1 - N_0 = 30; 2 - N_0 = 10; 3 - N_0 = 5; 4 - N_0 = 2; 5 - N_0 = 1; 6 - N_0 = 0,5; 7 - N_0 = 0,2; 8 - N_0 = 0,1; 9 - N_0 = 0,03; 10 - N_0 = 0,01.

Следует обратить внимание на изменение характера роста числа квантов при переходе через порог [16]

$$n_2 - n_1 = \mu_{TH2} = 2(N)^{1/2} = 2(n_2 + n_1)^{1/2}. \qquad (14)$$

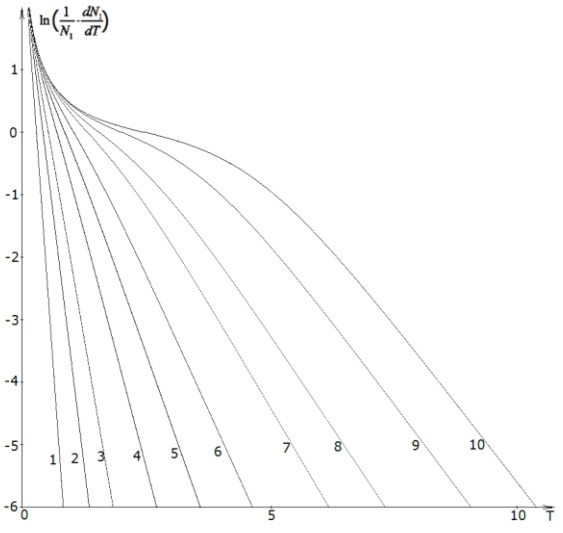

Рис.14 - Поведение величины $\ln\{dN_1 / N_1 dT\}$ от времени для значения параметра $N_0 = (n_1 + n_2)/(n_2 - n_1)^2$

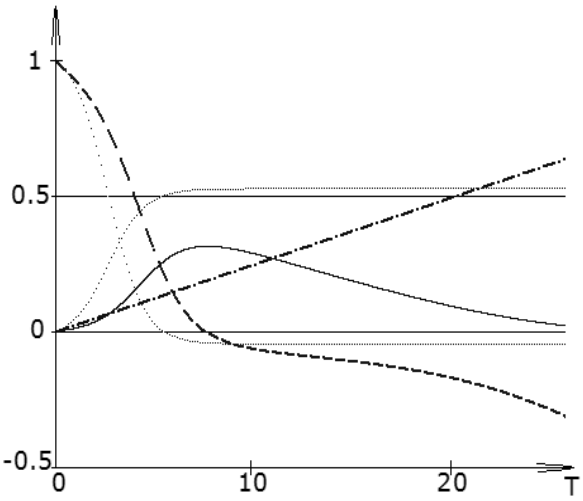

Рис.15 - Поведение величин M_1, N_1, N_c и N_{inc} при отсутствии поглощения

На рис.16б представлены зависимости, отражающие поведение величин M_1 (пунктир), N_1 (точки), N_c (сплошная линия) и N_{inc} (штрихпунктирная линия) при отсутствии поглощения ($\theta = 0$) и $N_0 = N/\mu_0^2 = 0.05$.

При больших значениях начальной инверсии начинает проявлять себя индуцированное излучение, причем все более четко выделяется режим экспоненциального роста числа квантов. В отсутствие поглощения энергии квантов, согласно качественному описанию (13), после уменьшения амплитуды импульса индуцированного излучения число квантов спонтанного излучения продолжает расти. В традиционной модели (12) процессы поглощения ограничивают рост полного числа квантов и уровень излучения выходит на свое стационарное значение. Однако сравнивая динамику процессов можно понять, что после уменьшения амплитуды импульса индуцированного излучения основной вклад в полное число квантов дает спонтанный процесс. То есть, на временах, превышающих длительность импульса индуцированного излучения, доминирует спонтанное некогерентное излучение.

Следует обратить внимание на тот факт, что в случае фиксированного конечного уровня потерь или поглощения энергии квантов, размер импульса индуцированного излучения не меняется даже при значительном увеличении уровня инверсии заселенностей (рис.16).

Так на рис.16а представлен вид когерентного импульса в реальном времени в отсутствии поглощения ($\Theta=0$) для различных значений инверсии (μ_0):

$$\sqrt{2}\cdot 10^6;\ 2\cdot 10^6;\ \sqrt{10}\cdot 10^6;\ \sqrt{20}\cdot 10^6;\ \sqrt{50}\cdot 10^6;\ 10^7;\ \sqrt{2}\cdot 10^7;\ 2\cdot 10^7;\ \sqrt{10}\cdot 10^7.$$

На рис.16б представлен вид когерентного импульса в реальном времени в поглощающей среде ($\delta=4\times10^5$) для тех же значений инверсии (μ_0).

Таким образом, если формирование переднего фронта импульса индуцированного излучения определяется начальным уровнем инверсии, то длительность его заднего фронта обусловлена в большей степени уровнями потерь энергии квантов в системе [17].

Обсуждаемый в данной работе порог индуцированного излучения отвечает случаю, когда случайно распределенное по фазам спонтанное излучение сравнимо с излучением индуцированным. Превышение порога, который чрезвычайно низкий (например, при $N = n_1 + n_2 = 10^{12}$, пороговая инверсия $n_2 - n_1 = \mu_{0th} = \sqrt{N} = 10^6$, относительная инверсия $(n_2 - n_1)/(n_2 + n_1) \approx 10^{-6}$), приводит к появлению импульсов индуцированного излучения, которое в значительной степени является когерентным.

При учете поглощения, даже небольшого, длительность такого импульса излучения слабо меняется при росте инверсии, по крайней мере, достаточно далеко от порога.

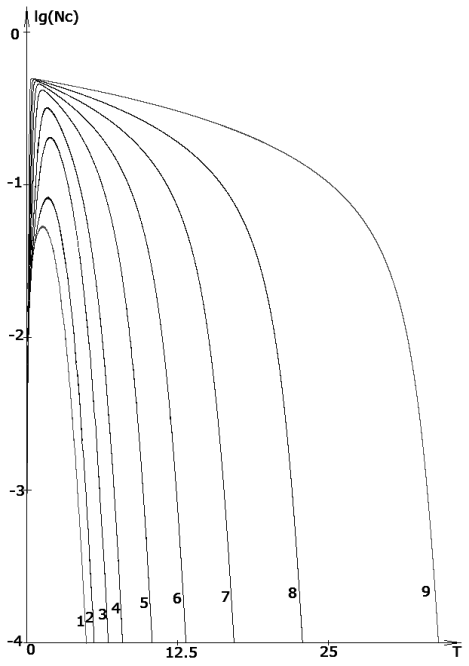

Рис.16.а - Вид когерентного импульса в реальном времени при отсутствии поглощения

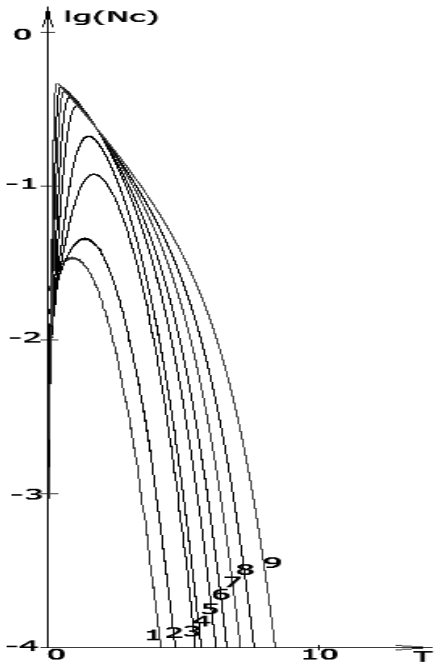

Рис.16.б - Вид когерентного импульса в реальном времени в поглощающей среде

Именно эти обстоятельства дают основание предполагать, что данный механизм может являться одной из причин формирования в космических условиях, в атмосферах звезд (где относительные уровни инверсии крайне невелики), когерентных импульсов примерно одной длительности.

Ссылки

[1] Belkin E.V. Modulyatsionnaya neustoichivost' voln, podderzhivaemykh vneshnim istochnikom v crede s pogloshcheniem/ E.V. Belkin, A.V. Kirichok, V.M. Kuklin // VANT. Ser.: Plazmennaya elektronika i novye metody uskoreniya. – 2010. – №4(68). – S.291-295.

[2] Belkin E.V. The mathematical models of the modulation instability processes of waves in media with cubic nonlinearity- manuscript : PhD-thesis by speciality 01.05.02 «Mathematical modeling and computational methods» / E.V. Belkin . – Kharkiv, 2010.

[3] Belkin E.V. Development of modulation instabilities in media with damping and forcing / E.V. Belkin, A.V. Kirichok, V.M. Kuklin // High-power pulsed electrophysics: international conference XIV Khariton's topical scientific readings. Digest of technical papers. – Саров, 2013. – С. 14-20.

[4] Anomal'nye volny v modulyatsionno neustoichivom volnovom pole / E.V. Belkin, A.V. Kirichok, V.M. Kuklin, A.V. Priimak // East Eur. J. Phys. – 2014. – V.1 – №.2. – P. 4-39.

[5] Kirichok A.V. Allocated Imperfections of Developed Convective Structures / A.V. Kirichok, V.M. Kuklin // Physics and Chemistry of the Earth. Part A. – 1999. – № 6. – P. 533-538.

[6] Strukturnye perekhody v modeli Proktora-Sivashinskogo / E.V. Belkin, I.V. Gushchin, A.V. Kirichok, V.M. Kuklin // VANT. Ser.: Plazmennaya elektronika i novye metody uskoreniya. – 2010. – №4(68). – S. 296-298.

[7] Gushchin I.V. Pattern formation in unstable viscous convective medium / I.V. Gushchin, A.V. Kirichok, B.M. Куклин // VANT. Ser.: Plasma Electronics and New Methods of Acceleration. – 2013. – №4 (86). – Issue 8. – P.248-255; Gushchin I.V.. Structural-phase transitions and state function in unstable convective medium / I.V. Gushchin, A.V. Kirichok, V.M. Kuklin // Problems of Atomic Science and Technology. Ser.: Plasma Electronics and New Methods of Acceleration. – 2015. – N4 . – P. 252-254.

[8] Gushchin I.V. Pattern Transitions in Unstable Viscous Convective Medium / I.V. Gushchin, A.V. Kirichok, V.M. Kuklin. - arxiv:1311.3884v1 [nlin.PS].- 2013. - 15 Nov.

[9] Gushchin I.V. Pattern formation in convective media/ I.V. Gushchin, A.V. Kirichok, V.M. Kuklin // Journal of Kharkiv National University. Physical Series: Nuclei, Particles, Fields. – 2013. – № 1040. – Issue 1 (57). – P. 4 – 27.

[10] Kuklin V.M. Symetrii' 1D opysu parametrychnoi' nestijkosti lengmjurovs'kyh hvyl' // Visnyk Harkivs'kogo nacional'nogo universytetu . Ser. fizychna : Jadra, chastynky, polja. – 2013. – № 1041. – vyp. 2(58). – S. 69-80.

[11] Dynamics of ions during development of parametric instability of langmuir waves / E.V. Belkin , A.V. Kirichok, V.M. Kuklin, A.V. Pryjmak, A.G. Zagorodny // VANT. Ser.: Plasma Electronics and New Methods of Acceleration. – 2013. – №4 (86). – Issue 8. – P.260-266.

[12] Ion heating, burnout of the HF field and ion sound generation with the development of modulation instability of an intensive Langmuir wave in a plasma / A.V. Kirichok, V.M. Kuklin, A.V. Pryjmak, A.G Zagorodny // Physics of Plasmas. – 2015. – № 22. – P. 92-118.

[13] Zagorodnii A.G. O spektrakh zakhvachennogo v potentsial'nuyu yamu ostsillyatora / A.G. Zagorodnii, A.V. Kirichok, V.M. Kuklin // Fizicheskie osnovy priborostroeniya. – 2013. – T.2. – №3. – S. 56-63.
[14] Kirichok A.V. On the emission spectrum of oscillator trapped in a potential well/ A.V. Kirichok ,V.M. Kuklin, A.G. Zagorodny // VANT. Ser.: Plasma Electronics and New Methods of Acceleration. – 2013. – №4 (86). – Issue 8. – P. 256-259.
[15] Kuklin V.M. Ob otnositel'noi roli fononnogo spektra i stolknovitel'noi relaksatsii v protsessakh generatsii i rasseyaniya / O.V Kuklina, V.M. Kuklin // Visnik KhNU im. V. N. Karazina. – 2009. – № 846. – Vyp. 2(50). –S. 20-28.
[16] Zagorodny A. G. To realization conditions of maser radiation / A. G. Zagorodny, V. M. Kuklin // High-power pulsed electrophysics: International conference XIV Khariton's topical scientific readings. Digest of technical papers – Sarov, 2013. – P. 38-43.
[17] On the formation of pulses of coherent radiation in weakly inverted media/ A.V. Kirichok, V.M. Kuklin, A.V. Mischin, A.V. Pryjmak, A.G. Zagorodny // VANT. Ser.: Plasma Electronics and New Methods of Acceleration. – 2013. – №4 (86). – Issue 8. – P. 267-271.

Reviewer: Nikołay Karpinskiy Dr., Full Professor, University of Bielsko-Biala, Poland.
E-mail: mkarpinski@ath.bielsko.pl

Received: February 2016.

Authors:
Vladimir Kuklin, Dr., Full Professor, head of the chair, V.N. Karazin Kharkiv National University, Kharkov, Ukraine.
E-mail: kuklinvm1@gmail.com
Anatoliy Zagorodny, Dr., Full Professor, Academician of National Academy of Science of Ukraine, Director of Bogolyubov Institute for Theoretical Physics. Kiev, Ukraine.
E-mail: azagorodny@bitp.kiev.ua

Computer simulation as a tool for physical research

Abstract. Announced new the description of physical phenomena and new physical effects that were able to detect by computer simulation.

Keywords: Computer models, computer simulation, physical event, physical effects.

Рецензент: Микола Карпінський, д.т.н., проф., університет Бельсько-Бяла, Польща.
E-mail: mkarpinski@ath.bielsko.pl

Надійшло: лютий 2016.

Автори:
Володимир Куклін, д.ф.-м.н., проф., завідувач кафедри, Харківський національний університет імені В.Н. Каразіна, Харків, Україна. E-mail: kuklinvm1@gmail.com
Анатолій Загородний, д.ф.-м.н., проф., академік НАН України, директор Інституту теоретичної фізики імені М.М. Боголюбова. Київ, Україна.
E-mail: azagorodny@bitp.kiev.ua

Комп'ютерне моделювання як інструмент фізичних досліджень

Анотація. Анонсовані нові описи фізичних явищ та нові фізичні ефекти, котрі вдалося виявити шляхом комп'ютерного моделювання процесів.

Ключові слова: комп'ютерні моделі, імітаційне моделювання, фізичні явища, фізичні ефекти.

UDC 004.056.55

BLIND ELECTRONIC SIGNATURE MECHANISMS ON ELLIPTIC CURVES IMPROVEMENT

I. Gorbenko, M. Yesina, V. Ponomar

V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
gorbenkoi@iit.kharkov.ua, rinayes20@gmail.com, Laedaa@gmail.com

Reviewer: Alexandr Potii, Doctor of Sciences (Engineering), Full Professor, Department of Information Systems and Technologies Security, V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
potav@ua.fm

Received February 2016

Abstract. *The work is devoted to consideration the blind electronic signature mechanisms based on algorithms, described in ISO/IEC 14888-3:2006 and national standard DSTU 4145-2002. It is tested protocol security based on these algorithms by the anonymity criterion. It is proved, that the considered protocol is protected by the anonymity criterion, that is impossible to identify the author of the signed document.*

Keywords*: anonymity, electronic signature, blind signature.*

1 Introduction

The requirement of providing electronic anonymity service (non-traceability), for example, in systems of secret electronic voting, electronic money and so on is mandatory in some applications of electronic trust services. Recognized mechanism of providing anonymity service is the use of blind signature mechanism. Blind is a signature, that is imposed on the previously disguised message by trust third face.

