ISSN 2519-2310

COMPUTER SCIENCE AND CYBERSECURITY

ISSUE 3(7) 2017

V. N. Karazin Kharkiv National University Publishing

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

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

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

Issue 3(7) 2017

Заснований 2015 року

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

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

Journal is published quarterly.
Approved for placement on the Internet by Academic Council of the Karazin Kharkiv National University (November 27, 2017, protocol No. 17).

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

Published articles have been internally and externally peer reviewed

TABLE OF CONTENTS

Issue 3(7) 2017

UDC 004.056.55

PERIODIC CHARACTERISTICS OF OUTPUT FEEDBACK ENCRYPTION MODE

Alexandr Kuznetsov, Ievgeniia Kolovanova, Tetiana Kuznetsova

V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
kuznetsov@karazin.ua, e.kolovanova@gmail.com, kuznetsova.tatiana17@gmail.com

Reviewer: Serhii Toliupa, Doctor of Sciences (Engineering), Full Prof., Taras Shevchenko National University of Kiev, Lomonosova St., 81, Kyiv, 03189, Ukraine.
tolupa@i.ua

Received on May 2017

Abstract. *We investigate periodic characteristics of sequence of output blocks in the output feedback encryption mode. The model of random homogeneous substitution is used for an abstract description of this formation. This property is directly related to the periodic properties of output feedback encryption mode, since it characterizes the probabilistic distribution of output blocks with certain period appearance, provided that the assumption is made that the properties of the block symmetric cipher are consistent with certain properties of the random substitution. Also in the work specific practical tasks are solved, namely recommendations are being developed for the application of the outbound feedback on the encryption threshold, certain requirements and limitations are justified.*

Keywords: *encryption mode; random substitution; periodic characteristics of output blocks; output feedback.*

1 Introduction

One of the most common block symmetric encryption modes used to provide confidentiality services is Outbound Feedback (OFB). The OFB has several advantages: firstly, the output block can be formed in advance, even before the message, which can greatly speed up the process of protecting information; and secondly, in this mode, as in the mode Electronic Codebook - ECB, errors that can arise when transmitting ciphertext over the communication channels, are localized in the block, not extending to the neighboring, and in the OFB mode only changed bits will be false (in the ECB mode the entire block will change). Thirdly, the cryptographic properties of the output block do not depend on the open text, they are determined only by the properties of the base cryptographic transformation, and, possibly, by the value of the initialization block, which determines the specific form and frequency of the output block. This work is devoted to study of the periodic properties of output block in OFB mode, because the occurrence of output block repetition is the most dangerous case, it gives an attacker the possibility to violate the established mode of message confidentiality.

We derive a formula for estimating the probability of a cycle occurrence for an arbitrary fixed value of a set of transformations. This property is directly related to the periodic properties of the output blocks, since it characterizes the probabilistic distribution of the output block with certain period appearance, provided that the assumption is made that the properties of the block symmetric cipher are consistent with certain properties of the random substitution. Also in the work specific practical tasks are solved, namely recommendations are being developed for the application of the Outbound Feedback on the encryption threshold, certain requirements and limitations are justified. The conclusions summarize and concretize our results, discuss possible ways of further research.

2. Output Feedback Encryption Mode

The output feedback encryption mode is intended to provide a confidentiality service. This mode is based on encryption of the initialization vector to generate a sequence of output blocks that are added to the normal text to form encrypted text and, conversely, to the ciphertext to decrypt it. This mode requires unique initialization vector for each application with the provided (fixed) key. Let's

consider the specification of output feedback encryption mode.

The parameters of the mode are encryption key K, $|K|=k$, and initialization vector S, $|S|=l$. Additional requirements for initialization vector are not imposed. When encrypting the message M ($|M|\geq 1$) is presented as a sequence of blocks:

$$M=m_1\|m_2\|...\|m_n,\ |m_i|=l$$

for $i=1,2,..,n-1$, $1\leq|m_n|\leq l$.

The initial value of the output block γ_0 ($|\gamma_0|=l$) is calculated as

$$\gamma_0=T_{l,k}^{(K)}(S). \quad (1)$$

Each ciphertext block is calculated according to the ratio

$$c_i=m_i\oplus L_{l,|m_i|}(\gamma_{i-1}) \quad (2)$$

for $i=1,2,..,n$, and

$$\gamma_i=T_{l,k}^{(K)}(\gamma_{i-1}) \quad (3)$$

for $i=1,2,..,n-1$.

The result of message encrypting is ciphertext $C=c_1\|c_2\|...\|c_n$.

When decrypting, the ciphertext C ($|C|\geq 1$) is presented in the form of a sequence of blocks:

$$C=c_1\|c_2\|...\|c_n,\ |c_i|=l$$

for $i=1,2,..,n-1$, $1\leq|c_n|\leq l$.

The initial value of the output block γ_0 ($|\gamma_0|=l$) is calculated as

$$\gamma_0=T_{l,k}^{(K)}(S).$$

Each message block is calculated according to the ratio

$$m_i=c_i\oplus L_{l,|m_i|}(\gamma_{i-1}) \quad (4)$$

for $i=1,2,..,n$, and

$$\gamma_i=T_{l,k}^{(K)}(\gamma_{i-1})$$

for $i=1,2,..,n-1$.

The result of the decryption of ciphertext is the message $M=m_1\|m_2\|...\|m_n$.

The encryption and decryption scheme in the output feedback encryption mode is shown in Fig. 1. This scheme formally depicts the sequence of execution of transformations (2), (4) for all values of the cyclic variable $i=1,2,..,n$.

Let's consider the periodic characteristics of output feedback encryption mode. First, we note that, by definition, the output block consists of the initial value of the block γ_0 and the remaining blocks γ_i, which are calculated for (1), (3) for each value of the cyclic variable $i=1,2,..,n-1$. That is, the task of the research is precisely in determining the period of the sequence of blocks $\gamma_i, i=0,1,..,n-1$.

Each output block γ_i is the result of encrypting the previous block γ_{i-1}, where the initial value γ_0 is equal to the result of the initialization vector encryption. If you use the terminology of the substitutions theory [1-3] and present the basic encryption transformation $T_{l,k}^{(K)}$ initiated by the secret key K as some substitution s acting on the set of open texts, then the period of the sequence of

output blocks γ_0, γ_1, …, γ_{n-1} will correspond to one of the cycles $s_i = (y, s_i(y), s_i^2(y), ..., s_i^{l_i-1}(y))$ of the substitution s where the initial value of the cycle y is equal to the initialization vector value S.