The recognition typical blind signature scheme involves, as usual, three faces [7]: signer – A, issuer of the document – B and verifier – C. The issuer creates a document that signer must sign anonymously. That is, the signer shouldn't know the document semantic content and final signature form. For this issuer masking document uses specific cryptographic conversion and sends it to the signer. Then signer signs the disguising document and sends it to the issuer. Issuer removes the disguising conversion from the document, and electronic signature (ES), created by the signer, remains under the document in an open type. Thus verifier gets signed document, that verifies its integrity, authenticity and sets authorship using the signer public key.

Considering the relevance, currently Committee ISO/IEC JTC1/SC27 (one of participant is Ukraine) developed the package of standards concerning electronic trust services. Blind signature is one of such services and concerning it is developing inter-national standard ISO/IEC DIS 18370-2 [2], which will regulate types of blind signature, its using and standardize the specific mechanisms, and blind signature protocols.

Blind ES mechanisms and protocols, based on GOST 34.10-2001, Schnorr and El Gamal algorithms are proposed in [7,8]. But nowadays in Ukraine ES algorithms, that defined in DSTU ISO/IEC 14888-3 and DSTU 4145-2002, are permitted or those, that are recommended for use. Therefore, the task of developing and detailed investigation of these ES algorithms in terms of their use in blind signature mechanisms is important. For this it is necessary to prove the safety of blind signature on elliptic curves mechanism and protocols in general, and the safety of protocols during their implementation using standards on ES, that are recommended for use. Also it is necessary to give the assessments to the cryptographic sustainability directly to ES methods and algorithms on elliptic curves.

The purpose of this article is identifying opportunities and conditions of implementation, justification and development of generalized mechanism of the safe blind ES on elliptic curves, and proof

the safety and determine the conditions of specific blind ES protocols implementation using specific algorithms, defined by DSTU ISO/IEC 14888-3 and DSTU 4145-2002.

2 General description of blind electronic signature mechanism on the elliptic curve

Let the blind ES on the elliptic curve mechanism (scheme) has interaction of three faces [7]: B – subscriber (issuer of the document/message m), A – the signer and verifier C. In this case verifier can be any of them, or a trusted third part. As indicated in the introduction, issuer creates a document m, that the signer has to sign anonymously, that is the signer doesn't have the access to its semantic content – in practice – to the real hash-value. For this purpose the issuer, getting the subscriber consent, disguising the document, and actually – hash-value, using specific cryptographic conversion and sends it to subscriber.

After signing the disguised document, signer sends it to the issuer. The issuer carries out the opposite, relatively disguise, transformation and removes it, leaving ES unharmed. Verifier, after receiving the signed document, verifies its integrity, authenticity and sets authorship using the signer public key.

The certain general parameters of cryptographic transformations on elliptic curves analysis must be previously generated and safe distributed by safe manner to ensure security of mechanism. The list of transformations and requirements to them are defined in the relevant standards [1,4]. Also, asymmetric key pairs for signers A must be generated, and verifier C must have access to signers public keys (certificates). The issuer must have general parameters and disguising and undisguising keys.

Signer A begins the signature statement stage directly [5-7]. He chooses a random or pseudo-random value of disposable ES key k, $1 < k < (n-1)$ and calculates a point on elliptic curve $E = k \cdot G \bmod n = (x_E, y_E)$, where G – basic point with order n. Further signer A sends point E to the issuer B.

Issuer B computes hash-value h of message m and chooses a disguising parameter α, where $1 < \alpha < (n-1)$. Then issuer calculates point $C = \alpha \cdot E \bmod n = (x_C, y_C)$, and also calculates values r and r' according to the following formulas:

$$r = x_C \bmod n \text{ and } r' = x_E \bmod n.$$

Issuer B uses to blind the valid hash-value h the obtained values r and r', for example, for EC DSA, gets h':

$$h' = (\frac{r'}{r} \cdot h) \bmod n.$$

Further issuer B sends the value h' to signer A, that using the obtained values h', r', session key k and his personal (private) key d, signs the disguised hash-value h' and gets s' for the selected standard, for example, for EC DSA:

$$s' = \frac{d \cdot r' + h'}{k} \bmod n,$$

and sends the value s' to the issuer B.

Issuer B authenticates the blinded signature s' using usual ES verification, that is defined in the relevant standard [1,4], using signer A public key Q. If s' is verified by B, that he forms from it message m blind signature in form $< r, s >$, that is undisguises s', turning it into s.

In signature $\{m, < r, s >\}$ verification, verifier calculates point $R = (x_R, y_R)$, using algorithm, that is specified in the relevant standard [1,4], and signer A public key Q.

Signature is considered to be authentic, if the following ratio is performed [7]:

$$r = x_R \bmod n,$$

where x_R – coordinate of point R.

3 Checking the protection mechanism for anonymity criterion

For blind signature schemes, unlike other varieties of ES, the attack of anonymity violation is actual. Assuming, that applied ES is resistant to all known and potential attacks, then blind signature mechanism have to prove the resistance to attack of anonymity violation for the proof its safety.

The essence of the attack on anonymity is concluded that it can be implemented by signer on condition, that he will have all known to him blind signature scheme parameters together with the issuer identifier for each signature statement session. Accumulated thereby database (DB) can be used in the attack, which is to try to determine the author of a certain document m with a signature $<r,s>$, which will be verified by the signer public key Q.

In the proposed protocol anonymous violation attack can be carried out, for example, as follows. Signer A for each row of his DB should calculate the possible blinding parameter α'. Then he, using calculated parameters (h',r',s'), for each DB row calculates point R'. Finally – row, in such way constructed DB, for which the ratio is executed

$$r = x_{R'} \bmod n,$$

indicates the message issuer. In practice point R' always coincides with the verification point R and does not depend on the parameters h',r',s' and, so, does not allow to identify the author of the document m. To prove this assertion in a standard electronic signature verification value R', that is calculated for the relevant standard is used. According to specified condition, the blind signature protocol is considered to protect for the anonymity criterion, because it is impossible to identify the author of the document m [7,8].

4 Safety analysis of blind ES against anonymity attack

As noted above, all algorithms are verified on anonymity and, even, if signer A will keep all parameters h',r',s', then later he can not establish a correspondence of these parameters for the issuer, for which the signature was made. But, if this is true for ECDSA algorithm fully, then for the other algorithms there is feature – α' is expressed by two ratios, that will take the same value only for the subscriber B, that formed final signature on these parameters. And the probability, that there will be yet another issuer, for which two expressions of α' will have the same value, equals 2^{-n}. So it is believed, that the blind signature mechanisms, implemented using, for example, EC GDSA, EC KCDSA and DSTU 4145-2002 provide a blind signature with traceability anonymity [6]. This is considered more detail below.

Point to a possible way of ensuring anonymity using hardware or hardware and software means of cryptographic information protection (CIP). The use of such means for blind signature, like the use of cryptographic modules for users key generation in the Certification Authority (CA). User can generate own key on the station in the center, but because of using certified means CIP, the user can be confident, that only he has the key and CA are not copies of this key.

Cryptographic means (module) for blind signature can be used in the same way. It is considered more detail. Let D be a micromodule, which will be recorded asymmetric key pair for signature implementation and ensure confidentiality on receipt blinded hash-value. In this case, signer A is only cryptographic module D operator, because he has no direct access to the keys. Also cryptographic module D can completely replace A, then the issuer B is granted access to work with the CIP means and signer is unnecessary in such condition.

In this case, the following operations are performed [6]:

1) subscriber B encrypts h' directly on the cryptographic module D public key;
2) obtained $E_D(h')$ is sent to D directly or using operator A;
3) D decrypts h' and creates s';
4) r' and s' sent to the issuer B, and h' is removed from D's memory.

Signer can not make an attack on anonymity, because he will not have one of the parameters, because of h' is processed only in D and A has not opportunity to decrypt $E_D(h')$.

The proposed mechanism, as the analysis revealed, can be used in providing services of blind ES in the clouds. Also it can be used at electronic voting. At the voting voter enters to the cabin, where there is an automated station and carries out a vote according to the paragraphs 1) – 4). The vote anonymity and confirmed the validity and integrity of each voice are ensured by using the blind signature mechanism and CIP means, that are programmed on this [6].

5 Blind electronic signature protocol based on DSTU ISO/IEC 14888-3:2006 (EC DSA)

At first it is built and performed detailed analysis of blind signature protocol for electronic signature algorithm EC DSA [1,5,6].

Signer A generates or chooses a random or pseudo-random value of private key d, $1 < d < (n-1)$ and calculates public key Q:

$$Q = d \cdot G \bmod n.$$

The signer A begins the signature statement stage directly. He chooses a random or pseudo-random value of one-time ES key k, $1 < k < (n-1)$ and calculates a point on elliptic curve E:

$$E = k \cdot G \bmod n = (x_E, y_E),$$

where G – basic point with order n.

After that signer A sends point E to the issuer B.

Issuer B computes hash-value h of message m:

$$h = H(m)$$

and chooses a disguising parameter α, where $1 < \alpha < (n-1)$.

Then issuer calculates point C:

$$C = \alpha \cdot E \bmod n = (x_C, y_C),$$

and also calculates values r and r' according to the following formulas:

$$r = x_C \bmod n \text{ and } r' = x_E \bmod n.$$

Issuer B uses to blind the valid hash-value h the obtained values r and r', gets h':

$$h' = (\frac{r'}{r} \cdot h) \bmod n.$$

Further issuer B sends the value h' to signer A, that using the obtained values h', r', session key k and his personal long-term key d, signs the disguised hash-value h', gets s' according to the ratio:

$$s' = \frac{d \cdot r' + h'}{k} \bmod n$$

and sends the obtained value s' to the issuer B.

Issuer B authenticates the blinded signature s' using usual ES verification, that is defined in the relevant standard, using signer A public key Q. For EC DSA [1]:

$$R' = (\frac{h'}{s'} \cdot G + \frac{r'}{s'} \cdot Q) \bmod n. \quad (1)$$

We're calculating R' according to (1) and point out, that the mathematical expression of the blind signature s' is verified by subscriber B:

$$R' = (\frac{h'}{\underline{d \cdot r' + h'}} \cdot G + \frac{r'}{\underline{d \cdot r' + h'}} \cdot Q) \bmod n = (\frac{h' \cdot k}{d \cdot r' + h'} \cdot G + \frac{r' \cdot k}{d \cdot r' + h'} \cdot dG) \bmod n =$$
$$= k \cdot G \frac{h' + d \cdot r'}{d \cdot r' + h'} \bmod n = E, \quad \textit{that is} \quad x_{R'} = x_E .$$

If s' is verified by B, that he forms from it message m blind signature in form $< r, s >$, previously turning s' into s:

$$s = \frac{s' \cdot (r / r')}{\alpha} \bmod n .$$

In signature $\{m, < r, s >\}$ verification, verifier calculates point $R = (x_R, y_R)$, using algorithm, that is specified in the relevant standard [1], and signer A public key Q:

$$R = (\frac{h}{s} \cdot G + \frac{r}{s} \cdot Q) \bmod n = (x_R, y_R) .$$

We point out, that the mathematical expression of the final signature s is verified by verifier:

$$R = (\frac{h}{s} \cdot G + \frac{r}{s} \cdot Q) \bmod n = \frac{dr + h}{s} \cdot G \bmod n = \frac{k\alpha G(dr + h)}{(dr' + h') \cdot r / r'} \bmod n =$$
$$= \frac{k\alpha G(dr + h)}{(dr' + \frac{r'}{r} \cdot h) \cdot r / r'} \bmod n = \frac{k\alpha G(dr + h)}{dr + h} \bmod n = k\alpha G \bmod n =$$
$$= \alpha E \bmod n = (x_R, y_R) = C = (x_C, y_C).$$

Signature is considered to be authentic, if the following ratio is performed [7]:

$$r = x_R \bmod n ,$$

where x_R – coordinate of point R.

In the proposed protocol anonymous violation attack can be carried out, for example, as follows. Signer A for each row of his DB should calculate the possible blinding parameter α':

$$\alpha' = \frac{s' \cdot (r / r')}{s} \bmod n .$$

Then he, using calculated parameters, for each DB row calculates point R':

$$R' = \alpha' \cdot E \bmod n = (x_{R'}, y_{R'}) .$$

Row, in such way constructed DB, for which the ratio is executed

$$r = x_{R'} \bmod n$$

indicates the message issuer. In practice point R' always coincides with the verification point R and does not depend on the parameters h', r', s' and, so, does not allow to identify the author of the document m.

To prove this assertion in a standard electronic signature verification value R', that is calculated for the relevant standard [1] is used. For EC DSA [1]:

$$R' = \alpha' \cdot E \bmod n = \frac{s' \cdot (r / r')}{s} \cdot E \bmod n = \frac{\frac{dr' + h'}{k} \cdot \frac{r}{r'}}{s} \cdot E \bmod n =$$

$$= \frac{\frac{dr' + \frac{r'}{r} \cdot h}{k} \cdot \frac{r}{r'}}{s} \cdot E \bmod n = \frac{\frac{dr + h}{k}}{s} \cdot E \bmod n = \frac{dr + h}{ks} \cdot kG \bmod n =$$
$$= (\frac{dr}{s} \cdot G + \frac{h}{s} \cdot G) \bmod n = (\frac{r}{s} \cdot Q + \frac{h}{s} \cdot G) \bmod n.$$

According to specified condition, appropriate blind signature protocol is considered to protect for the anonymity criterion, because it is impossible to identify the author of the document m [7,8].

6 Determination the parameters for blind electronic signature protocol based on DSTU ISO/IEC 14888-3:2006 (EC GDSA)

The proof of blind electronic signature protocol safety for EC GDSA executes similarly to section 5. The results of analysis and parameters of blind signature protocol based on ES algorithm EC GDSA are shown in tables 1 and 2 [1].

Table 1 – Formulas for the blind and final signature and its verification

Parameters	EC GDSA
Blinded signature	$s' = (kr' - h')d \bmod n$
Blinded signature verification	$R' = (\frac{h'}{r'} \cdot G + \frac{s'}{r'} \cdot Q) \bmod n,\ r = x_{R'} \bmod n$
Final signature	$s = s' \cdot \frac{r}{r'} \cdot \alpha \bmod n$
Final signature verification	$R = (\frac{h}{r} \cdot G + \frac{s}{r} \cdot Q) \bmod n = (x_R, y_R),\ r = x_R \bmod n$

Table 2 – Parameters of blind electronic signature protocol and verification protocol protection for the anonymity criterion

Parameters	EC GDSA
Public key	$Q = d^{-1} \cdot G \bmod n$
Point E	$E = k \cdot G \bmod n = (x_E, y_E)$
Hash-value	$e = h(m)$
Point C	$C = \alpha \cdot E \bmod n = (x_C, y_C)$
Values r and r'	$r = x_C \bmod n,\ r' = x_E \bmod n$
Blinded hash-value	$h' = \frac{r'}{r} \cdot \frac{h}{\alpha} \bmod n$
Parameter for anonymity verification	$\alpha' = \frac{s}{s' \cdot \frac{r}{r'}} \bmod n,\ \alpha' = \frac{r}{r'} \cdot \frac{h}{h'} \bmod n$
Anonymity verification	$R' = \alpha' \cdot E \bmod n = (x_{R'}, y_{R'}) \Rightarrow$ $R' = (\frac{h}{r} \cdot G + \frac{s}{r} \cdot Q) \bmod n$, $r = x_{R'} \bmod n$

7 Determination the parameters for blind electronic signature protocol based on DSTU ISO/IEC 14888-3:2006 (EC KCDSA)

The proof of blind electronic signature protocol safety for EC KCDSA executes similarly to section 5. The results of analysis and parameters of blind signature protocol based on ES algorithm EC KCDSA are shown in tables 3 and 4 [1].