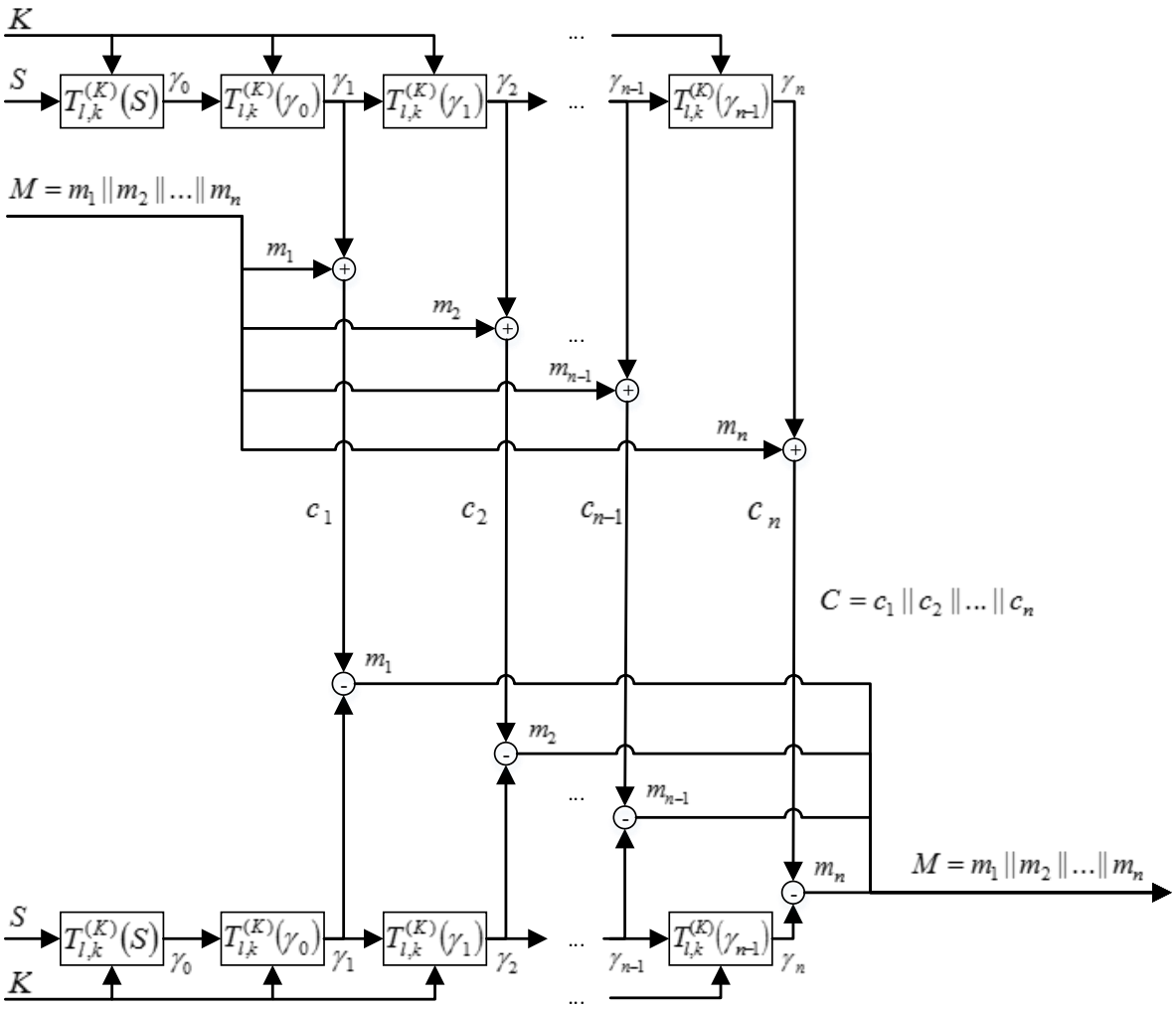

Fig. 1 – Scheme of encryption and decryption

Each next element $s_i^j(y)$ of the cycle s_i with the length l_i is the result of multiple encoding of the initialization vector:

$$y = S;$$

$$s_i(y) = T_{l,k}^{(K)}(S) = \gamma_0;$$

$$s_i^2(y) = T_{l,k}^{(K)}\left(T_{l,k}^{(K)}(S)\right) = \gamma_1;$$

$$\dots$$

$$s_i^{l_i-1}(y) = \underbrace{T_{l,k}^{(K)}\left(T_{l,k}^{(K)} \dots T_{l,k}^{(K)}(S)\right)}_{l_i-1 \text{ разів}} = \gamma_{l_i-2};$$

$$s_i^{l_i}(y) = \underbrace{T_{l,k}^{(K)}\left(T_{l,k}^{(K)} \dots T_{l,k}^{(K)}(S)\right)}_{l_i \text{ разів}} = \gamma_{l_i-1} = \gamma_0;$$

$$\dots$$

$$s_i^n(y) = \underbrace{T_{l,k}^{(K)}\left(T_{l,k}^{(K)} \dots T_{l,k}^{(K)}(S)\right)}_{n \text{ разів}} = \gamma_{n-1}.$$

Thus, the investigation of the periodic properties of the sequence of output blocks $\gamma_i, i = 0,1,..,n$ is to study the cyclic structure of the substitution s, namely, in estimating the distribution of the length l_i of the cycles s_i for different initial values $y = S$ of the basic ciphering transformation $T_{l,k}^{(K)}$. Such investigations will make it possible to estimate the length l_i of output blocks period for different $y = S$ and K or to determine the probability of forming the output blocks of a certain period for an arbitrary fixed value of the initialization vector $y = S$ and a randomly selected secret key K.

Let us consider some of the provisions of the theory of substitutions and their relation to the properties of BSC, in particular, we introduce the basic concepts and definitions associated with certain properties of symmetric block crypto-transformations (the distribution of the number of cycles, magnifications and inversions, etc.).