Table 3 – Formulas for the blind and final signature and its verification

Parameters	EC KCDSA
Blinded signature	$s' = (k - e')d \bmod n$, $e = (r \oplus h) \bmod n$
Blinded signature verification	$R' = (e' \cdot G + s' \cdot Q) \bmod n$, $r = x_{R'} \bmod n$
Final signature	$s = s' \cdot \alpha \bmod n$
Final signature verification	$R = (e \cdot G + s \cdot Q) \bmod n = (x_R, y_R)$

Table 4 – Parameters of blind electronic signature protocol and verification protocol protection for the anonymity criterion

Parameters	EC KCDSA
Public key	$Q = d^{-1} \cdot G \bmod n$
Point E	$E = k \cdot G \bmod n = (x_E, y_E)$
Hash-value	$h = H(m)$
Point C	$C = \alpha \cdot E \bmod n = (x_C, y_C)$
Values r and r'	$r = H(x_C \parallel y_C) \bmod n$, $r' = H(x_E \parallel y_E) \bmod n$
Blinded hash-value	$h' = \frac{r \oplus h}{\alpha} \oplus r' \bmod n$
Parameter for anonymity verification	$\alpha' = \frac{s}{s'} \bmod n$, $\alpha' = \frac{r \oplus h}{r' \oplus h'} \bmod n$
Anonymity verification	$R' = \alpha' \cdot E \bmod n = (x_{R'}, y_{R'}) \Rightarrow$ $R' = (e \cdot G + s \cdot Q) \bmod n$, $r = x_{R'} \bmod n$

8 Determination the parameters for blind electronic signature protocol based on DSTU 4145-2002

The proof of blind electronic signature protocol safety for DSTU 4145-2002 executes similarly to section 5. The results of analysis and parameters of blind signature protocol based on ES algorithm DSTU are shown in tables 5 and 6 [4-6].

Table 5 – Formulas for the blind and final signature according to DSTU 4145-2002 and its verification

Parameters	DSTU
Blinded signature	$s' = (e + dr') \bmod n$
Blinded signature verification	$R' = (s' \cdot G + r' \cdot Q) \bmod n$, $r = x_{R'} \bmod n$
Final signature	$s = s' \cdot \alpha \bmod n$
Final signature verification	$R = (s \cdot G + r \cdot Q) \bmod n = (x_R, y_R)$

Table 6 – Parameters of blind electronic signature protocol and verification protocol protection by the anonymity criterion

Parameters	DSTU
Public key	$Q = -d \cdot G \bmod n$
Point E	$E = k \cdot G \bmod n = (x_E, y_E)$
Hash-value	$h = H(m)$
Point C	$C = \alpha \cdot E \bmod n = (x_C, y_C)$
Values r and r'	$r = h \cdot x_C \bmod n$, $r' = h' \cdot x_E \bmod n$
Blinded hash-value	$h' = \frac{x_C \cdot h}{x_E \cdot \alpha} \bmod n$
Parameter for anonymity verification	$\alpha' = \frac{s}{s'} \bmod n$, $\alpha' = \frac{x_C \cdot h}{x_E \cdot h'} \bmod n = \frac{r}{r'} \bmod n$
Anonymity verification	$R' = \alpha' \cdot E \bmod n = (x_{R'}, y_{R'})$ => $R' = (s \cdot G + r \cdot Q) \bmod n$, $r = x_{R'} \bmod n$

9 Safety analysis of blind signature protocol

It is necessary to perform blind signature verification on the protection from attacks on ES algorithms, because blind signature based on ordinary ES.

Blind signature uses ordinary ES algorithm, only when making final signature change of s' value is performed, using a special coefficient. Because this coefficient is not associated with key parameters, then this transformation not poses a threat to secret parameters at blind signature creation. That is such signature will have the same resistance as the ordinary ES.

9.1 Attack «Full Disclosure» based on signed data

The security of all ES algorithms, that were considered above, based on difficulty of solving discrete logarithm in the group of points an elliptic curve. It is necessary to solve the equations based on public key Q calculation, that are individual for each of the considered algorithms, relatively d, for finding the secret key [3].

As noted above, the same attacks exist for blind signature protocols, such as for standard ES algorithms.

Let's consider the possibility of finding private key d based on attack with known signed (intercepted) messages. Let intercept and sign messages [3,6].

Blind signature for EC DSA has the form:

$$s' = \frac{d \cdot r' + h'}{k} \bmod n,$$

that is, we get the following relatively d:

$$\begin{cases} d = \frac{k_1 s'_1 - h'_1}{r'_1} \bmod n \\ \dots \\ d = \frac{k_i s'_i - h'_i}{r'_i} \bmod n \end{cases}.$$

Blind signature for EC GDSA has the form:

$$s' = (kr' - h')d \bmod n,$$

that is, we get the following relatively d:

$$\begin{cases} d = \dfrac{s'_1}{k_1 r'_1 - h'_1} \bmod n \\ \dots \\ d = \dfrac{s'_i}{k_i r'_i - h'_i} \bmod n \end{cases}.$$

Blind signature for EC KCDSA has the form:

$$s' = (k - e')d \bmod n,\ e' = (r' \oplus h') \bmod n,$$

that is, we get the following relatively d:

$$\begin{cases} d = \dfrac{s'_1}{k_1 - e'_1} \bmod n \\ \dots \\ d = \dfrac{s'_i}{k_i - e'_i} \bmod n \end{cases}.$$

Blind signature for DSTU 4145-2002 has the form:

$$s' = (e + dr') \bmod n,$$

that is, we get the following relatively d:

$$\begin{cases} d = \dfrac{s'_1 - e'_1}{r'_1} \bmod n \\ \dots \\ d = \dfrac{s'_i - e'_i}{r'_i} \bmod n \end{cases}.$$

Thus, in the case of blind signature we also have a system of equations with order i equations with $i+1$ indeterminates. That has not any difference with standard algorithm [3].

Now we consider the situation with the final signature in the blind signature protocol.

The previously formed blind signature, relatively that is carried out opposite, relatively disguising, transformation is used at the final blind signature formation.

The final signature has the following form by using EC DSA:

$$s = \frac{s' \cdot (r / r')}{\alpha} \bmod n,$$

where α – random number from a specified range, $\frac{r}{r'}$ – the ratio of values of x_C and x_E coordinates [3,6].

Write the formula for s completely:

$$s = \frac{(e + dr') \cdot \dfrac{r}{r'}}{\alpha} \bmod n = \frac{e \cdot \dfrac{r}{r'} + dr}{\alpha} \bmod n$$

and obtain the following relatively d:

$$\begin{cases} d = \dfrac{s_1 \alpha - e_1 \dfrac{r_1}{r'_1}}{r_1} \bmod n \\ \dots \\ d = \dfrac{s_i \alpha - e_i \dfrac{r_i}{r'_i}}{r_i} \bmod n \end{cases}.$$

The final signature has the following form by using EC GDSA:

$$s = s' \cdot \frac{r}{r'} \cdot \alpha \bmod n .$$

Write the formula for s completely:

$$s = (kr' - h')d\frac{r}{r'}\alpha \bmod n = (kr\alpha - h'\alpha\frac{r}{r'})d \bmod n$$

and obtain the following relatively d:

$$\begin{cases} d = \dfrac{s_1}{k_1 r_1 \alpha - h'_1 \alpha \dfrac{r_1}{r'_1}} \bmod n \\ \ldots \\ d = \dfrac{s_i}{k_i r_i \alpha - h'_i \alpha \dfrac{r_i}{r'_i}} \bmod n \end{cases}.$$

The final signature has the following form by using EC KCDSA:

$$s = s' \cdot \alpha \bmod n .$$

Write the formula for s completely:

$$s = (k - e')d\alpha \bmod n = (k\alpha - e'\alpha)d \bmod n$$

and obtain relatively d the formula:

$$\begin{cases} d = \dfrac{s_1}{k_1\alpha - e'_1\alpha} \bmod n \\ \ldots \\ d = \dfrac{s_i}{k_i\alpha - e'_i\alpha} \bmod n \end{cases}.$$

The final signature has the following form by using DSTU 4145-2002:

$$s = s' \cdot \alpha \bmod n .$$

Write the formula for s completely:

$$s = (e + dr')\alpha \bmod n = (e\alpha + dr'\alpha)d \bmod n$$

and obtain relatively d the formula:

$$\begin{cases} d = \dfrac{s_1 - e_1\alpha}{r'_1\alpha} \bmod n \\ \ldots \\ d = \dfrac{s_i - e_i\alpha}{r'_i\alpha} \bmod n \end{cases}.$$

Thus, it is necessary to solve the system of i-th order with $i+1$ indeterminates for full disclosure, that is the definition of private key d by i received ES.

In case, if the message M is encrypted, hash functions values $h_1, h_2, ..., h_i$ are indeterminates. As the result, we obtain a system of equations with $2i+1$ indeterminates, so the encryption of signed messages allow to significantly increase the security [3].

9.2 Analysis of protection ES against attacks on implementation

Let the developer can lay a loophole in the software implementation of signature production. The theoretical and experimental results relatively the protection of blind signature in the blind signature protocols based on standard ES algorithms from such attacks for all mentioned above algorithms are given below [3,6].

For EC DSA the violator knows:

$$r'_1 = \pi(x_1, y_1) = x_1 \bmod n;$$
$$r'_2 = \pi(x_1, -y_1) = x_1 \bmod n.$$

Thereby:

$$r'_1 = r'_2 = x_1 \bmod n.$$

We have for s'_1 and s'_2:

$$s'_1 = \frac{dr'_1 + h'_1}{k_1} \bmod n;$$
$$s'_2 = \frac{dr'_2 + h'_2}{k_1} \bmod n.$$

Because $k_1 = k_2 = k$ and $r'_1 = r'_2 = x_1 \bmod n$, then:

$$s'_1 = \frac{dr' + h'_1}{k_1} \bmod n;$$
$$s'_2 = \frac{dr' + h'_2}{k_1} \bmod n.$$

We have the following, solving relatively d and k:

$$d = \frac{s'_1 h'_2 - s'_2 h'_2}{r'(s'_2 - s'_1)} \bmod n;$$
$$k = \frac{dr' + h'_1}{s'_1} \bmod n.$$

For EC GDSA:
The violator knows:

$$k_1 = k_2 = k \in (1, n-1);$$
$$r'_1 = r'_2 = x_1 \bmod n = r'.$$

We have for s'_1 and s'_2:

$$s'_1 = (k_1 r'_1 - h'_1) d \bmod n = (kr' - h'_1) d \bmod n; \quad (2)$$
$$s'_2 = (k_2 r'_2 - h'_2) d \bmod n = (kr' - h'_2) d \bmod n. \quad (3)$$

We have the following, solving (2) and (3) relatively (k, d):

$$k = \frac{h'_1 s'_2 - h'_2 s'_1}{r'(s'_2 - s'_1)} \bmod n;$$
$$d = \frac{s'_1}{kr' - h'_1} \bmod n.$$

For EC KCDSA:

$$k_1 = k_2 = k \in (1, n-1);$$
$$r'_1 = r'_2 = r' = H(c) = r';$$
$$w'_1 = r'_1 + h'_1 = r' + h'_1;$$
$$w'_2 = r'_2 + h'_2 = r' + h'_2.$$

We have for s'_1 and s'_2:

$$s'_1 = (k - w'_1) d \bmod n; \quad (4)$$
$$s'_2 = (k - w'_2) d \bmod n. \quad (5)$$

We have the following, solving (4) and (5) relatively (k, d):

$$k = \frac{w'_1 s'_2 - w'_2 s'_1}{s'_2 - s'_1} \bmod n;$$

$$d = \frac{s'_1}{(k - w'_1)} \bmod n.$$

We propose for DSTU 4145-2002:

$$k_1 = k_2 = k \in (1, n-1);$$
$$R_1 = R_2 = kG = (x_R, y_R) = R;$$
$$fk_1 = fk_2 = x_R = fk;$$
$$y_1 = h'_1 \, fk;$$
$$y_2 = h'_2 \, fk;$$
$$y_1 \Rightarrow r'_1; y_2 \Rightarrow r'_2.$$

We have for s'_1 and s'_2:

$$s'_1 = (k + dr'_1) \bmod n; \quad (6)$$
$$s'_2 = (k + dr'_2) \bmod n. \quad (7)$$

We have the following, solving (6) and (7) relatively (k, d):

$$d = \frac{s'_1 - s'_2}{r'_1 - r'_2} \bmod n;$$
$$k = (s'_1 - dr'_1) \bmod n.$$

There are exist attacks on the ES program implementation for blind signature protocols based on ES algorithms EC DSA, EC GDSA, EC KCDSA, DSTU 4145-2002. If violator able to make the «production signature» program twice uses the same value k for the two messages, then he detects private long-term key d in real time and can impose the false messages and distort the true.

To protect against such attacks must use a reliable CIP means of ES type in the content of available for it conformity certificates, expert opinions and possibility of continuous monitoring of the integrity and authenticity of the production ES program. The best method to protect against such threat is a hardware implementation of ES production and verification procedures [3].

9.3 Analysis of protection ES against related keys attack

We will understand such key pair (k_1, k_2), with the knowledge of one of them with polynomial complexity uniquely or with necessary probability is determined another, as related keys.

Let's consider an attack on related keys on the above discussed ES algorithms [3,6].

At first we define the required input. We'll consider, that long-term key d is valid during some time ΔT. Make ES for messages m_1 and m_2, assuming, that the session data k_1 and k_2 are related, that is, $k_1 + k_2 = n$, where n – base point G order [3].

9.3.1 Analysis of protection algorithm EC DSA against related keys attack

Let's consider the attack with related keys on a blind signature:

$$s' = \frac{d \cdot r' + h'}{k} \bmod n.$$

Then, when making signature for m_1 and m_2 the following steps are performed:

For message m_1	For message m_2
1) $h_1' = (\frac{r_1'}{r_1} \cdot h_1) \bmod n$	1) $h_2' = (\frac{r_2'}{r_2} \cdot h_2) \bmod n$
2) $k_1 \in [1, n-1]$	2) $k_2 = (n - k_1) \in [1, n-1]$
3) $(x_1, y_1) = k_1 \cdot G$	3) $(x_2, y_2) = k_2 \cdot G$

4) $r_1' = \pi(k_1 G) = \pi(x_1, y_1) = x_1 \bmod n$

5) $s_1' = \dfrac{d \cdot r_1' + h_1'}{k_1} \bmod n$

$r_2' = \pi(k_2 G) = \pi((n - k_1)G) \bmod n =$

4) $= \pi(nG - k_1 G) \bmod n = \pi(-k_1 G) \bmod n =$

$= \pi(x_1, -y_1) = x_1 \bmod n = r_1'$

5) $s_2' = \dfrac{d \cdot r_2' + h_2'}{k_2} \bmod n = \dfrac{d \cdot r_1' + h_2'}{k_2} \bmod n$

It is followed, that $r_2' = r_1'$ from the described above, because: $\pi(x_1, y_1) = \pi(x_1, -y_1) = x_1 \bmod n = r_1'$. Thereby, $r_2' = r_1'$ and messages m_1 and m_2 have the same first signature components r_1' and r_2'.

Next, we find the conditions, for that $s_1' = s_2'$, that is find private key d, for that the messages m_1 and m_2 ES are coincide:

$$s_1' = s_2';$$

$$\frac{d \cdot r_1' + h_1'}{k_1} \bmod n = \frac{d \cdot r_1' + h_2'}{k_2} \bmod n;$$

$$\frac{d \cdot r_1' + h_1'}{k_1} \bmod n = \frac{d \cdot r_1' + h_2'}{n - k_1} \bmod n;$$

$$(n - k_1)(dr_1' + h_1') \bmod n = k_1(dr_1' + h_2') \bmod n;$$

$$(dr_1' n - dr_1' k_1 + h_1' n - h_1' k_1) \bmod n = (dr_1' k_1 + h_2' k_1) \bmod n;$$

$$(-dr_1' k_1 - h_1' k_1) \bmod n = (dr_1' k_1 + h_2' k_1) \bmod n;$$

$$(-dr_1' k_1 - dr_1' k_1) \bmod n = (h_2' k_1 + h_1' k_1) \bmod n;$$

$$-2dr_1' k_1 \bmod n = k_1(h_1' + h_2') \bmod n;$$

$$-d = \frac{k_1(h_1' + h_2')}{2r_1' k_1} \bmod n;$$

$$d = -\frac{h_1' + h_2'}{2r_1'} \bmod n.$$

Thereby, if the user-violator generates itself long-term key by the defined rule, then the messages m_1 and m_2 will have the same blind signatures – $r_1' = r_2'$ and $s_1' = s_2'$.