3. Special Provisions of the Theory of Substitutions

By the definition BSC is a key-parameterized function of a bijective mapping of a set of plaintexts into a set of ciphertexts $V_l \to V_l$, $K \in V_k$ [4]. In general, for any *l*-bit block cipher there are $2^l!$ possible permutations of plaintext. These transformations, called permutations of degree 2^l, form a group under the operation of performing sequential transformations. Such a group is called a symmetric group of permutations of degree 2^n and is denoted by S_{2^l} [1]. In practice, it means that the number of bits of the key, which is necessary to obtain all possible permutations, is about $\ln 2^l! \approx l \cdot 2^l$ bits (by the Stirling formula $\ln(x!) = x\ln(x) - x - O(\ln(x))$). For example, for l = 128, we have $2^{128}! \approx 2^{128 \cdot 2^{128}}$ possible permutations of 128-bits blocks, of which, depending on the length of the key, only 2^{128} or 2^{256} transformations are used. Thus, the basic transformation of the cipher is essentially a subset of the complete set of all possible substitutions acting on a set of processed data blocks. The basic assumption that is adopted in substantiating the stability of symmetric cryptographic transformation is in preserving the probabilistic properties of random substitution. It is assumed that while encrypting and applying a limited set of substitutions from S_{2^l}, however, certain distribution probabilities of this subset elements correspond to the properties of randomly selected substitutions from the whole set S_{2^l} [5-8].

Let's consider the basic concepts and definitions of the theory of substitutions [1] and associate them with cyclic properties of BSC. For this we consider the set of all biective transformations of the set $Y = \{y_1, y_2, ..., y_n\}$ to itself, forming a symmetric group S_n with the power $n!$ of all possible substitutions of degree *n*. By definition of the symmetric group [1], each substitution $s \in S_n$ corresponds to a unique substitution $s^{-1} \in S_n$, such that

$$s^{-1} \cdot s(y) = s \cdot s^{-1}(y) = e(y), \; y \in Y,$$

where $e(y) \in S_n$ is the unit substitution, i.e. $e(y) = y$ for all $y \in Y$.

Let's use the following symbols:

$$s \cdot s \cdot ... \cdot s = s^k, \; s^{-1} \cdot s^{-1} \cdot ... \cdot s^{-1} = s^{-k},$$

where products contain k multipliers. Accordingly, we have

$$s^k \cdot s^{-k} = s^{-k} \cdot s^k = s^0 = e.$$

The set of substitutions of degree *n*, which is locked in relation to the multiplication and inverse computation operation for $s \in S_n$ an element $s^{-1} \in S_n$, is called substitution group. Each such group is a subgroup of the symmetric group S_n [1].

Consider some substitutions $s \in S_n$ that act on a set Y. We will define a binary relation on a set Y, while we will assume that $y \sim y'$ for $y, y' \in Y$ if there exists such j that $y' = s^j(y)$. This bina-

ry relation is reflexive, symmetric and transitive, i.e. the relation is equivalence. Indeed, according to [1] we have:

- $y \sim y$, because $y = s^0(y) = e(y)$;
- - it follows from condition $y \sim y'$ that $y' \sim y$, because it follows from equality $y' = s^j(y)$ that $y = s^{-j}(y')$;
- - it follows from $y \sim y'$ and $y' \sim y"$ that $y \sim y"$, because from the equalities $y' = s^j(y)$ and $y" = s^i(y')$ it follows that $y" = s^i(s^j(y)) = s^{i+j}(y)$.

The cycle s_i of substitution $s \in S_n$ with the length l_i is defined as follows:

$$s_i = (y, s_i(y), s_i^2(y), ..., s_i^{l_i-1}(y)),$$

where $s_i^{l_i}(y) = y$.

An arbitrary substitution $s \in S_n$ can be expanded into the corresponding cycles [1]:

$$s = (y_1, s_1(y_1), s_1^2(y_1), ..., s_1^{l_1-1}(y_1))...(y_k, s_k(y_k), s_k^2(y_k), ..., s_k^{l_k-1}(y_k)). \quad (5)$$

Elements y_i and y_{i+1} in substitution $s \in S_n$ form increment, if $s(y_i) > s(y_{i+1})$ it is assumed that an element y_1 always preceded by increment. A pair of elements y_i and y_j in substitution $s \in S_n$ forms an increment if $s(y_i) > s(y_j)$, $i < j$.

For example, the substitution s of degree 4

$$s = \begin{pmatrix} y_1 & y_2 & y_3 & y_4 \\ s(y_1) & s(y_2) & s(y_3) & s(y_4) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

can be given in the form of a schedule for 3 cycles:

$$s_1 = (y_1) = (1),\ l_1 = 1;$$
$$s_2 = (y_2, s_2(y_2)) = (2,4),\ l_2 = 2;$$
$$s_3 = (y_3) = (3),\ l_3 = 1.$$

We have the following schedule:

$$s = (y_1)(y_2, s_2(y_y))(y_3) = (1)(2,4)(3).$$

In this substitution there are two increments (the element $y_1 = 1$ always preceded by one increment, and one more increment forms the elements $y_1 = 1$ and $y_2 = 2$, because $s(y_1) = 1 > s(y_2) = 4$) and three inversions (they form pairs of elements y_2 and y_3, y_2 and y_4, y_3 and y_4, because there are inequalities $s(y_2) > s(y_3)$, $s(y_2) > s(y_4)$, $s(y_3) > s(y_4)$, respectively).

On the set of all permutations of the symmetric group S_n, we give a uniform probabilistic distribution, i.e. for each selected substitution $s \in S_n$ we put in correspondence the probability of its selection equal to $1/n!$. According to modern views of symmetric cryptography, such a set of equivalence mappings corresponds to the idea of an "ideal" cipher. After all, if the random selection of a separate substitution $s \in S_n$ is associated with the value of the entered encryption key, then the resulting conversion will match the random and evenly selected ciphertext for each open text with any key, i.e. in all possible variants of open text mapping in the ciphertext.

We will investigate the probabilistic properties of random substitution, in particular, the probabilities of a cycle of a certain length in a randomly selected substitution, since this particular event will correspond to the case when the output block γ_i of a certain period is formed for an arbitrary fixed value of the initialization vector S.