Let's consider the attack with related keys on a final signature similarly:

$$s = \frac{s' \cdot (r / r')}{\alpha} \bmod n.$$

Then, when making signature for m_1 and m_2 the following steps are performed:

For message m_1

1) $s_1 = \dfrac{s_1' \cdot (r_1 / r_1')}{\alpha} \bmod n$

For message m_2

1) $s_2 = \dfrac{s_2' \cdot (r_2 / r_2')}{\alpha} \bmod n = \dfrac{s_2' \cdot (r_1 / r_1')}{\alpha} \bmod n$

$$s_1 = s_2;$$

$$\frac{s_1' \cdot (r_1 / r_1')}{\alpha} \bmod n = \frac{s_2' \cdot (r_2 / r_2')}{\alpha} \bmod n;$$

$$\frac{(d \cdot r_1' + h_1') \dfrac{r_1}{r_1'}}{k_1 \alpha} \bmod n = \frac{(d \cdot r_1' + h_2') \dfrac{r_1}{r_1'}}{(n - k_1)\alpha} \bmod n;$$

$$(n - k_1)\alpha(dr_1' + h_1') \frac{r_1}{r_1'} \bmod n = k_1 \alpha (dr_1' + h_2') \frac{r_1}{r_1'} \bmod n;$$

$$(n\alpha dr_1' + n\alpha h_1' - k_1\alpha dr_1' - k_1\alpha h_1')\frac{r_1}{r_1'} \bmod n = (k_1\alpha dr_1' + k_1\alpha h_2')\frac{r_1}{r_1'} \bmod n;$$

$$(-k_1\alpha dr_1' - k_1\alpha h_1')\frac{r_1}{r_1'} \bmod n = (k_1\alpha dr_1' + k_1\alpha h_2')\frac{r_1}{r_1'} \bmod n;$$

$$-(k_1\alpha dr_1 + k_1\alpha \frac{r_1'}{r_1}\cdot\frac{r_1}{r_1'}h_1) \bmod n = (k_1\alpha dr_1 + k_1\alpha \frac{r_1'}{r_1}\cdot\frac{r_1}{r_1'}h_2) \bmod n;$$

$$-(k_1\alpha dr_1 + k_1\alpha h_1) \bmod n = (k_1\alpha dr_1 + k_1\alpha h_2) \bmod n;$$

$$(-k_1\alpha dr_1 - k_1\alpha dr_1) \bmod n = (k_1\alpha h_1 + k_1\alpha h_2) \bmod n;$$

$$-2k_1\alpha dr_1 \bmod n = k_1\alpha(h_1 + h_2) \bmod n;$$

$$-d = \frac{k_1\alpha(h_1 + h_2)}{2k_1\alpha r_1} \bmod n;$$

$$d = -\frac{h_1 + h_2}{2r_1} \bmod n.$$

Rules of long-term key formation for blind and final ES are coincide. Thereby, if the user-violator generates itself long-term key by the defined rule, then the messages m_1 and m_2 will have the same blind signatures too – $r_1' = r_2'$ and $s_1' = s_2'$.

It proves once again, that set of attacks on the final blind signature is the same as on the standard ES. Blind signature formation algorithm coincides with the usual ES construction algorithm, and the final signature formation in protocol uses a previously formed blind signature, relatively that is carried out opposite, relatively disguising, transformation [3,6].

9.3.2 Analysis of protection algorithm EC GDSA against related keys attack

Let's consider the attack with related keys on a blind signature:

$$s' = (kr' - h')d \bmod n.$$

Then, when making signature for m_1 and m_2 the following steps are performed:

For message m_1	For message m_2
1) $h_1' = \frac{r_1'}{r_1}\cdot\frac{h_1}{\alpha} \bmod n$	1) $h_2' = \frac{r_2'}{r_2}\cdot\frac{h_2}{\alpha} \bmod n$
2) $k_1 \in [1, n-1]$	2) $k_2 = (n - k_1) \in [1, n-1]$
3) $(x_1, y_1) = k_1 \cdot G$	3) $(x_2, y_2) = k_2 \cdot G = (n - k_1)G = nG - k_1G$
4) $r_1' = \pi(k_1G) = \pi(x_1, y_1) = x_1 \bmod n$	$r_2' = \pi(k_2G) = \pi((n-k_1)G) \bmod n =$ 4) $= \pi(nG - k_1G) \bmod n = \pi(-k_1G) \bmod n =$ $= \pi(x_1, -y_1) = x_1 \bmod n = r_1'$
5) $s_1' = (k_1r_1' - h_1')d \bmod n$	5) $s_2' = (k_2r_2' - h_2')d \bmod n =$ $= ((n-k_1)r_2' - h_2')d \bmod n$

It is followed, that $r_2' = r_1'$ from the described above, because: $\pi(x_1, y_1) = \pi(x_1, -y_1) = x_1 \bmod n = r_1'$. Thereby, $r_2' = r_1'$ and messages m_1 and m_2 have the same first signature components r_1' and r_2'.

Next, we find the conditions for that $s_1' = s_2'$, that is find private key d, for that the messages m_1 and m_2 ES are coincide:

$$s_1' = s_2';$$

$$(k_1r_1' - h_1')d \bmod n = ((n-k_1)r_1' - h_2')d \bmod n.$$

Both parts can be reduced by d:

$$(k_1 r_1' - h_1') \bmod n = ((n-k_1) r_1' - h_2') \bmod n;$$
$$(k_1 r_1' + k_1 r_1') \bmod n = (-h_2' + h_1') \bmod n;$$
$$2k_1 r_1' \bmod n = (h_1' - h_2') \bmod n;$$
$$k_1 = \frac{h_1' - h_2'}{2r_1'} \bmod n = \frac{h_1' - h_2'}{2\pi(k_1 G)} \bmod n = \frac{h_1' - h_2'}{2x_1} \bmod n$$

or

$$(2k_1 x_1) \bmod n = (h_1' - h_2') \bmod n. \quad (8)$$

EC GDSA standard is more resistant to manipulation of ES means of creating collision and, in fact, selective forgery [3,6]. Thus, it is necessary to solve the equation (8) to determine s_1' and s_2' respectively.

Let's consider it in another representation:

$$x_1 = \frac{h_1' - h_2'}{2k_1} \bmod n$$

or

$$k_1 = \frac{h_1' - h_2'}{2x_1} \bmod n,$$

or

$$2k_1 \pi(k_1 G) = (h_1' - h_2') \bmod n. \quad (9)$$

The first method of solving this equation is the method of trials and errors [3,6]. Its essence is to form various k_1, calculation x_1 and verification condition (9).

Let's consider the attack with related keys on a final signature similarly:

$$s = s' \cdot \frac{r}{r'} \cdot \alpha \bmod n.$$

Then, when making signature for m_1 and m_2 the following steps are performed:

For message m_1

1) $s_1 = s_1' \cdot \frac{r_1}{r_1'} \cdot \alpha \bmod n$

For message m_2

1) $s_2 = s_2' \cdot \frac{r_2}{r_2'} \cdot \alpha \bmod n = s_2' \cdot \frac{r_1}{r_1'} \cdot \alpha \bmod n$

$$s_1 = s_2;$$
$$(k_1 r_1' - h_1') d \frac{r_1}{r_1'} \alpha \bmod n = (k_2 r_2' - h_2') d \frac{r_2}{r_2'} \alpha \bmod n;$$
$$(k_1 r_1 - \frac{r_1'}{r_1} \cdot \frac{h_1}{\alpha} \cdot \frac{r_1}{r_1'}) d\alpha \bmod n = ((n-k_1) r_1 - \frac{r_1'}{r_1} \cdot \frac{h_2}{\alpha} \cdot \frac{r_1}{r_1'}) d\alpha \bmod n;$$
$$(k_1 r_1 - \frac{h_1}{\alpha}) d\alpha \bmod n = (-k_1 r_1 - \frac{h_2}{\alpha}) d\alpha \bmod n;$$
$$(k_1 r_1 d\alpha - h_1 d) \bmod n = (-k_1 r_1 d\alpha - h_2 d) \bmod n.$$

Both parts can be reduced by d:

$$(k_1 r_1 \alpha - h_1) \bmod n = (-k_1 r_1 \alpha - h_2) \bmod n;$$
$$(k_1 r_1 \alpha + k_1 r_1 \alpha) \bmod n = (h_1 - h_2) \bmod n;$$
$$2k_1 r_1 \alpha \bmod n = (h_1 - h_2) \bmod n;$$
$$k_1 \bmod n = \frac{h_1 - h_2}{2r_1 \alpha} \bmod n = \frac{h_1 - h_2}{2\alpha\pi(k_1 G)} \bmod n = \frac{h_1 - h_2}{2\alpha x_1} \bmod n$$

or

$$2k_1 \alpha x_1 \bmod n = (h_1 - h_2) \bmod n;$$

$$x_1 \bmod n = \frac{h_1 - h_2}{2\alpha k_1} \bmod n$$

or

$$k_1 \bmod n = \frac{h_1 - h_2}{2\alpha x_1} \bmod n,$$

or

$$2k_1\alpha\pi(k_1 G) \bmod n = (h_1 - h_2) \bmod n. \quad (10)$$

It is necessary to solve the equation (10) for determination s_1 and s_2 respectively. This equation for the blind and final ES is the same, only that for formation the final signature random parameter α [3] is attached.

9.3.3 Analysis of protection algorithm EC KCDSA against related keys attack

Let's consider the attack with related keys on a blind signature:

$$s' = (k - e')d \bmod n.$$

Then, when making signature for m_1 and m_2 the following steps are performed:

For message m_1	For message m_2
1) $h_1' = \frac{r_1 \oplus h_1}{\alpha} \oplus r_1' \bmod n$	1) $h_2' = \frac{r_2 \oplus h_2}{\alpha} \oplus r_2' \bmod n$
2) $k_1 \in [1, n-1]$	2) $k_2 = (n - k_1) \in [1, n-1]$
3) $(x_1, y_1) = k_1 \cdot G$	3) $(x_2, y_2) = k_2 \cdot G = (n - k_1)G = (nG - k_1 G) \bmod n = = (O_E - k_1 G) \bmod n = (x_1, -y_1)$
4) $x_1 \to c_1$	4) $x_2 = x_1 \Rightarrow c_2 = c_1$
5) $r_1' = H(c_1)$	5) $r_2' = r_1' = H(c_2) = H(c_1)$
6) $e_1' = r_1' \oplus h_1'$	6) $e_2' = r_2' \oplus h_2' = r_1' \oplus h_2'$
7) $s_1' = (k_1 - e_1')d \bmod n$	7) $s_2' = (k_2 - e_2')d \bmod n$

Thereby, $r_2' = r_1'$ and messages m_1 and m_2 have the same first signature components r_1' and r_2'.

Next, we find the conditions for that $s_1' = s_2'$, that is find private key d, for that the messages m_1 and m_2 ES are coincide: $s_1' = s_2'$; $(k_1 - e_1')d \bmod n = (k_2 - e_2')d \bmod n$.

Both parts can be reduced by d:

$$(k_1 - e_1') \bmod n = (n - k_1 - e_2') \bmod n;$$
$$(k_1 + k_1) \bmod n = (n + e_1' - e_2') \bmod n;$$
$$2k_1 \bmod n = (e_1' - e_2') \bmod n;$$
$$k_1 = \frac{e_1' - e_2'}{2} \bmod n;$$
$$k_1 = \frac{(r_1' \oplus h_1') - (r_1' \oplus h_2')}{2} \bmod n = \frac{h_1' - h_2'}{2} \bmod n.$$

Let's consider the attack with related keys on a final signature similarly:

$$s = s' \cdot \alpha \bmod n.$$

Then, when making signature for m_1 and m_2 the following steps are performed:

For message m_1	For message m_2
1) $s_1 = s_1' \cdot \alpha \bmod n$	1) $s_2 = s_2' \cdot \alpha \bmod n$

$$s_1 = s_2;$$

$$\alpha(k_1 - e_1')d \bmod n = \alpha(k_2 - e_2')d \bmod n;$$
$$\alpha d(k_1 - e_1') \bmod n = \alpha d(n - k_1 - e_2') \bmod n.$$

Both parts can be reduced by d and α:

$$(k_1 - e_1') \bmod n = (n - k_1 - e_2') \bmod n;$$
$$(k_1 + k_1) \bmod n = (e_1' - e_2') \bmod n;$$
$$2k_1 \bmod n = ((r_1' \oplus h_1') - (r_1' \oplus h_2')) \bmod n;$$
$$2k_1 \bmod n = (h_1' - h_2') \bmod n;$$
$$2k_1 \bmod n = ((\frac{r_1 + h_1}{\alpha} \oplus r_1') - (\frac{r_2 + h_2}{\alpha} \oplus r_2')) \bmod n;$$
$$2k_1 \bmod n = (\frac{r_1 + h_1}{\alpha} - \frac{r_1 + h_2}{\alpha}) \bmod n;$$
$$2k_1 \bmod n = \frac{h_1 - h_2}{\alpha} \bmod n;$$
$$k_1 = \frac{h_1 - h_2}{2\alpha} \bmod n.$$

So, ES algorithm EC DSA is vulnerable to attacks on related keys, and ES algorithms EC GDSA and EC KCDSA – protected, from the three algorithms of standard DSTU ISO/IEC 14888-3:2006 [3].

9.3.4 Analysis of algorithm DSTU 4145-2002 protection against related keys attack

Let's consider the attack with related keys on a blind signature:

$$s' = (k + dr') \bmod n.$$

Then, when making signature for m_1 and m_2 the following steps are performed:

For message m_1	For message m_2
1) $k_1 \in [1, n-1]$	1) $k_2 = (n - k_1) \in [1, n-1]$
2) $f_{k_1} = \pi(k_1 G) = \pi(x_{E_1}, y_{E_1}) = x_{R_1}$	2) $f_{k_2} = \pi((n-k_1)G) = \pi(nG - k_1 G) = \pi(x_{E_1}, -y_{E_1}) = x_{R_1}$
3) $(k_1, f_{k_1}) = (k_1, x_{E_1})$	3) $(k_2, f_{k_2}) = (k_2, x_{E_1})$
4) $h_1' = \frac{x_{C_1} \cdot h_1}{x_{E_1} \cdot \alpha} \bmod n$	4) $h_2' = \frac{x_{C_1} \cdot h_2}{x_{E_1} \cdot \alpha} \bmod n$
5) $y_1 = h_1' x_{E_1} = r_1'$	5) $y_2 = h_2' x_{E_1} = r_2'$
7) $s_1' = (k_1 + dr_1') \bmod n$	6) $s_2' = (k_2 + dr_2') \bmod n$

Let's carry out an analysis of results, that are obtained in line 5. In this case $r_1' \neq r_2'$, but r_1' and h_1' are known, so:

$$x_{E_1} = \frac{y_1}{h_1'};$$
$$y_2 = r_2' = h_2' \frac{y_1}{h_1'} = y_1 \frac{h_2'}{h_1'} = r_1' \frac{h_2'}{h_1'}.$$

This means, that if we know r_1' and h_1', we can find x_{E_1}.

So, components r_1', r_2' are interconnected and computationally easy to find at known m_1 and m_2, although $r_1' \neq r_2'$.

Next, let's consider the conditions, for that $s_1' = s_2'$:

$$s_1' = s_2';$$
$$(k_1 + dr_1') \bmod n = (k_2 + dr_2') \bmod n;$$
$$(k_1 + dr_1') \bmod n = (n - k_1 + dr_1' \frac{h_2'}{h_1'}) \bmod n;$$
$$(dr_1' - dr_1' \frac{h_2'}{h_1'}) \bmod n = (n - k_1 - k_1) \bmod n;$$
$$d(r_1' - r_1' \frac{h_2'}{h_1'}) \bmod n = (-2k_1) \bmod n;$$
$$d = -\frac{2k_1}{(r_1' - r_1' \frac{h_2'}{h_1'})} \bmod n = -\frac{2k_1 h_1'}{r_1'(h_1' - h_2')} \bmod n.$$

Let's carry out an analysis of protection level to the case, when values y_1 and y_2 are calculated as sums:

$$y_1 = (h_1' + x_{E_1}); \qquad y_2 = (h_2' + x_{E_2});$$
$$r_1' = y_1 = (h_1' + x_{E_1}); \qquad r_2' = y_2 = (h_2' + x_{E_2});$$
$$r_2' = (h_2' - h_1' + h_1' + x_{E_1}) = (h_2' + x_{E_1}),$$

that is r_2' related with r_1' on x_{E_1}.

We have for the basic field in the case of product:

$$r_2' = h_2' x_{E_1} = h_2' \frac{y_1}{h_1'} = r_1' \frac{h_2'}{h_1'}, \quad \text{and} \quad r_1' = h_1' x_{E_1}.$$

Thus, we have in the case of calculation r_1' and r_2' due the sum h_1' and x_{E_1}, and h_2' and x_{E_1} the following:

$$r_1' = (h_1' + x_{E_1}(k_1)),$$

and

$$r_2' = (h_2' + x_{E_1}(k_1)) = ((h_2' - h_1') + r_1').$$

We have, in the case of calculation r_1' and r_2', due the multiplication the following:

$$r_1' = h_1' x_{E_1}(k_1);$$
$$r_2' = r_1' \frac{h_2'}{h_1'}.$$

Let's consider the attack with related keys on a final signature similarly: $s = s' \cdot \alpha \bmod n$.

Then, when making signature for m_1 and m_2 the following steps are performed:

For message m_1

1) $s_1 = s_1' \cdot \alpha \bmod n$

For message m_2

1) $s_2 = s_2' \cdot \alpha \bmod n$

$$s_1 = s_2;$$
$$\alpha(k_1 + dr_1') \bmod n = \alpha(k_2 + dr_2') \bmod n;$$
$$\alpha(k_1 + dr_1') \bmod n = \alpha((n - k_1) + dr_1' \cdot \frac{h_2'}{h_1'}) \bmod n;$$
$$\alpha(k_1 + dr_1') \bmod n = \alpha(-k_1 + dr_1' (\frac{x_{C_1} h_2}{x_{E_1} \alpha} \Big/ \frac{x_{C_1} h_1}{x_{E_1} \alpha})) \bmod n;$$
$$\alpha(k_1 + dr_1') \bmod n = \alpha(-k_1 + dr_1' \cdot \frac{h_2}{h_1}) \bmod n;$$

$$(\alpha k_1 + \alpha dr_1') \bmod n = (-\alpha k_1 + \alpha dr_1' \cdot \frac{h_2}{h_1}) \bmod n;$$

$$(\alpha dr_1' - \alpha dr_1' \cdot \frac{h_2}{h_1}) \bmod n = (-\alpha k_1 - \alpha k_1) \bmod n;$$

$$d(\alpha r_1' - \alpha r_1' \cdot \frac{h_2}{h_1}) \bmod n = (-2\alpha k_1) \bmod n;$$

$$d = -\frac{2\alpha k_1}{\alpha r_1' - \alpha r_1' \cdot \frac{h_2}{h_1}} \bmod n;$$

$$d = -\frac{2\alpha k_1}{\alpha(r_1' - r_1' \cdot \frac{h_2}{h_1})} \bmod n = -\frac{2k_1}{r_1' - r_1' \cdot \frac{h_2}{h_1}} \bmod n = -\frac{2k_1 h_1}{r_1'(h_1 - h_2)} \bmod n.$$

It can make the conclusion that, as in the case of the multiplication r_1' depends on h_1' and $x_{E_1}(k_1)$, and r_2' depends on r_1', h_1' and h_2', that is depends are identical in its nature.

The above results of researches allow to make the conclusion that, the ES algorithm DSTU 4145-2002 has weak protection against attacks on related keys [3,6].

10 Conclusions

1. Improved blind ES mechanism provides documents authenticity confirmation without revealing their authorship and can be implemented using standard ES EC DSA, EC KCDSA, EC GDSA, and DSTU 4145-2002.
2. In case of given blind ES to the checking protection ES mechanism criteria the anonymity criterion adds. The inability to identify the document author by the signer is proved in its application, if he uses all known parameters, that were used at signature statement.
3. Should find out, can signer calculates the signature in not disguised form, using DB intermediate values, which he creates at signature statement on examination blind ES mechanism for the anonymity criterion.
4. It is shown that blind signature mechanisms, based on standards DSTU ISO/IEC 14888-3: 2006 (EC DSA, EC GDSA and EC KCDSA) and DSTU 4145-2002, ensure their security, that is they are stable for the anonymity criterion. Researches, also, have shown, that the ratios between the disguising parameters to be chosen so, that the signer could not identify the document author with their use.
5. The main advantage of the proposed blind signature mechanism, comparatively existing, is that the signer and validator actions are the same, as described in the relevant standards for ordinary signature and verification in the group of points of elliptic curves. The only difference is that the signer receives a hash-value instead of calculates its by himself. Steps, that distinguish blind signature from ordinary, are performed by the issuer. This technique makes blind signature functionality implementation into existing information and telecommunication systems so, that almost not to require additional efforts. It is only necessary to implement the protocol for the issuer, and signer and validator can use existing tools to develop and verify ES.
6. We can directly refer to existing standards and not to enter into conflict with them (signature verification by one standard, both for the ES and for the blind signature) on the considered approach.
7. The blind signature algorithms are vulnerable to the same attacks, as the standard ES algorithms, because the blind signature algorithms in blind signature mechanism coincide with the ES algorithms of relevant standards.
8. The final signature is formed from the blind, for that is carried out multiplication and division by a random number, which does not affect to the resistance to attacks, so in forming the final signature also using the same standard EP algorithm.

9. It is also found, that all reviewed algorithms provide only tracked anonymity. The CIP modules, that proposed in the section 4 of this article, must be used to ensure complete anonymity. The mechanism alteration can be able an alternative, but it will result in the loss of all its advantages.

References

[1] Information technology – Security techniques – Digital signatures with appendix. Part 3. Discrete logarithm based mechanisms: ISO/IEC 14888-3. - (Edition 2 (2006-11-15)): 2006. – 68 p.
[2] Information technology – Security techniques – Blind digital signatures. Part 2. Discrete logarithm based mechanisms: ISO/IEC DIS 18370-2:2014(E):2015. – 70 p.
[3] Gorbenko I.D. Applied cryptology. Theory. Practice. Application: monograph. / I.D. Gorbenko, U.I. Gorbenko. - Kh.: Fort, 2012. - 870 p.
[4] Information technology – Security techniques – Digital signature based on elliptic curves – Generation and verification: DSTU 4145-2002. – K.: State Standard of Ukraine, 2003. – 35 p. – (National standards of Ukraine).
[5] Yesina M.V. Blind digital signature protocol on elliptic curves based on international standard ISO/IEC 14888-3:2006 (EC DSA) and national standard DSTU 4145-2002 / M. V. Yesina // Theoretical and applied aspect of program systems development (TAAPSD'15): 12th International Conference Proceeding, 23-26 November 2015 – K.: National University of «Kyiv-Mohyla Academy», 2015. – P. 65–69.
[6] Yesina M.V. Mathematical model of a protocol of electronic signature based on elliptic curves / M.V. Yesina // Applied Radioelectronics. – Kh.: Kharkiv National University of Radio Electronics, 2015. – Vol. 14. - № 4. – P. 300–305.
[7] Nikulishchev H.I. Blind digital signature protocol on elliptic curves over vector finite field / H.I. Nikulishchev // Radioelectronics, informatics, management. – 2013. – № 2. – P. 71–76.
[8] Nikulishchev H.I. Anonymity as a criterion of evaluation blind digital signature protocols security / H.I. Nikulishchev, G.L. Kozina // The legal, regulatory and metrological support of information security in Ukraine. – 2012. – № 2. – P. 59–65.

Рецензент: Олександр Потій, доктор техн. наук, проф., Харківський національний університет імені В.Н. Каразіна, м. Харків, Україна. E-mail: potav@ua.fm

Надійшло: лютий 2016.

Автори:
Іван Горбенко, д.т.н., проф., лауреат Державної премії України, Харківський національний університет імені В.Н. Каразіна, м. Харків, Україна. E-mail: gorbenkoi@iit.kharkov.ua
Марина Єсіна, аспірантка, Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: rinayes20@gmail.com
Володимир Пономар, аспірант, Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: Laedaa@gmail.com

Удосконалення механізмів сліпої електронної підписи на еліптичних кривих

Анотація. Робота присвячена розгляду механізмів сліпого електронного підпису на основі алгоритмів, що описані у ISO/IEC 14888-3:2006 та національному стандарті ДСТУ 4145-2002. Проводиться перевірка захищеності протоколу на основі цих алгоритмів за критерієм анонімності. Доводиться, що розглянутий протокол є захищеним за критерієм анонімності, тобто неможливо визначити автора підписаного документу.

Ключові слова: анонімність, електронний підпис, сліпий підпис.

Рецензент: Александр Потий, д.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, г. Харьков, Украина. E-mail: potav@ua.fm

Поступила: февраль 2016.

Авторы:
Иван Горбенко, д.т.н., проф., лауреат Государственной премии Украины, Харьковский национальный университет имени В. Н. Каразина, г. Харьков, Украина. E-mail: gorbenkoi@iit.kharkov.ua
Марина Есина, аспирантка, Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
E-mail: rinayes20@gmail.com
Владимир Пономарь, аспирант, Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
E-mail: Laedaa@gmail.com

Усовершенствование механизмов слепой электронной подписи на эллиптических кривых

Аннотация. Работа посвящена рассмотрению механизмов слепой электронной подписи на основе алгоритмов, которые описаны в ISO/IEC 14888-3:2006 и национальном стандарте ДСТУ 4145-2002. Проводится проверка защищенности протокола на основе этих алгоритмов по критерию анонимности. Доказывается, что рассмотреный протокол является защищенным по критерию анонимности, то есть невозможно определить автора подписанного документа.

Ключевые слова: анонимность, электронная подпись, слепая подпись.

UDC 004.415.3

ESTIMATE OF NOISE-IMMUNITY FOR INDIVISIBLE CODES

V. Kalashnikov[1], O. Borysenko[2]
[1] Department of Systems and Industrial Engineering, Tecnológico de Monterrey, Eugenio Garza Sada av. 2501, 64849 Monterrey, Nuevo León, México
kalash@itesm.mx

[2] Sumy State University, Rimsky-Korsakov str. 2, Sumy 40007, Ukraine;
electron@sumdu.edu.ua

Reviewer: Serghii Rassomakhin, Doctor of Sciences (Engineering), Full Professor, Department of Information Systems and Technologies Security, V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
rassomakhin@karazin.ua

Received March 2016

Abstract. *Considered the problem of finding general criteria to assess the effectiveness of indivisible codes.*

Keywords*: noise immunity, indivisible code, unsymmetrical channel.*

Since recently, the problems connected with the telecommunication, in particular with binary encoding, transmission, and decoding of the digital information, have acquired a special importance. The latter phenomenon is well comprehensible because of the wide use of personal computers in the telecommunication processes.

As the flows of digital information transmitted steadily grow, the probability of errors caused by the channel noise also increases. The classical approach to removing the influence of noise consists in adding redundancy to the encoded messages [1]. The codes with redundancy are usually subdivided into two classes: divisible and indivisible ones [2]. It is well-known that for the divisible codes, the code distance serves as an estimate of their efficiency [3]. Unfortunately, this is not the case for the indivisible codes. Therefore, the problem of finding a general criterion for estimation of the efficiency of the indivisible codes with redundancy arises naturally.

One of the most important tasks for a telecommunication system consists in transmission of the maximal amount of information for a certain (fixed) period of time with the error probability p_e subject to the constraint $p_e \le p < 1$. In order to obtain an estimate of a code's noise-immunity, we determine a quotient of detected erroneous combinations as follows:

$$D = 1 - \frac{M}{N}; \tag{1}$$

here M is the number of allowed (i.e. regular) code words, whereas N is the total number of possible combinations in the code.

The potential noise-immunity of a code is determined by expression (1). It is usually assumed that the information source generates the code words with equal probabilities, as well as the probabilities of them being transformed into both the regular and forbidden code words also coincide. Such an assumption however ignores the real properties of both the telecommunication channel and the information sources. Indeed, the latter most often generates the code words with unequal probabilities. Moreover, the code words are transformed into regular and forbidden ones with different probabilities, too.

In this paper, we take the above features into account by considering separately the probabilities for *i-th* code word: *(a)* to be generated as $P_i \ge 0$; *(b)* to be transformed into a forbidden word as p_i^f; *(c)* the same into a regular code word as p_i^r; and *(d)* to be transmitted correctly as p_i^i.

It is evident that

$$\sum_{i=1}^{M} P_i = 1, \tag{2}$$

and $p_i^f + p_i^r + p_i^i = 1.$ (3)

Now calculate the quotient of detected errors as

$$Z = \sum_{i=1}^{M} P_i p_i^f = \sum_{i=1}^{M} \sum_{j=M+1}^{N} P_i p_{ij}^f ; \tag{4}$$

here p_{ij}^f is the probability of transmission of *i*-th regular code word into *j*-th forbidden word. Similarly, the quotient of undetectable errors is equal to

$$V = \sum_{i=1}^{M} P_i p_i^r = \sum_{i=1}^{M} \sum_{j=1,\, j\neq i}^{M} P_i p_{ij}^r ; \tag{5}$$

here p_{ij}^r is the probability for *i*-th regular code word to be transformed into *j*-th allowed one. Therefore, the summary quotient of errors equals

$$W = Z + V \tag{6}$$

whereas the quotient of correct transmissions is

$$\Pi = \sum_{i=1}^{M} P_i p_i^i . \tag{7}$$

Now making use of (1) - (7) it is readily verified that

$$Z + V + \Pi = 1, \tag{8}$$

which means that Z, V, Π are equal to probabilities of transmission of the regular words into forbidden, other regular ones, and itself, respectively.

In particular case when $p_{ij}^f = p_{ij}^r = p_i^i = 1/N, \forall i, j, ,$ it is easy to verify that the values Z, V, Π do not depend upon the characteristics of the information source. Conversely, if $P_i = 1/M$ for each *i*, the values Z, V, II depend only upon the probabilities p_i^f , p_i^r , p_i^i .

One of the most important features of a code is the probability of transmission of a regular code word to some other regular word, i.e. the probability of undetectable error

$$p_e = V = 1 - Z - \Pi, \tag{9}$$

which increases when Z decreases. Therefore, in order to diminish p_e one needs either to maximize Z or to minimize V. The problem can be solved by a reasonable encoding of the symbols generated by the information source. An optimal encoding algorithm is proposed.

Example 1. We need transmitting three symbols A, B, C generated with probabilities $P_1 = 0{,}6$; $P_2 = 0{,}3$; $P_3 = 0{,}1$, respectively. They all are encoded by binary words. The channel is subject to some amount of noise which causes the following errors: 0 can be transformed to 1 with probability $q_{01} = 0{,}1$ whereas 1 can be transmitted to 1 with than of $q_{10} = 0{,}2$. The problem of developing a good coding system arises.

First choose the binary words 000, 001 and 011 to encode the symbols A, B, and C, resp. Therefore, the combinations 010, 100, 101, 110, and 111 are forbidden ones. At last, $M = 3$, $N = 8$.

Probabilities of correct transmissions of the regular words are readily calculated and equal resp.: $p_1^1 = 0{,}729$ for A, $p_2^2 = 0{,}648$ for B and $p_3^3 = 0{,}576$ for C.

From (7), we obtain the probability of the correct transmission as $\Pi = 0{,}6894$. In addition, (4) implies $Z = 0{,}1684$, whereas from (5) we have $V = 0{,}1422$.

In order to minimize V, we have to exchange the encoding rule as follows: A is encoded by 000, B – by 011 and C – by 001. Then it is obtained straightforward that $V_* = V_{min} = 0{,}1314$; $Z^* = 0{,}675$; $\Pi_* = 0{,}1936$.

Otherwise, in order to maximize Z, we need encode A by 011, B by 000 and C by 001. In this case, $Z^{**} = Z_{max} = 0{,}2125$; $V_{**} = 0{,}1584$; $\Pi = 0{,}6291$.