4. Probability Evaluation of a Certain Length Cycle in Randomly Selected Substitution

Consider a random value ξ_n equals to the number of cycles in a randomly chosen substitution $s \in S_n$. The substitution $s \in S_n$ refers to a cyclic class $\{1^{\alpha_1}2^{\alpha_2}...n^{\alpha_n}\}$ if it contains α_1 cycles of length 1, α_2 cycles of length 2, and so on:

$$s = (y_1)(y_2)...(y_{\alpha_1})(y'_1, y''_1)(y'_2, y''_2)...(y'_{\alpha_2}, y''_{\alpha_2})...,$$
$$1\alpha_1 + 2\alpha_2 + ... + n\alpha_n = n.$$

Denote by $C(\alpha_1, \alpha_2, ..., \alpha_n)$ the number of substitutions in the cyclic class $\{1^{\alpha_1}2^{\alpha_2}...n^{\alpha_n}\}$, and by $C(n,k)$ the number of substitutions of degree n that have k cycles. Then we have [1]:

$$C(\alpha_1, \alpha_2, ..., \alpha_n) = \frac{n!}{1^{\alpha_1}2^{\alpha_2}...n^{\alpha_n}\alpha_1!\alpha_2!...\alpha_n!},$$

$$C(n,k) = \sum_{\substack{1\alpha_1+2\alpha_2+...+n\alpha_n=n \\ \alpha_1+\alpha_2+...+\alpha_n=k,\ \alpha_i\geq 0}} \frac{n!}{1^{\alpha_1}2^{\alpha_2}...n^{\alpha_n}\alpha_1!\alpha_2!...\alpha_n!} = |s(n,k)|, \quad (6)$$

where $s(n,k)$ are Stirling numbers of first kind, which is determined by the ratio

$$(x)_n = x(x-1)...(x-n+1) = \sum_{k=0}^{n} s(n,k)x^k,$$

where $(x)_n = x(x-1)...(x-n+1)$ is the common designation of the declining factorial (*the symbol of Pohgammer*).

Formula (6) implies the expression for the exact probability distribution of a random event $\xi_n = k$, in the case where randomly selected substitutions will observe exactly k cycles (see expression (5)).

Using the formula for computing Stirling numbers of the first kind, we have [1]:

$$P(\xi_n = k) = \frac{C(n,k)}{n!} = \frac{|s(n,k)|}{n!},\ k = 0,1,...,n.$$

In [1] we obtain the expected value $M\xi_n$ and variance $D\xi_n$ of the random variable ξ_n:

$$M\xi_n = \sum_{j=1}^{n}\frac{1}{j} = \ln n + C + o(1),\ D\xi_n = \sum_{j=1}^{n}\frac{1}{j} - \sum_{j=1}^{n}\frac{1}{j^2} = \ln n + C + o(1),\ C = 0,5772...,$$

in addition, it is shown that when $n \to \infty$ a random variable $\xi'_n = (\xi_n - \ln n)/(\ln n)$ is distributed asymptotically with parameters $(0,\ 1)$

$$\lim_{n\to\infty} P(\xi'_n < u) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{u} e^{-y^2/2}dy$$

For random variables ζ_n and η_n, which are equal to the number of increments and inversions in randomly selected substitution $s \in S_n$, the corresponding expected value and variance have the form [1]:

$$M\zeta_n = \frac{n(n-1)}{4},\ D\zeta_n = \frac{2n^3+3n^2-5n}{72},\ M\eta_n = \frac{n}{2},\ D\eta_n = \frac{n}{12},$$

in this case random variables

$$\zeta'_n = (\zeta_n - M\zeta_n)/(D\zeta_n)$$

when $n \to \infty$ are also asymptotically distributed with parameters $(0,\ 1)$.

Empirical distributions of the probability of occurrence of a certain number of cycles, increments and inversions in randomly selected substitutions from a certain subset $V \subset S_n$, whose elements are substitutions implemented by the use of the encryption function on reduced cipher models, are investigated in [5, 8]. It is established that the obtained empirical distributions are very close to the theoretical distributions under consideration, i.e. it can be argued that the reduced models of BSC on these criteria are similar to the properties of random substitution from S_n.

At the same time, to evaluate the probability of forming output blocks γ_i of a certain period for an arbitrary fixed value of the initialization vector S another characteristic of random substitution is required, namely, the distribution of the number of cycles of a given length. In accordance with [1], this characteristic in random substitution is determined as follows.

We denote $\chi_{n,L}$ as the number of cycles of length L in an arbitrary equivalence arbitrary substitution of degree *n*. Obviously that

$$\xi_n = \chi_{n,L=1} + \chi_{n,L=2} + ... + \chi_{n,L=n}.$$

The probability distribution of a random event $\chi_{n,L} = k$ is defined as [1]:

$$P(\chi_{n,L} = k) = \frac{1}{L^k k!} \sum_{j=0}^{[n/L]-k} \frac{(-1)^j}{L^j j!},\ k = 0,1,...,[n/L]. \quad (7)$$

When $n \to \infty$ a random variable $\chi_{n,L}$ has a Poisson distribution with parameters $\lambda = 1/L$, i.e.

$$\lim_{n\to\infty} P(\chi_{n,L} = k) = \frac{1}{L^k k!} e^{-1/L},\ k = 0,1,.... \quad (8)$$

We use the formula for the exact distribution of probabilities of a random event $\chi_{n,L} = k$ in the form (7) [1]. The value $n!P(\chi_{n,L} = k)$ corresponds to the number of substitutions containing k cycles with the length L. We are interested in the number of such substitutions $s \in S_n$, which for an arbitrary fixed $y_i \in Y$ will necessarily have cycles $s_i = (y_i, s_i(y_i), s_i^2(y_i), ..., s_i^{l_i-1}(y_i))$ of lengths $L = l_i$. Consider the case when $L = 1$, i.e. we will count the number of such substitutions from S_n which, for an arbitrary fixed $y_i \in Y$ will necessarily have a cycle (y_i) of length $L = l_i = 1$. In cryptography, when considering block symmetric cryptographic transformations, such cases are called fixed points of substitution [5]. Taking into account that $L = 1$, formula (7) takes the form

$$P(\chi_{n,L=1} = k) = \frac{1}{k!} \sum_{j=0}^{n-k} \frac{(-1)^j}{j!},\ k = 0,1,...,n,$$

and for each $k = 1,...,n$ of $n!P(\chi_{n,L=1} = k)$ cases for an arbitrary fixed $y_i \in Y$ will be observed precisely

$$\frac{C_{n-1}^{k-1}}{C_n^k} = \frac{(n-1)!}{(k-1)!(n-k)!} \frac{k!(n-k)!}{n!} = \frac{k}{n} \quad (9)$$

times, i.e. the number of substitutions containing one fixed point of a specific form (cycle (y_i)) will be determined by the formula:

$$\sum_{k=1}^{n} n!P(\chi_{n,L=1} = k) \frac{C_{n-1}^{k-1}}{C_n^k} = \sum_{k=1}^{n} \left(\frac{(n-1)!}{(k-1)!} \sum_{j=0}^{n-k} \frac{(-1)^j}{j!} \right) = (n-1)!, \quad (10)$$

and the corresponding probability of the appearance of such fixed point (for given initial value $y_i \in Y$) in the randomly chosen substitution of the degree n will look like:

$$\sum_{k=1}^{n} P(\chi_{n,L=1} = k) \frac{C_{n-1}^{k-1}}{C_n^k} = \frac{(n-1)!}{n!} = \frac{1}{n}. \quad (11)$$

Let's explain the formula (9). In total, there are exactly C_n^k methods for simultaneously choosing values $y_i, y_{i_1}, y_{i_2}, ..., y_{i_{k-1}} \in Y$, $y_i \neq y_{i_1} \neq y_{i_2} \neq ... \neq y_{i_{k-1}}$ which uniquely determine cycles $(y_i)(y_{i_1})(y_{i_2})...(y_{i_{k-1}})$ of length $L=1$. But for each fixed $y_i \in Y$ there are exactly C_{n-1}^{k-1} ways for choosing the remaining values $y_{i_1}, y_{i_2}, ..., y_{i_{k-1}} \in Y$. I.e. from the total number $n!P(\chi_{n,L=1}=k)$ of substitutions containing *k* cycles of length $L=1$, only

$$n!P(\chi_{n,L=1}=k)\frac{C_{n-1}^{k-1}}{C_n^k} = n!P(\chi_{n,L=1}=k)\frac{k}{n}$$

substitutions will necessarily contain a cycle (y_i).

The last formula (11) can be obtained much simpler from trivial combinatorial considerations. Indeed, if on the set $Y=\{y_1, y_2, ..., y_n\}$ we will fix m elements, then there are $(n-m)!$ ways for permutations of the remaining elements. I.e. on the all set of substitutions from S_n with the random probability distribution, the probability of choosing a substitution with m fixed points is equal to

$$\frac{(n-m)!}{n!} = \frac{1}{(n-m+1)(n-m+2)...n} = \frac{1}{(n)_m}, \quad (12)$$

Which for $m=1$ coincides with (11).

Formulas (9-12) were obtained in [9] when studying Galois / Counter Mode and GMAC - GCM & GMAC, which allowed us to estimate the probability of a zero hash subkey, i.e. the probability of such event, when encryption of zero open text will get zero value of ciphertext. We extend the result obtained earlier to an arbitrary value of the length of cycle $L=l_i \in \{1,2,...,n\}$ in the study of periodic properties of the output blocks in OFB mode.

Consider the case of an arbitrary length of a cycle, we will calculate the number of such substitutions *s* from S_n which, for an arbitrary fixed $y_i \in Y$ will necessarily have a cycle

$$(y_i, s_i(y_i), s_i^2(y_i), ..., s_i^{L-1}(y_i))$$

of length $L=l_i \in \{1,2,...,n\}$.

For fixed lengths and quantities of cycles (L and k) there are exactly C_n^{kL} ways to simultaneously select values

$$\begin{gathered} y_i, y_{j_i}, y_{u_i}, ..., y_{v_i}, \\ y_{i_1}, y_{j_1}, y_{u_1}, ..., y_{v_1}, \\ y_{i_2}, y_{j_2}, y_{u_2}, ..., y_{v_2}, \\ ..., \\ y_{i_{k-1}}, y_{j_{k-1}}, y_{u_{k-1}}, ..., y_{v_{k-1}}, \end{gathered} \quad (13)$$

which collectively determine k cycles of length L each:

$$\begin{gathered} (y_i, y_j = s_i(y_i), y_u = s_i^2(y_i), ..., y_v = s_i^{L-1}(y_i)), \\ (y_{i_1}, y_{j_1} = s_{i_1}(y_{i_1}), y_{u_1} = s_{i_1}^2(y_{i_1}), ..., y_{v_1} = s_{i_1}^{L-1}(y_{i_1})), \\ (y_{i_2}, y_{j_2} = s_{i_2}(y_{i_2}), y_{u_2} = s_{i_2}^2(y_{i_2}), ..., y_{v_2} = s_{i_2}^{L-1}(y_{i_2})), \\ ..., \\ (y_{i_{k-1}}, y_{j_{k-1}} = s_{i_{k-1}}(y_{i_{k-1}}), y_{u_{k-1}} = s_{i_{k-1}}^2(y_{i_{k-1}}), ..., y_{v_{k-1}} = s_{i_{k-1}}^{L-1}(y_{i_{k-1}})), \end{gathered} \quad (14)$$

and all elements from (13) are unique, since the set of cycles (14) is included in the decomposition of the same substitution.

Of the C_n^{kL} ways of simultaneously choosing the values (13) for each fixed set $y_i, y_{j_i}, y_{u_i}, ..., y_{v_i} \in Y$ there are exactly C_{n-1}^{kL-1} ways for choosing the remaining values

$$y_{i_1}, y_{j_1}, y_{u_1}, ..., y_{v_1},$$
$$y_{i_2}, y_{j_2}, y_{u_2}, ..., y_{v_2},$$
$$...,$$
$$y_{i_{k-1}}, y_{j_{k-1}}, y_{u_{k-1}}, ..., y_{v_{k-1}},$$

because the selection of set $y_i, y_{j_i}, y_{u_i}, ..., y_{v_i} \in Y$ is determined by selecting only one element $y_i \in Y$, and from the remaining $n-1$ elements possible different combinations of $kL-1$ elements.

Thus, for each $k = 0,1,...,\lfloor n/L \rfloor$ of the total number $n!P(\chi_{n,l} = k)$ of substitutions containing k cycles of length L, only

$$n!P(\chi_{n,L} = k)\frac{C_{n-1}^{kL-1}}{C_n^{kL}} = n!P(\chi_{n,L} = k)\frac{(n-1)!kL!(n-kL)!}{n!(kL-1)!(n-kL)!} = n!P(\chi_{n,L} = k)\frac{kL}{n} = (n-1)!kLP(\chi_{n,L} = k)$$

substitutions will necessarily contain a cycle

$$(y_i, s_i(y_i), s_i^2(y_i), ..., s_i^{L-1}(y_i)).$$

Summing up the last expression for all $k = 0,1,...,\lfloor n/L \rfloor$, taking into account (7), we obtain an exact formula for determining the number of substitutions s from S_n which, for an arbitrary fixed $y_i \in Y$ will necessarily have a cycle

$$(y_i, s_i(y_i), s_i^2(y_i), ..., s_i^{L-1}(y_i))$$

of length $L = l_i \in \{1, 2, ..., n\}$:

$$\sum_{k=1}^{[n/L]} n!P(\chi_{n,L} = k)\frac{C_{n-1}^{kL-1}}{C_n^{kL}} = \sum_{k=1}^{[n/L]} \frac{(n-1)!}{(k-1)!L^{k-1}} \sum_{j=0}^{[n/L]-k} \frac{(-1)^j}{L^j j!} = (n-1)!, \qquad (15)$$

and the corresponding formula for calculating the probability of randomly choosing a substitution s from S_n with the following cycle:

$$\sum_{k=1}^{[n/L]} P(\chi_{n,L} = k)\frac{C_{n-1}^{kL-1}}{C_n^{kL}} = \frac{(n-1)!}{n!} = \frac{1}{n}. \qquad (16)$$

It is obvious that the last analytic expression for $L = 1$ completely coincides with the formula (8) in [9] with the corresponding statement.