As it is illustrated by the above example, for an unsymmetrical channel (i.e. if $q_{01} \neq q_{10}$), the minimal p_e corresponds to the V_{min}, but not to the Z_{max}.

References

[1] Pless V. Introduction to the Theory of Error-Correcting Codes / V. Pless. - John Wiley and Sons. - 1989.
[2] Gallager R.G. Information Theory and Reliable Communication / R.G. Gallager. - MIT. - John Wiley and Sons. – 1968.
[3] Fano R.M. Transmission of Information. A Statistical Theory of Communication / R.M. Fano.– MIT Press. - John Wiley and Sons. - 1961.

Рецензент: Сергій Рассомахін, д.т.н., професор., Харківський національний університет імені В.Н. Каразіна, Харків, Україна. E-mail: rassomakhin@karazin.ua

Надійшло: березень 2016.

Автори:
В'ячеслав Калашников, д.ф.-м.н., проф., департамент систем і промислового виробництва Технологічного університету Монтеррея, Монтеррей, Мексика. E-mail: kalash@itesm.mx
Олексій Борисенко, д.т.н., проф., Сумський державний університет, Суми, Украина. E-mail: electron@sumdu.edu.ua

Оцінка завадостійкості неподільних кодів

Анотація. Розглядається проблема знаходження загальних критеріїв для оцінки ефективності неподільних кодів.

Ключові слова: завадостійкість, неподільний код, несиметричний канал.

Рецензент: Сергей Рассомахин, д.т.н., профессор., Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина. E-mail: rassomakhin@karazin.ua

Поступила: март 2016.

Авторы:
Вячеслав Калашников, д.ф.-м.н., проф., департамент систем и промышленного производства Технологического университета Монтеррея, Монтерей, Мексика. E-mail: kalash@itesm.mx
Алексей Борисенко, д.т.н., проф., Сумской государственный университет, Сумы, Украина. E-mail: electron@sumdu.edu.ua

Оценка помехоустойчивости неделимых кодов

Аннотация. Рассматривается проблема нахождения общих критериев для оценки эффективности неделимых кодов.

Ключевые слова: помехоустойчивость, неделимый код, несимметричный канал.

UDC 004.451.5:621.3.037.372.7

THE METHOD OF ERROR DETECTION AND CORRECTION IN THE SYSTEM OF RESIDUAL CLASSES

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

[1] V. N. Karazin Kharkiv National University, Svobody sq.,4, Kharkov, 61022, Ukraine
krasnobaev_va@rambler.ru

[2] Poltava National Technical Yuri Kondratyuk University, Pershotravnevyi avenue 24, Poltava, 36011, Ukraine
al9_yanko@ukr.net

[3] Kharkov National Technical University of Agriculture named after Peter Vasylenko, Artyoma st., 44, Kharkiv, 61002, Ukraine
s_koshman@ukr.net

Reviewer: Alexandr Kuznetsov Dr., Full Professor, V.N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
kuznetsov@karazin.ua

Received on April 2016

Abstract. *The method of correcting of single errors in the system of residual classes (SRC) were presented in this paper. The results of the analysis of corrective capability of arithmetic code shown the high efficiency of using of nonpositional code structures in the SRC. The examples of correction of single data error witch provided by code of the SRC are given in the article.*

Keywords: *the system of residual classes, validity of data control, information redundancy, correction of data single errors.*

1 Problem formulation

In general, for the control, diagnosis and error correction data is needed to possess a specific structure of the code correction capacity. To do this, you need to enter some information redundancy, that is, to apply the method of information redundancy. This applies to nopositional code structure (NCS) of the residual classes (SRC) [1-3]. In the SRC value of redundancy $R = M_0 / M$ ($M_0 = \prod_{i=1}^{n+k} m_i$; $M = \prod_{i=1}^{n} m_i$.) uniquely determines the corrective possibilities of error-correcting code nonpositional. Correcting codes in SRC can have any value of the minimum code distance (MCD) $d_{\min}^{(SRC)}$. This depends on the values of redundancy R. In SRC established between redundancy correcting code R, the value $d_{\min}^{(SRC)}$ of MCD and the number k of check bases. Correcting code has a value $d_{\min}^{(SRC)}$ of MCD, if the degree R of redundancy is not less than the product of any $d_{\min}^{(SRC)} - 1$ bases SRC. On the one hand we have that $R \geq \prod_{i=1}^{d_{\min}^{(SRC)}-1} m_{q_i}$, on the other hand, 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, legitimately argue that $d_{\min}^{(SRC)} - 1 = k$, or

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

There are two approaches to the problem of ensuring NCS in SRC necessary corrective properties.

The first approach. Knowing the requirements for correcting the NCS properties, for example, the number of errors witch detected $t_{\text{det.}}$ or corrected $t_{cor.}$, to introduce, by controlling the amount k or magnitude $\{m_{n+k}\}$ of bases necessary redundancy information R. Information redundancy R

determines the minimum code distance $d_{\min}^{(SRC)}$ NCS in SRC.

Then, in accordance with the theory of error-correcting coding (TECC) for the orderly $(m_i < m_{i+1})$ SRC have that

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

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

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

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

The second approach. For a given type of NCS $A_{SRC} = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| ... \| a_{n+k})$ (for a given value of *k*) correction capabilities (defined value $d_{\min}^{(SRC)}$) code in SRC determined in accordance with the expressions (3) and (5).

Note that if ordered SRC expanded by adding *k* control bases to *n* information module, that MCD $d_{\min}^{(SRC)}$ of the error-correcting code increased on the value of *k* (see the expression (1)). Zoom values $d_{\min}^{(SRC)}$ can also be due to the reduction of the number *n* of information bases, that is due to the transition to computing with less precision. It is clear that between the correction capability R of error correcting codes and precision calculations W in SRC exists an inverse relationship. The same computer can perform data processing with high precision W, but a small correction capability R. Or with less precision W, but with a higher possibility of the correction control R, diagnosis and correction of data errors, as well as higher speed data (the run-time of basic operations in CSR inversely to the number *n* of information bases) [1,2].

Draw analysis of the possible correction of single data errors in SRC with a minimum of information redundancy by introducing only one $(k = 1)$ the control base. In this case, in accordance with a TECC in SRC [4-7], MCD equal magnitude $d_{\min}^{(SRC)} = k + 1$. When $k = 1$ we have MCD $d_{\min}^{(SRC)} = 2$ that, in accordance with the general theory of error-correcting coding will guarantee only detect any single error (error in one of the residues a_i $(i = \overline{1, n+1})$) in the NCS. In general, the process of correcting data errors in SRC as a positional numbering system (PNS), is composed of three stages. The first stage – control data (the definition of the rightness or wrongness of the original number A_{SRC}). The second stage. Diagnosis wrong number $\tilde{A}_{SRC}$ (defining a distorted residual $\tilde{a}_i$ of the base m_i of SRC of number $\tilde{A}_{SRC}$). And finally, the third stage, the correction of an incorrect residual $\tilde{a}_i$ of the true number a_i, that is correct a wrong number $\tilde{A}_{SRC}$ (getting the right number $A_{SRC} = \tilde{A}_{cor.}$). The degree of information redundancy R (correcting capacity of code) is estimated by a size of MCD $d_{\min}^{(PNS)}$. In the SRC, as noted above, the value of MCD determined by the ratio $d_{\min}^{(SRC)} = k + 1$, where k – the base control quantity in ordered SRC.

2 Scientific findings

In this article we consider the NCS $A_{SRC} = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| ... \| a_{n+k})$ in SRC with minimal $(k = 1)$ additional information redundancy. In this case, it is determined that $d_{\min}^{(SRC)} = 2$.

In accordance with the general TECC, in the PNS with minimum code distance $d_{\min}^{(PNS)} = 2$ in the code structure uniquely (reliably) is determined by a one-time mistake. In the PNS a single data error meant the distortion of one bit of information, the type of $0 \to 1$ or $1 \to 0$. To correct this single

error in the PNS is necessary to satisfy the condition that $d_{\min}^{(PNS)} = 3$.

In SRC, unlike PNS, a single error is the distortion of one residual a_i with base m_i. Since the residual a_i of the number $A_{SRC} = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| a_{n+1})$ with base m_i contains $z = \{[\log_2(m_i - 1)] + 1\}$ – binary digits, it is formally possible to assume that in SRC (at $d_{\min}^{(SRC)} = 2$ $(k = 1)$) within one residual a_i, can be found a stack of errors of no more than z bits. However, in the literature [4,5,8] shows that in some cases when $d_{\min}^{(SRC)} = 2$ the value in the SRC is possible to correct single errors.

Taking into account the specificity properties and features representation NCS in SRC opportunity to correct errors when $d_{\min}^{(SRC)} = 2$, you can try to explain as follows:

– a single error in the PNS and in the SRC refers to different concepts. This was shown above. In this regard, the MCD $d_{\min}^{(PNC)}$ for PNS and $d_{\min}^{(SRC)}$ for SRC has different meaning and quantitative assessment;

– existing (implicitly) in NCS natural (primary) information redundancy, which is available in the residual $\{a_i\}$ of the procedure due to the formation of these residual, positive (in terms of improved noise immunity and reliability of data transmission and processing) begins to appear only at presence of the artificial (secondary) information redundancy. Artificial information redundancy is introduced into the NCS due to the use (in addition to n the information base) k control bases SRC. A distinctive feature of SRC is a significant manifestation of primary information redundancy only if secondary, due to the introduction of control bases;

– in the literature [2] was shown, the correction code in the SRC with a simple pairs base is to the value MCD equal of value $d_{\min}^{(SRC)}$ only if the degree of information redundancy is not less than a product any $d_{\min}^{(SRC)} - 1$ base of SRC.

The presence and interaction of primary and secondary information redundant, additional time during the procedure (use of temporal redundancy) in the error correction process, provides in some cases, able to correct single errors in SRC $d_{\min}^{(SRC)} = 2$ (at $k = 1$).

Really, if given the expression (3) and (5), for the orderly SRC, it can be draw a conclusion. When one $(k = 1)$ control based m_{n+1} of the SRC, the NCS $A = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| a_{n+1})$ may have different meanings $d_{\min}^{(SRC)}$. In this case, it depends on the magnitude of the control base m_{n+1}.

If, for each individual module of SRC condition $m_i < m_{n+1}$ $(i = \overline{1, n})$, then, in accordance with the expression (1), we can conclude that $d_{\min}^{(SRC)} = 2$, i. e., in accordance with equation (2) we obtain that $t_{\text{det.}} = 1$. If the totality of information bases $\{m_i\}$ for an arbitrary pair of modules condition $m_i \cdot m_j < m_{n+1}$ $(i, j = \overline{1, n};\ i \neq j)$, in this case $d_{\min}^{(SRC)} = 3$ и $t_{\text{det.}} = 2$. Thus, for the NCS in the SRC with $k = 1$, MCD $d_{\min}^{(SRC)}$ can be different depending on the magnitude of the control base m_{n+1} of the SRC.

Consider the ratio by which the error can be corrected in the residual $\tilde{a}_i$ [1]. Let the wrong number ($\tilde{A} \geq M$) $\tilde{A} = (a_1 \| a_2 \| ... \| a_{i-1} \| \tilde{a}_i \| a_{i+1} \| ... \| a_n \| a_{n+1})$ including error $\tilde{a}_i = (a_i + \Delta a_i) \bmod m_i$ reliably contained in the residue a_i modulo m_i.

It is obvious

$$\tilde{A} = (A + \Delta A) \bmod M_0. \qquad (6)$$

Given that the amount of error may be represented as $\Delta A = (0 \| 0 \| ... \| 0 \| \Delta a_i \| 0 \| ... \| 0 \| 0)$, when the correct ($A < M$) number A can be determined as follows:

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

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

Obtain a quantitative estimate of the value of *A*. Since the number *A* is correct, i.e. stored in the numerical range [0, *M*), then the following inequality must be fulfilled

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

Given that the value ΔA of the error value is equal $\Delta A=\Delta a_i\cdot B_i$, then the inequality (7) will have the following form:

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

Given that the orthogonal basis for the module m_i of the SRC is represented as $B_i=\bar{m}_i\cdot M_0/m_i$, the expression (8) becomes:

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

Since the value of the residual a_i is a natural number, then the value of $m_i(1+r\cdot m_{n+1})/(\bar{m}_i\cdot m_{n+1})-\tilde{A}/B_i$ in the expression (9) must be an integer. Therefore, taking the whole of the last relation, we obtain a formula for the correction of an error in the residual $\tilde{a}_i$ of $\tilde{A}$ as

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

To confirm the results of theoretical studies, we consider examples of monitoring and correction of the data in the SRC.

Example 1. Implement control and, if necessary, to carry out a correction of the number $A_{SRC}=(0\|0\|0\|0\|5)$ which is set in the SRC with the information base $m_1=3$, $m_2=4$, $m_3=5$, $m_5=7$ and with the reference base $m_k=m_5=11$. However $M=\prod_{i=1}^{n}m_i=\prod_{i=1}^{4}m_i=420$ and $M_0=M\cdot m_{n+1}=420\cdot 11=4620$. Orthogonal bases B_i $(i=\overline{1,n+1})$ of SRC are in [6].

I. Data control $A_{SRC}=(0\|0\|0\|0\|5)$. In accordance with the control procedure [1], we define the value of

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

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

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

Thus, the process control is determined that $A_{SRC}=3360>M=420$. In this case, the possible occurrence of only once errors, it is concluded that the number of considered $\tilde{A}_{3360}=(0\|0\|0\|0\|5)$ is incorrect ($3360>M=420$). To correct the number $\tilde{A}_{3360}=(0\|0\|0\|0\|5)$, you must first make a diagnosis data, i.e. identify distorted residual $\tilde{a}_i$. Then it is necessary to determine the true value of the residual a_i to modular m_i and then spend correcting distorted residual $\tilde{a}_i$.

II. Diagnostics data $\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$. In accordance with the method of projections [1,2], we construct possible projections $\tilde{A}_j$ of the number $\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$:

$\tilde{A}_1 = (0 \| 0 \| 0 \| 5)$, $\tilde{A}_2 = (0 \| 0 \| 0 \| 5)$, $\tilde{A}_3 = (0 \| 0 \| 0 \| 5)$, $\tilde{A}_4 = (0 \| 0 \| 0 \| 5)$ и $\tilde{A}_5 = (0 \| 0 \| 0 \| 0)$.

The formula for calculating of the projections of values $\tilde{A}_{j\,PNS}$ in the PNS has the form [1]

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

In accordance with the formula (11) we can calculate all the values $\tilde{A}_{j\,PNS}$. Next, we perform $(n+1)$ a comparison of numbers $\tilde{A}_{j\,PNS}$ with the number $M = M_0 / m_{n+1}$. If among the projections $\tilde{A}_l$ have number no inside information $[0, M)$ numerical range (i.e. $\tilde{A}_k \geq M$), which contains k of the correct numbers, than it is concluded that these k residual of the number A are not distorted. Erroneous may be only the remains which are among the remaining $[(n+1)-k]$ residual number $\tilde{A}_{SRC}$. Set of the partial working base for a given SRC and set of partial orthogonal bases are presented in [6-9]. So, we have that

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

We conclude that the residual a_1 of числа $\tilde{A}_1$ – it is possibly $\bar{a}_1$ distorted residual;

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

Thus, we find that a_2 accurate not distorted residual;

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

We find that a_3 accurate not distorted residual;

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

Conclusion: the residual a_4 to modular m_4 of number $\tilde{A}_4$ – perhaps distorted residual $\bar{a}_4$

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

Since $M_5 = M = 420$, that the residual $\bar{a}_5$ of the control module $m_k = m_5$ will be always a range of possible $\bar{a}_i$ distorted residual of number in the SRC.

The general conclusion. In the process of data diagnostics introduced in NCS $\tilde{A} = (0 \| 0 \| 0 \| 0 \| 5)$, decided not exactly distorted residual: $a_2 = 0$ and $a_3 = 0$. Erroneous may be the residual of the bases m_1, m_4 and m_5, i. e. residual $\bar{a}_1 = 0$, $\bar{a}_4 = 0$ and $\bar{a}_5 = 5$. In this case it is necessary to carry out the correction of residual $\bar{a}_1$, $\bar{a}_4$ and $\bar{a}_5$.