The resulting analytic expression (16) can also be considered as a combinatorial identity (simplified formula) for the sum of the members of formula (7) with the corresponding proportional coefficients

$$\frac{C_{n-1}^{kL-1}}{C_n^{kL}} = \frac{kL}{n},$$

or even for the Poisson distribution (8). The probability estimate (16) of a cycle of a certain length can be obtained by another, in a much simpler way, using simple combinatorial considerations.

We fix some arbitrary value y_i from the set $Y = \{y_1, y_2, ..., y_n\}$. There are totally $n!$ substitutions on the set Y, of which only

$$\frac{n!}{n} = (n-1)!$$

substitutions will contain a cycle (y_i) of length $L = 1$ in their cyclic schedule.

In addition, from $n!$ substitutions of the symmetric group

$$\frac{n!}{n(n-1)}(n-1) = (n-1)!$$

substitutions will contain a cycle $(y_i, y_{j\neq i})$ of length $L=2$,

$$\frac{n!}{n(n-1)(n-2)}(n-1)(n-2)=(n-1)!$$

substitutions will contain a cycle $(y_i, y_{j\neq i}, y_{u\neq i,j})$ of length $L=3$ and so on.

That is, for an arbitrary fixed value $y_i \in Y$ the number of substitutions from S_n containing the cycle $(y_i, s_i(y_i), s_i^2(y_i), ..., s_i^{L-1}(y_i))$ is defined as $(n-1)!$, and the corresponding probability of randomly choosing a substitution containing such a cycle is defined as

$$\frac{(n-1)!}{n!}=\frac{1}{n},$$

regardless of the length of the cycle $L=l_i \in \{1,2,...,n\}$, nor its own value y_i from $Y=\{y_1, y_2, ..., y_n\}$.

Thus, the probability of a cycle of a certain length is determined only by the degree n of substitution. For example, for $n=4$ from $n!=24$ substitutions of the symmetric group for any fixed y_i from $Y=\{y_1, y_2, y_3, y_4\}$ we have $(n-1)!=6$ substitutions each that necessarily contain cycles of different lengths (or (y_i), or $(y_i, y_{j\neq i})$, or $(y_i, y_{j\neq i}, y_{u\neq i,j})$, or $(y_i, y_{j\neq i}, y_{u\neq i,j}, y_{v\neq i,j,u})$, respectively). Consequently, the probability that a randomly selected substitution from S_4 contained cycle of length $L=l_i \in \{1,2,...,4\}$ will be equal to $1/n=1/4$ independent from either y_i no $L=l_i$.

Since the obtained analytical expressions (15) and (16) are rather complicated and cumbersome, especially the order of their output, we illustrate the example of calculating the probabilities of a cycle of given length in a randomly chosen substitution from a symmetric group S_4. An example will be supplemented by explanations showing the validity of the formulas obtained and the combinatorial arguments presented.

5 Example For Symmetric Group S_4

Consider an example of all biective transformations of the set $Y=\{y_1, y_2, y_3, y_4\}$ to itself, i.e. the set with $n!=24$ substitutions of degree *n = 4*.

Table 1 shows all substitutions that make up the symmetric group S_4 (the results of each substitution are given, the order of each substitution for cycles, total number of cycles and the distribution of the number of cycles of a certain length, each substitution is numbered for convenience).

Table 2 shows the distribution of the number of values $\xi_n = k$ and $\chi_{n,L} = k$ for different k (the symbol # (x) indicates the number of cases *(x)* for all substitutions from S_4).

Consider the case when for an arbitrary fixed $y_i \in Y$ randomly chosen substitution *s* from S_4 will necessarily contain a cycle (y_i) of length $L=1$.

First we consider substitutions with *k = 1* cycles of length $L=1$. We have 8 such substitutions (table 2). But each individual $y_i \in Y$ generates a cycle of length $L=1$ only twice, that is, for each arbitrary fixed $y_i \in Y$ there are precisely 2 substitutions that contain a cycle of length $L=1$ of the form (y_i). For example, for $y_1 \in Y$ these are 4th and 5th substitutions, for $y_2 \in Y$ these are the 16th and 21st substitutions, etc. The number of substitutions, which for an arbitrary fixed $y_i \in Y$ containing k = 1 cycle of length $L=1$ of form (y_i) are calculated as follows. In total, there are exactly $C_{n=4}^{kL=1}=4$ ways to select a value $y_i \in Y$. This choice is no longer limited, because for each $y_i \in Y$ cycle (y_i) is defined unambiguously (according to the formula there are $C_{n-1=3}^{kL-1=0}=1$ options for choosing a value $y_{j\neq i} \in Y$). That is, the total number of substitutions containing only k = 1 cycle of

length $L=1$ (such 8 substitutions) must be multiplied by value $\frac{C_{n-1=3}^{kL-1=0}}{C_{n=4}^{kL=1}}=\frac{1}{4}$. Thus, for an arbitrary fixed $y_i \in Y$ the number of substitutions containing only one cycle (y_i) is equal to two.

Table 1 – The set of substitutions from S_4 and their cyclic properties

№	Result of substitution				Decomposition of substitution to cycles	Number of cycles, ξn	Number of cycles of length L, χn, L			
	$s(y_1)$	$s(y_2)$	$s(y_3)$	$s(y_4)$			L=1	L=2	L=3	L=4
1	y_1	y_2	y_3	y_4	$(y_1)(y_2)(y_3)(y_4)$	4	4	0	0	0
2	y_1	y_2	y_4	y_3	$(y_1)(y_2)(y_3, y_4)$	3	2	1	0	0
3	y_1	y_3	y_2	y_4	$(y_1)(y_2,y_3)(y_4)$	3	2	1	0	0
4	y_1	y_3	y_4	y_2	$(y_1)\ (y_2, y_3, y_4)$	2	1	0	1	0
5	y_1	y_4	y_2	y_3	$(y_1)\ (y_2, y_4, y_3)$	2	1	0	1	0
6	y_1	y_4	y_3	y_2	$(y_1)\ (y_2, y_4)\ (y_3)$	3	2	1	0	0
7	y_2	y_1	y_3	y_4	$(y_1, y_2)\ (y_3)\ (y_4)$	3	2	1	0	0
8	y_2	y_1	y_4	y_3	$(y_1, y_2)\ (y_3, y_4)$	2	0	2	0	0
9	y_2	y_3	y_1	y_4	$(y_1, y_2, y_3)\ (y_4)$	2	1	0	1	0
10	y_2	y_3	y_4	y_1	(y_1, y_2, y_3, y_4)	1	0	0	0	1
11	y_2	y_4	y_1	y_3	(y_1, y_2, y_4, y_3)	1	0	0	0	1
12	y_2	y_4	y_3	y_1	$(y_1, y_2, y_4)\ (y_3)$	2	1	0	1	0
13	y_3	y_1	y_2	y_4	$(y_1, y_3, y_2)\ (y_4)$	2	1	0	1	0
14	y_3	y_1	y_4	y_2	(y_1, y_3, y_4, y_2)	1	0	0	0	1
15	y_3	y_2	y_1	y_4	$(y_1, y_3)\ (y_2)\ (y_4)$	3	2	1	0	0
16	y_3	y_2	y_4	y_1	$(y_1, y_3, y_4)\ (y_2)$	2	1	0	1	0
17	y_3	y_4	y_1	y_2	$(y_1, y_3)\ (y_2, y_4)$	2	0	2	0	0
18	y_3	y_4	y_2	y_1	(y_1, y_3, y_2, y_4)	1	0	0	0	1
19	y_4	y_1	y_2	y_3	(y_1, y_4, y_3, y_2)	1	0	0	0	1
20	y_4	y_1	y_3	y_2	$(y_1, y_4, y_2)\ (y_3)$	2	1	0	1	0
21	y_4	y_2	y_1	y_3	$(y_1, y_4, y_3)\ (y_2)$	2	1	0	1	0
22	y_4	y_2	y_3	y_1	$(y_1, y_4)\ (y_2)\ (y_3)$	3	2	1	0	0
23	y_4	y_3	y_1	y_2	(y_1, y_4, y_2, y_3)	1	0	0	0	1
24	y_4	y_3	y_2	y_1	$(y_1, y_4)\ (y_2, y_3)$	2	0	2	0	0

Table 2 – Distributions of quantities of values $\xi_n = k$ and $\chi_{n,L} = k$ for all substitutions from S_4

k	0	1	2	3	4
$\#(\xi_n = k)$	0	6	11	6	1
$\#(\chi_{n,L=1} = k)$	9	8	6	0	1
$\#(\chi_{n,L=2} = k)$	15	6	3	0	0
$\#(\chi_{n,L=3} = k)$	16	8	0	0	0
$\#(\chi_{n,L=4} = k)$	18	6	0	0	0

Estimation of the Probability of the Cycle (y_i)

Consider now the substitutions containing k = 2 cycles of length $L=1$. We have 6 substitutions (table 4), of which three substitutions in a cyclic decomposition contain cycles $(y_1)\ (y_{i\neq 1})$, three substitutions contain cycles $(y_2)\ (y_{i\neq 2})$, three substitutions contain cycles $(y_3)\ (y_{i\neq 3})$ and three sub-

stitutions contain cycles (y_4) $(y_{i\neq 4})$. It is clear that one and the same substitution can be assumed to different ways, i.e. it can, in its cyclic decomposition, be treated to substitutions containing cycles (y_i) $(y_{j\neq i})$ and substitutions containing cycles (y_j) $(y_{i\neq j})$. For example, the sixth substitution has a cyclic decomposition (y_1) (y_2, y_4) (y_3), it should be considered as a substitution with cycles (y_1) $(y_{j\neq 1})$ and with substitutions with cycles (y_3) $(y_{i\neq 3})$.

Table 3 – Substitutions containing 1 cycle of length 1 and one cycle of length 3

№	Result of substitution				Decomposition of substitution to cycles
	$s(y_1)$	$s(y_2)$	$s(y_3)$	$s(y_4)$	
4	y_1	y_3	y_4	y_2	(y_1) (y_2, y_3, y_4)
5	y_1	y_4	y_2	y_3	(y_1) (y_2, y_4, y_3)
9	y_2	y_3	y_1	y_4	(y_1, y_2, y_3) (y_4)
12	y_2	y_4	y_3	y_1	(y_1, y_2, y_4) (y_3)
13	y_3	y_1	y_2	y_4	(y_1, y_3, y_2) (y_4)
16	y_3	y_2	y_4	y_1	(y_1, y_3, y_4) (y_2)
20	y_4	y_1	y_3	y_2	(y_1, y_4, y_2) (y_3)
21	y_4	y_2	y_1	y_3	(y_1, y_4, y_3) (y_2)

Table 4 – Substitutions containing 2 cycle of length 1 and one cycle of length 2

№	Result of substitution				Decomposition of substitution to cycles
	$s(y_1)$	$s(y_2)$	$s(y_3)$	$s(y_4)$	
2	y_1	y_2	y_4	y_3	(y_1) (y_2) (y_3, y_4)
3	y_1	y_3	y_2	y_4	(y_1) (y_2, y_3) (y_4)
6	y_1	y_4	y_3	y_2	(y_1) (y_2, y_4) (y_3)
7	y_2	y_1	y_3	y_4	(y_1, y_2) (y_3) (y_4)
15	y_3	y_2	y_1	y_4	(y_1, y_3) (y_2) (y_4)
22	y_4	y_2	y_3	y_1	(y_1, y_4) (y_2) (y_3)

The number of substitutions containing k = 2 cycles (y_i) $(y_{j\neq i})$ of length $L=1$ for fixed $y_i \in Y$ are calculated as follows. In total, there are exactly $C_{n=4}^{kL=2} = 6$ ways to simultaneously select values $y_i, y_{j\neq i} \in Y$. But for fixed $y_i \in Y$ there are exactly $C_{n-1=3}^{kL-1=1} = 3$ ways for choosing a value $y_{j\neq i} \in Y$. That is, the total number of substitutions containing k = 2 cycles of length $L=1$ must be multiplied by the value $\frac{C_{n-1=3}^{kL-1=1}}{C_{n=4}^{kL=2}} = \frac{3}{6}$, we obtain the desired value, for an arbitrary fixed $y_i \in Y$ the number of substitutions containing k = 2 cycles (y_i) $(y_{j\neq i})$ of length $L=1$, is equal to three. For example, for fixed value $y_1 \in Y$ the second, third, and sixth substitutions contain k = 2 cycles of length $L=1$ with cyclic decompositions: (y_1) (y_2) (y_3, y_4), (y_1) (y_2, y_3) (y_4) та (y_1) (y_2, y_4) (y_3).