III. It is correction of data error $\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$. As known [1] formula

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

spend correcting $\overline{a}_1$, $\overline{a}_4$ and $\overline{a}_5$ of possible distorted residuals a_1, a_4 and a_5, where $r = 1, 2, 3, \ldots$.

So we have that

$$a_1 = \left(\overline{a}_1 + \left[\frac{m_1 \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \overline{m}_1} - \frac{\tilde{A}}{B_1} \right] \right) \bmod m_1 = \left(0 + \left[\frac{3 \cdot (1 + r \cdot 11)}{11 \cdot 1} - \frac{3360}{1540} \right] \right) \bmod 3 = (0 +$$

$$+ [3,27 - 2,18]) \bmod 3 = (0 + [1,09]) \bmod 3 = (0 + 1) \bmod 3 = 1;$$

$$a_4 = \left(\overline{a}_4 + \left[\frac{m_4 \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \overline{m}_4} - \frac{\tilde{A}}{B_4} \right] \right) \bmod m_4 = \left(0 + \left[\frac{7 \cdot 12}{11 \cdot 4} - \frac{3360}{2640} \right] \right) \bmod 7 = (0 + [1,9 -$$

$$- 1,27]) \bmod 7 = (0 + [0,63]) \bmod 7 = (0 + 0) \bmod 7 = 0;$$

$$a_5 = \left(\overline{a}_5 + \left[\frac{m_{n+1} \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \overline{m}_{n+1}} - \frac{\tilde{A}}{B_5} \right] \right) \bmod m_{n+1} = \left(5 + \left[\frac{11 \cdot (1 + 11)}{11 \cdot 6} - \frac{3360}{2520} \right] \right) \bmod 11 =$$

$$= (5 + [2 - 1,3]) \bmod 11 = (5 + [0,7]) \bmod 11 = (5 + 0) \bmod 5 = 0.$$

According to the resulting residuals $a_1 = 1$, $a_4 = 0$ and $a_5 = 0$, rebuilding (correcting) the number of distorted $\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$, i.e. the correct number, will have the following form: $\tilde{A}_{cor.} = (1 \| 0 \| 0 \| 0 \| 5)$. To verify the data correction, by the known formula [1], we define the value of the number $\tilde{A}_{cor.} = (1 \| 0 \| 0 \| 0 \| 5)$ as follows [4]

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

$$= (1 \cdot 1540 + 0 \cdot 3465 + 0 \cdot 3696 + 0 \cdot 2640 + 5 \cdot 2520) \bmod 4620 = 14140 (\bmod 4620) = 280.$$

Since $280 < M = 420$, so the number $\tilde{A}_{280} = (1 \| 0 \| 0 \| 0 \| 5)$ is correct. In order to clarify the correct procedures of correction of number $\tilde{A}_{3360}$ we spend calculation and comparison of the values and the right residuals $a_2 = 0$ and $a_3 = 0$.

In this case we have $a_2 = \left(0 + \left[\frac{4 \cdot (1 + 11)}{11 \cdot 3} - \frac{3360}{3465} \right] \right) \bmod 4 = 0$ and

$$a_3 = \left(0 + \left[\frac{5 \cdot (1 + 11)}{11 \cdot 4} - \frac{3360}{3696} \right] \right) \bmod 5 = 0.$$

The obtained results $a_2 = 0$ and $a_3 = 0$ of calculations of residuals by modular m_2 and m_3 of SRC, validate the correction of wrong number $\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$. Thus, the original number $\tilde{A}_{SRC} = (0 \| 0 \| 0 \| 0 \| 5)$ is wrong $\tilde{A}_{3360}$, where the single error $\Delta a_1 = 1$ has occurred on the base m_1. This error is transferred the correct number A_{280} to not correct $\tilde{A}_{3360}$. In order to determine whether the correct number A_{280} is true we will carry out additional research of processes of distortion and correction of number A_{280} by the base $m_1 = 3$. The number N_{NW} of possible wrong (distorted) $\tilde{A}_{SRC}$ code words (only a single error) for each correct number A_{SRC} equals $N_{NW} = \sum_{i=1}^{n+1} m_i - (n+1)$.

The results showed that the distortion of the residuals a_1 by modular $m_1 = 3$ of the correct number A_{280} can lead to only two wrong numbers $\tilde{A}_{3360} = (\tilde{0} \| 0 \| 0 \| 0 \| 5)$ and $\tilde{A}_{1820} = (\tilde{2} \| 0 \| 0 \| 0 \| 5)$. This fact indicates that the corrected number $A_{ucn.} = A_{280} = (1 \| 0 \| 0 \| 0 \| 5)$ is not only correct (which lying in the range [0, 420)) but also true. The truth of the resulting number $A_{280} = (\hat{1} \| 0 \| 0 \| 0 \| 5)$ by

the fact that only a single error $\Delta a_1 = 2$ on the base $m_1 = 3$ transfer the number

$$(\tilde{A} = (A + \Delta A) \bmod M_0 = (1 \| 0 \| 0 \| 0 \| 5) + (2 \| 0 \| 0 \| 0 \| 0) = [(1+2) \bmod 3 \| 0 \| 0 \| 0 \| 5] = (\tilde{0} \| 0 \| 0 \| 0 \| 5))$$

to the only wrong number $\tilde{A}_{3360} = (\tilde{0} \| 0 \| 0 \| 0 \| 5)$.

Example 2. Assume that the correct number $A_{280} = (1 \| 0 \| 0 \| 0 \| 5)$ and let $\Delta a_1 = 1$. Then $\tilde{A} = (A + \Delta A) \bmod M_0 = (1 \| 0 \| 0 \| 0 \| 5) + (1 \| 0 \| 0 \| 0 \| 0) = \left[(1+1) \bmod 3 \| 0 \| 0 \| 0 \| 5\right] = (\tilde{2} \| 0 \| 0 \| 0 \| \| 5)$. This number in SRC is corresponded to the number 1820 in the PNS, i.e. number $\tilde{A}_{1820}$ is wrong. Carry out fix number $\tilde{A}_{1820}$. Before correction of number $\tilde{A}_{1820}$ spend data diagnosis. For this we first form the projection A_j ($j = \overline{1, 5}$) of number $\tilde{A}_{1820} = (2 \| 0 \| 0 \| 0 \| 5)$. It will have the following code structure in SRC: $\tilde{A}_1 = (0 \| 0 \| 0 \| 5)$, $\tilde{A}_2 = (2 \| 0 \| 0 \| 5)$, $\tilde{A}_3 = (2 \| 0 \| 0 \| 5)$, $\tilde{A}_4 = (2 \| 0 \| 0 \| 5)$ and $\tilde{A}_5 = (2 \| 0 \| 0 \| 0)$.

Next, we will define all the projections values $\tilde{A}_{j\,PNS}$:

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

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

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

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

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

So as $\tilde{A}_{2ПСС}$, $\tilde{A}_{3ПСС}$ and $\tilde{A}_{4ПСС} > 420$, then it is concluded that the residuals $a_2 = 0$, $a_3 = 0$ and $a_4 = 0$ of number $\tilde{A}_5 = (2 \| 0 \| 0 \| 0 \| 5)$ is not distorted. Distortions $\bar{a}_1 = 2$ and $\bar{a}_5 = 5$ can be only residuals a_1 and a_5. At first spend correcting of residual $\bar{a}_1 = 2$. We have that

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

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

Thus the corrected residual by modular m_1 is equal $a_1 = 1$.

The similar way we obtain the value $a_5 = 5$. According to the resulting residual a_1, a_5 we correct the wrong number $\tilde{A}_{1820} = (\tilde{2} \| 0 \| 0 \| 0 \| 5)$. Eventually, in the process correcting we obtain the correct number $A_{280} = (1 \| 0 \| 0 \| 0 \| 5)$.

Example 3. Implement number control $A_{SRC} = (0 \| 0 \| 0 \| 2 \| 1)$. In the case of distortion diagnose and correct the data.

I. Data check $A_{SRC} = (0 \| 0 \| 0 \| 2 \| 1)$. In accordance with a known procedure of control determine A_{PNS} by the formula

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

$$+ 1 \cdot 2520) \bmod 4620 = 7800 (\bmod 4620) = 3180 > 420.$$

This number is wrong $\tilde{A}_{3180}$.

II. Data diagnostic $\tilde{A}_{3180} = (0 \| 0 \| 0 \| 2 \| 1)$. We construct all possible projections $\tilde{A}_j$ of number $\tilde{A}_{3180}$: $\tilde{A}_1 = (0 \| 0 \| 2 \| 1)$, $\tilde{A}_2 = (0 \| 0 \| 2 \| 1)$, $\tilde{A}_3 = (0 \| 0 \| 2 \| 1)$, $\tilde{A}_4 = (0 \| 0 \| 0 \| 1)$ and $\tilde{A}_5 = (0 \| 0 \| 0 \| 2)$.

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

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

As a result of calculations of values $\tilde{A}_{j\,PNS}$ and comparing them with the value $M = 420$ of the interval length $[0, 420)$ of processing of correct numbers A_{SRC} in SRC we obtain the following.

Set of residuals $a_2 = 0$, $a_4 = 0$ is correct (residuals are not distorted), and the residuals $\bar{a}_1 = 0$, $\bar{a}_3 = 0$ and $\bar{a}_5 = 1$ of the wrong number $\tilde{A}_{3180} = (0\,\|\,0\,\|\,0\,\|\,2\,\|\,1)$ may be distorted (may be wrong).

III. Correction is possible distorted residuals $\bar{a}_1$, $\bar{a}_3$ и $\bar{a}_5$ of the number $\tilde{A}_{3180}$.

It is necessary to be corrected, possibly distorted residuals $\bar{a}_1 = 0$, $\bar{a}_3 = 0$ and $\bar{a}_5 = 1$ by the formula $a_i = \left(\tilde{a}_i + \left[\frac{m_i \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \bar{m}_i} - \frac{\tilde{A}}{B_i} \right] \right) \bmod m_i$. Then we have that

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

In this way $a_1 = 1$. For value $\bar{a}_3$ we have

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

In this way $a_3 = 0$. To obtain the value of the residual $\bar{a}_5$

$$a_5 = \left(\tilde{a}_5 + \left[\frac{m_5 \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \bar{m}_5} - \frac{\tilde{A}}{B_5} \right] \right) \bmod m_5 = \left(1 + \left[\frac{11 \cdot (1 + r \cdot 11)}{11 \cdot 6} - \frac{3180}{2520} \right] \right) \bmod 11 =$$
$$= \left(1 + [2 - 1,26]\right) \bmod 11 = \left(1 + [0,74]\right) \bmod 11 = (1 + 0) \bmod 11 = 1.$$

We have that $a_5 = 1$. According to the obtained values $a_1 = 1$, $a_3 = 0$ and $a_5 = 1$ of the recovered residuals we correct the distorted number $\tilde{A}_{SRC} = (0\,\|\,0\,\|\,2\,\|\,1)$ to the correct number $A_{SRC} = (1\,\|\,0\,\|\,2\,\|\,1)$. It is the check $100 < 420$.

3 Conclusions

In contrast to the code of PNS, the arithmetic codes in the SRC has additional corrective opportunities was shows in the paper. Thus, it is available to the NCS both primary and secondary information redundancy, in some cases, may allow the correction of single errors in SRC with MCL of $d_{\min}^{(KB)} = 2$. However, for correction of single error require carrying out of additional time procedures data processing i.e. use of addition to the information redundancy use of time redundancy. These examples of realization of the specific implementation of correction procedures of single error show

practical feasibility of this method the error correction of error data witch present in the SRC.

References

[1] Akushskii I. Ya. Mashinnaya arifmetika v ostatochnykh klassakh / I. Ya. Akushskii, D. I. Yuditskii. – M.: Sov. radio, 1968. – 440 s.
[2] Torgashov V. A. Sistema ostatochnykh klassov i nadezhnost' TsVM / V. A. Torgashov. – M.: Sov. radio, 1973. – 118 s.
[3] Krasnobaev V. A. Nadezhnostnaya model' EVM v sisteme ostatochnykh klassov / V. A. Krasnobaev // Elektronnoe modelirovanie. – 1985. – №4. – S. 44 – 46.
[4] 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. – 2014. – Vol. 50. – Issue 6. – P. 969-976.
[5] Krasnobaev V.A. Metod ispravleniya odnokratnykh oshibok dannykh, predstavlennykh kodom klassa vychetov / V.A. Krasnobaev, S.A. Koshman, M.A. Mavrina // Elektronnoe modelirovanie. – 2013. – T. 35, № 5. – S. 43–56.
[6] Moroz S.A. Metody kontrolya, diagnostiki i korrektsii oshibok dannykh v informatsionno-telekommunikatsionnoi si-steme, funktsioniruyushchei v klasse vychetov / S.A. Moroz, V.A. Krasnobaev // Informacijno-kerujuchi systemy na zaliznychnomu transporti. – 2012. – № 2. – S. 60–78.
[7] Kuznetsov A. A. Statisticheskii analiz setevogo trafika dlya sistem obnaruzheniya i predotvrashcheniya vtorzhenii / A. A. Kuznetsov, A. A. Smirnov, D. A. Danilenko, A. Berezovskii // Radiotekhnika: Vseukr. mezhved. nauch.-tekhn. sb. – Kh.: KhNURE. – 2014. – Vyp. 176. – S. 97-110.
[8] Kuznetsov A. A. Modelirovanie algebraicheskoi struktury shifra AES s ispol'zovaniem apparata tsepnykh drobei / A. A. Kuznetsov, Yu. I. Gorbenko, S. V. Kostenko // Visnyk KhNU imeni V. N. Karazina. Ser.: Matematychne modeljuvannja. Informacijni tehnologii'. Avtomatyzovani systemy upravlinnja. – 2014. – № 1131. – S. 37-53.
[9] Gorbenko I. D. Statystychni vlastyvosti blokovyh symetrychnyh shyfriv vidpovidno do ISO/IEC 29192-2 / I. D. Gorbenko, O. O. Kuznecov, A. V. Samojlova // Radiotekhnika: Vseukr. mezhved. nauch.-tekhn. sb. – Kh.: KhNURE. – 2014. – Vyp. 176. – S. 40-44.

Рецензент: Олександр Кузнецов, д.т.н., проф., Харківський національний університет імені В. Н. Каразіна, Харків, Україна. E-mail: kuznetsov@karazin.ua

Надійшло: квітень 2016.

Автори:
Віктор Краснобаєв, д.т.н., проф., Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: krasnobaev_va@rambler.ru
Аліна Янко, аспірантка кафедри комп'ютерної інженерії, Полтавський національний технічний університет імені Юрія Кондратюка, Полтава, Україна. E-mail: al9_yanko@ukr.net
Сергій Кошман, к.т.н., доцент, Харківський національний технічний університет сільського господарства імені Петра Василенка, Харків, Україна. E-mail: s_koshman@ukr.net

Метод виявлення і корекції помилок у системі залишкових класів

Анотація. Розглянуто метод виправлення однократних помилок у системі залишкових класів (СЗК). Результати аналізу коригувальних можливостей арифметичного коду показали високу ефективність використання непозиційних кодових структур у СЗК. У статті наведені приклади виправлення одноразових помилок даних, що представлені кодом СЗК.

Ключові слова: система залишкових класів, достовірність контролю даних, інформаційна надмірність, корекція однократних помилок даних.

Рецензент: Александр Кузнецов, д.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина. E-mail: kuznetsov@karazin.ua

Поступила: апрель 2016.

Авторы:
Виктор Краснобаев, д.т.н., проф., Харьковский национальный университет имени В. Н. Каразина, Харьков, Украина.
E-mail: krasnobaev_va@rambler.ru
Алина Янко, аспирантка кафедры компьютерной инженерии, Полтавский национальный технический университет имени Юрия Кондратюка, Полтава, Украина. E-mail: al9_yanko@ukr.net
Сергей Кошман, к.т.н., доцент, Харьковский национальный технический университет сельского хозяйства имени Петра Василенка, Харьков, Украина. E-mail: s_koshman@ukr.net

Метод обнаружения и коррекции ошибок в системе остаточных классов

Аннотация. Рассмотрен метод исправления однократных ошибок в системе остаточных классов (СОК). Результаты анализа корректирующих возможностей арифметического кода показали высокую эффективность использования непозиционных кодовых структур в СОК. В статье приведены примеры исправления однократных ошибок данных, представленных кодом СОК.

Ключевые слова: система остаточных классов, достоверность контроля данных, информационная избыточность, коррекция однократных ошибок данных.

Vesa A. Niskanen
Ph.D., Adjunct Professor,
Department of Economics & Management, University of Helsinki,
P.O. Box 27 (Latokartanonkaari 9), 00014 Helsinki, Finland
E-mail: vesa.a.niskanen@helsinki.fi

Igor Romenskiy
Doktor für physikalische-mathematische Wissenschaften,
GFaI Gesellschaft zur Förderung angewandter Informatik e.V.,
Volmerstraße 3, 12489 Berlin, Deutschland
E-mail: iromensky@mail.ru

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

Vadim Geurkov
Ph.D., Associate Professor,
Department of Electrical and Computer Engineering
Ryerson University,
350 Victoria Street, Toronto, Ontario, M5B 2K3, Canada
E-mail: vgeurkov@ee.ryerson.ca

Fionn Murtagh
Ph.D., Professor,
Department of Computing and Mathematics, University of Derby,
Kedleston Road, Derby DE22 1GB, UK
Email: f.murtagh@derby.ac.uk
Department of Computing, Goldsmiths, University of London,
New Cross, London SE14 6NW, UK
E-mail: f.murtagh@gold.ac.uk

C. Pandu Rangan
PhD, FNAE, Senior Professor,
Department of Computer Science and Engineering,
Indian Institute of Technology,
Madras, Chennai - 600036, India
E-mail: prangan55@gmail.com

Håvard Raddum
Ph.D.,
Simula Research Laboratory, P.O. Box 134, 1325 Lysaker, Norway
E-mail: haavardr@simula.no

Oleksandr Kazymyrov
Ph.D.,
EVRY Norge AS,
Snarøyveien 30A, 1360 Fornebu, Norway
E-mail: oleksandr.kazymyrov@evry.com

Mikołaj Karpiński
Doctor of Sciences (Engineering), Full Professor,
University of Bielsko-Biala,
ul. Willowa 2, 43-309 Bielsko-Biala, Poland
E-mail: mkarpinski@ath.bielsko.pl

Веса А. Нисканен
доктор філософії, ад'юнкт професор,
департамент економіки та менеджменту, Університет Гельсінкі,
Р.О. Бокс 27 (Латокартанонкаарі 9), 00014 Гельсінкі, Фінляндія
E-mail: vesa.a.niskanen@helsinki.fi

Ігор Роменський
доктор фізико-математичних наук,
GFaI - Спільнота з просування прикладної інформатики,
Фольмерштрассе 3, 12489 Берлін, Німеччина
E-mail: iromensky@mail.ru

Олексій Стахов
доктор технічних наук, професор, академік Академії інженерних наук України,
Міжнародний Клуб Золотого Перетину,
6 МаккКрері Трейл, Болтон, Онтаріо, L7E 2C8, Канада
E-mail: goldenmuseum@rogers.com

Вадим Геворков
доктор філософії, доцент,
факультет електротехніки та обчислювальної техніки університету Раєрсон,
350 Вікторія-стріт, Торонто, Онтаріо, M5B 2K3, Канада
E-mail: vgeurkov@ee.ryerson.ca

Фінн Мерта
доктор філософії, професор,
факультет обчислювальної математики університету Дербі,
Кедлестон Роад, Дербі DE22 1GB, Великобританія
Email: f.murtagh@derby.ac.uk
факультет обчислень Голдсмітського коледжу Лондонського університету,
Нью-Крос, Лондон SE14 6NW, Великобританія
E-mail: f.murtagh@gold.ac.uk

С. Панду Ренген
доктор філософії, FNAE, старший викладач,
факультет комп'ютерних наук та інженерії Індійського технологічного інституту,
Мадрас, Ченнаї - 600036, Індія
E-mail: prangan55@gmail.com

Ховард Радум
доктор філософії,
науково-дослідна лабораторія Симула, Р.О. Бокс 134, 1325, Лісакер, Норвегія
E-mail: haavardr@simula.no

Олександр Казіміров
доктор філософії,
EBPI Норге АС,
Снаройвиен 30А, 1360 Форнебу, Норвегія
E-mail: oleksandr.kazymyrov@evry.com

Микола Карпінський
доктор технічних наук, професор,
Університет Бельсько-Бяла,
вул. Віллова 2, 43-309 Бельсько-Бяла, Польща
E-mail: mkarpinski@ath.bielsko.pl

Volodymyr Khoma
Doctor of Sciences (Engineering), Full Professor,
Institute «Automatics and Informatics», The Opole University of Technology,
76 Prószkowska Street, 45-758 Opole, Poland
E-mail: xoma@wp.pl

Joanna Świątkowska
Ph.D., CYBERSEC Programme Director,
Senior Research Fellow of the Kosciuszko Institute,
Feldmana ul. 4/9-10, 31-130 Kraków, Poland
E-mail: joanna.swiatkowska@ik.org.pl

Nick Bilogorskiy
Director of Security Research,
Cyphort, 5451 Great America Parkway, Suite 225,
Santa Clara, California 95054, USA
E-mail: nick@novaukraine.org

Richard Kemmerer
Ph.D., Professor,
Computer Science Department, University of California,
Santa Barbara, CA 93106, USA
E-mail: kemm@cs.ucsb.edu

Dimiter Velev
Ph.D., Professor,
Department of Information Technologies and Communications, Faculty of Applied Informatics and Statistics, University of National and World Economy,
„8-ми декември“ st., UNSS - Studentski grad, 1700 Sofia, Bulgaria
E-mail: dgvelev@unwe.bg

Robert Brumnik
Ph.D., Professor Assistant,
GEA College, Dunajska cesta 156, 1000 Ljubljana, Slovenia
Metra Engineering Ltd, Špruha 19, 1236 Trzin, Slovenia
E-mail: robert.brumnik@metra.si

Ludmila Babenko
Doctor of Sciences (Engineering), Full Professor,
Institute of Computer Technologies and Information Safety of Southern Federal University
Chekhov str., 2, Taganrog, Rostov obl., Russia
E-mail: blk@tsure.ru

Valeriy Zadiraka
Doctor of Sciences (Physics and Mathematics),
Full Professor, Academician of the National Academy of Sciences of Ukraine, Glushkov Institute of Cybernetics (GIC) of National Academy of Sciences of Ukraine,
40 Glushkov av., Kyiv, 03187, Ukraine
E-mail: zvk140@ukr.net

Ludmila Kovalchuk
Doctor of Sciences (Engineering), Associate Professor,
Department of mathematical methods of information security Institute of Physics and Technology,
National Technical University of Ukraine
"Kyiv Polytechnic Institute"
37, Prospect Peremohy, 03056, Kyiv-56, Ukraine
E-mail: lusi.kovalchuk@gmail.com

Володимир Хома
доктор технічних наук, професор,
Інститут «Автоматика та інформатика», Технологічний університет Ополе,
76 Пружовська Вулиця, 45-758 Ополе, Польща
E-mail: xoma@wp.pl

Джоана Святковська
доктор філософії, директор програми CYBERSEC,
старший науковий співробітник Інституту Костюшки
вул. Фельдман 4 / 9-10, 31-130 Краків, Польща
E-mail: joanna.swiatkowska@ik.org.pl

Нік Білогорський
директор з досліджень безпеки,
Цифорт, 5451 Гріт Америка Парквей, Люкс 225,
Санта-Клара, Каліфорнія 95054, США
E-mail: nick@novaukraine.org

Річард Кеммерер
PhD., професор,
факультет інформатики, Каліфорнійський університет,
Санта-Барбарі, CA 93106, США
E-mail: kemm@cs.ucsb.edu

Дімітер Велев
доктор філософії, професор,
кафедра інформаційних технологій і комунікацій,
факультет прикладної інформатики та статистики,
Університет національної та світової економіки,
вул. "8-ми декември", UNSS - Студентські град, 1700 Софія, Болгарія
E-mail: dgvelev@unwe.bg

Роберт Брумнік
доктор філософії, доцент,
GEA коледж, Дунайська цеста 156, 1000 Любляна, Словенія
Метра Інжиніринг ЛТД, Шпруха 19,1236 Тржин, Словенія
E-mail: robert.brumnik@metra.si

Людмила Бабенко
доктор технічних наук, професор,
Інститут комп'ютерних технологій та інформаційної безпеки Південного федерального університету
вул. Чехова 2, Таганрог, Ростовська обл., Росія
E-mail: blk@tsure.ru

Валерій Задірака
доктор технічних наук, професор,
академік Національної академії наук України,
Інститут кібернетики імені В.М. Глушкова Національної академії наук України,
проспект Академіка Глушкова, 40, Київ, 03187, Україна
E-mail: zvk140@ukr.net

Людмила Ковальчук
доктор технічних наук, доцент,
кафедра математичних методів захисту інформації фізико-технічного інституту
національного технічного університету України «КПІ»,
03056, Київ, пр. Перемоги, 37, НТУУ "КПІ"
E-mail: lusi.kovalchuk@gmail.com

Anton Alekseychuk
Doctor of Sciences (Engineering), Associate Professor, Department of application of means of cryptographic and technical defense of information, Institute of Special Communication and Information Security, National Technical University of Ukraine "Kyiv Polytechnic Institute"
37, Prospect Peremohy, 03056, Kyiv-56, Ukraine
E-mail: alex-dtn@ukr.net

Антон Олексійчук
доктор технічних наук, доцент, кафедра застосування засобів криптографічного та технічного захисту інформації Інституту спеціального зв'язку та захисту інформації національного технічного університету України «КПІ», 03056, Київ, пр. Перемоги, 37, НТУУ "КПІ"
E-mail: alex-dtn@ukr.net

Volodymyr Maxymovych
Doctor of Sciences (Engineering), Full Professor, Institute of Computer Technologies, Automation and Metrology (ICTA), Lviv Polytechnic National University, 12 Bandera st., Lviv, 79013, Ukraine
E-mail: vmax@polynet.lviv.ua

Володимир Максимович
доктор технічних наук, професор, Інститут комп'ютерних технологій, автоматики та метрології Національного університету «Львівська політехніка», вул. Степана Бандери, 12, м. Львів, 79013, Україна
E-mail: vmax@polynet.lviv.ua

Oleksiy Borysenko
Doctor of Sciences (Engineering), Full Professor, Sumy State University,
2, Rymskogo-Korsakova st., 40007 Sumy, Ukraine
E-mail: 5352008@ukr.net

Олексій Борисенко
доктор технічних наук, професор, Сумський державний університет, вул. Римського-Корсакова, 2, 40007 Суми, Україна
E-mail: 5352008@ukr.net

Anatoliy Biletsky
Doctor of Sciences (Engineering), Full Professor, Institute of Air Navigation, National Aviation University, Kosmonavta Komarova av. 1, Kyiv, 03058, Ukraine
E-mail: abelnau@ukr.net

Анатолій Білецький
доктор технічних наук, професор, навчально-науковий інститут аеронавігації національного авіаційного університету, пр. Космонавта Комарова 1, Київ, 03058, Україна
E-mail: abelnau@ukr.net

Sergii Kavun
Doctor of Sciences (Economics), Ph.D. (Engineering), Full Professor, Department of Information Technologies, Kharkiv Educational and Research Institute of the University of Banking,
Peremogy av. 55, Kharkiv, 61174, Ukraine
E-mail: kavserg@gmail.com

Сергій Кавун
доктор економічних наук, кандидат технічних наук, професор, кафедра інформаційних технологій, Харківський навчально-науковий інститут ДВНЗ "Університет банківської справи", пр. Перемоги 55, м. Харків, 61174, Україна
E-mail: kavserg@gmail.com

Vyacheslav Kharchenko
Doctor of Sciences (Engineering), Full Professor, Academician of the Academy of Applied Radioelectronics Sciences, N.Ye. Zhukovskiy National Aerospace University – Kharkiv Aviation Institute (KhAI),
17 Chkalov st., 61070, Kharkiv, Ukraine
E-mail: v_s_kharchenko@ukr.net

В'ячеслав Харченко
доктор технічних наук, професор, академік Академії наук прикладної радіоелектроніки, Національний аерокосмічний університет ім. М. Є. Жуковського, вул. Чкалова, 17, 61070, м. Харків, Україна
E-mail: v_s_kharchenko@ukr.net

Valentin Lazurik
Doctor of Sciences (Physics and Mathematics), Full Professor, V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: vtlazurik@karazin.ua

Валентин Лазурик
доктор фізико-математичних наук, професор, Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, м. Харків, 61022, Україна
E-mail: vtlazurik@karazin.ua

Volodymyr Kuklin
Doctor of Sciences (Physics and Mathematics), Full Professor, V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: kuklinvm1@gmail.com

Володимир Куклін
доктор фізико-математичних наук, професор, Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, м. Харків, 61022, Україна
E-mail: kuklinvm1@gmail.com

Ivan Gorbenko
Doctor of Sciences (Engineering), Full Professor, Academician of the Academy of Applied Radioelectronics Sciences, V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: gorbenkoi@iit.kharkov.ua

Іван Горбенко
доктор технічних наук, професор, академік Академії наук прикладної радіоелектроніки, Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, м. Харків, 61022, Україна
E-mail: gorbenkoi@iit.kharkov.ua

Victor Krasnobayev
Doctor of Sciences (Engineering), Full Professor,
Honourable Inventor of Ukraine,
Honourable Radio Specialist of the USSR,
V. N. Karazin Kharkiv National University,
Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: krasnobayev@karazin.ua

Irina Lisitska
Doctor of Sciences (Engineering), Full Professor,
Corresponding Member of the Academy of Applied Radioelectronics Sciences,
V. N. Karazin Kharkiv National University,
Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: lisitska@karazin.ua

Oleksandr Potii
Doctor of Sciences (Engineering), Full Professor,
Academician of the Academy of Applied Radioelectronics Sciences, V. N. Karazin Kharkiv National University,
Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: potav@ua.fm

Viktor Dolgov
Doctor of Sciences (Engineering), Full Professor,
Academician of the Academy of Applied Radioelectronics Sciences, V. N. Karazin Kharkiv National University,
Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: dolgovvi@mail.ru

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

Volodymyr Mashtalir
Doctor of Sciences (Engineering), Full Professor,
V. N. Karazin Kharkiv National University,
Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: mashtalir@kture.kharkov.ua

Grygoriy Zholtkevych
Doctor of Sciences (Engineering), Full Professor,
V. N. Karazin Kharkiv National University,
Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: g.zholtkevych@karazin.ua

Віктор Краснобаєв
доктор технічних наук, професор, заслужений винахідник України, почесний радист СРСР,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: krasnobayev@karazin.ua

Ірина Лисицька
доктор технічних наук, професор,
член-кореспондент Академії наук прикладної радіоелектроніки, Харківський національний університет імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: lisitska@karazin.ua

Олександр Потій
доктор технічних наук, професор,
академік Академії наук прикладної радіоелектроніки,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: potav@ua.fm

Віктор Долгов
доктор технічних наук, професор,
академік Академії наук прикладної радіоелектроніки,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: dolgovvi@mail.ru

Роман Олійников
доктор технічних наук, професор,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: roliynykov@gmail.com

Володимир Машталір
доктор технічних наук, професор,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: mashtalir@kture.kharkov.ua

Григорій Жолткевич
доктор технічних наук, професор,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: g.zholtkevych@karazin.ua

Статті пройшли внутрішнє та зовнішнє рецензування.

Наукове видання

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА

Випуск 1(1) 2016

Міжнародний електронний науково-теоретичний журнал

Англійською, українською, російською мовами

Комп'ютерне верстання – Федоренко В.В.

61022, Харків, майдан Свободи, 6
Харківський національний університет імені В.Н. Каразіна

V. N. Karazin Kharkiv National University Publishing