Consider substitutions containing k = 4 cycles of length $L=1$ (no substitution can have k = 3 cycles of length $L=1$). We have 1 substitution (Table 1), its cyclic decomposition has the form: (y_1) (y_2) (y_3) (y_4). Applying the same formula, we have $\frac{C_{n-1=3}^{kL-1=3}}{C_{n=4}^{kL=4}} = \frac{1}{1} = 1$, that is, the total number of

substitutions containing four cycles of length 1 coincides with the number of substitutions with cyclic decomposition (y_i) $(y_{j\neq i})$ $(y_{u\neq i,j})$ $(y_{v\neq i,j,u})$, as it should be.

We will calculate the number of substitutions from S_4 (Table 1), which for fixed $y_i \in Y$ necessarily contain a cycle (y_i) of length (y_i). To do this, we must summarize the number of substitutions that for fixed $y_i \in Y$ in their cyclic decomposition contain a different number of cycles of length $L=1$, namely, 2 substitutions with k = 1 cycle (y_i), three substitutions with k = 2 cycles (y_i) $(y_{j\neq i})$ and one substitution with k = 4 cycles (y_i) $(y_{j\neq i})$ $(y_{u\neq i,j})$ $(y_{v\neq i,j,u})$. In general, we have 6 substitutions from the total of 24 substitutions of the symmetric group. That is, at randomly equal probable selection of substitutions from S_4 the probability that in it for arbitrary fixed $y_i \in Y$ will be observed cycle (y_i) of length $L=1$ is equal to 6/24 = 1/4.

Estimation of probability of occurrence of a cycle $(y_i, y_{j\neq i})$

Consider the case when for arbitrary fixed $y_i \in Y$ randomly chosen substitution s from S_4 will necessarily contain a cycle $(y_i, y_{j\neq i})$ of length $L=2$.

First we consider substitutions containing k = 1 cycle of length $L=2$. We have 6 such substitutions, which are given in Table 4 (if the substitution from S_4 contains two cycles of length 1, then it necessarily contains one cycle of length 2). We will calculate the number of substitutions, which for an arbitrary fixed $y_i \in Y$ contain k = 1 cycle of length $L=2$ of form $(y_i, y_{j\neq i})$. In total, there are exactly $C_{n=4}^{kL=2}=6$ ways to simultaneously select values $y_i, y_{j\neq i} \in Y$. But for each $y_i \in Y$ there is exactly $C_{n-1=3}^{kL-1=1}=3$ ways to choose a value $y_{j\neq i} \in Y$. That is, the number of substitutions, which for an arbitrary fixed $y_i \in Y$ in a cyclic decomposition contain k = 2 cycles (y_i) $(y_{j\neq i})$ of length l=1, is equal to $6 \cdot \frac{C_{n-1=3}^{kL-1=1}}{C_{n=4}^{kL=2}}=3$. For example, for $y_1 \in Y$ the seventh, fifteenth and twenty second substitutions contain k=1 cycles of length l=2 each.

Let's also consider substitutions containing k = 2 cycles of length $L=2$. In total there are 3 such substitutions in S_n, this (see Table 1):

- the eighth substitution with a cyclic decomposition (y_1, y_2) (y_3, y_4);
- seventeenth substitution with cyclic decomposition (y_1, y_3) (y_2, y_4);
- last, twenty fourth substitution with cyclic decomposition (y_1, y_4) (y_2, y_3).

The number of substitutions, which for any fixed $y_i \in Y$ contains k = 2 cycles $(y_i, y_{j\neq i})$ and $(y_{u\neq i,j}, y_{v\neq i,j,u})$ of length $L=2$, is calculated in the same way. In total, there are exactly $C_{n=4}^{kL=4}=1$ ways to simultaneously select values $y_i, y_{j\neq i}, y_{u\neq i,j}, y_{v\neq i,j,u} \in Y$. This choice is no longer limited, because for selected $y_i, y_{j\neq i}, y_{u\neq i,j}, y_{v\neq i,j,u} \in Y$ corresponding k=2 cycles $(y_i, y_{j\neq i})$ та $(y_{u\neq i,j}, y_{v\neq i,j,u})$ are defined unambiguously (according to the formula there are $C_{n-1=3}^{kL-1=3}=1$ variants). That is, the number of substitutions, which for an arbitrary fixed value $y_i \in Y$ have cyclic decomposition $(y_i, y_{j\neq i})$ $(y_{u\neq i,j}, y_{v\neq i,j,u})$ coincides with the total number of substitutions with k = 2 cycles of length $L=2$, i.e. equal to 3. No substitution from S_4 can have k = 3 and k = 4 cycles of length $L=2$. We immediately proceed to calculate the probability of occurrence of the cycle $(y_i, y_{j\neq i})$ in randomly selected substitutions. We sum up the number of substitutions, which for an arbitrary fixed $y_i \in Y$ in their cyclic decomposition contain a different number of cycles of length

$L=2$, namely, we have 3 substitutions with k = 1 cycle $(y_i, y_{j\neq i})$, and three substitutions with k = 2 cycles $(y_i, y_{j\neq i})(y_{u\neq i,j}, y_{v\neq i,j,u})$. In general, we have 6 substitutions from the total of 24 substitutions of the symmetric group, that is, at randomly equal probable selection of substitutions from S_4 the probability that in it for arbitrary fixed $y_i \in Y$ will be observed cycle $(y_i, y_{j\neq i})$ of length $L=2$ is equal to 6/24=1/4.

Estimation of probability of occurrence of a cycle $(y_i, y_{j\neq i}, y_{u\neq i,j})$

Similar to the above, we will calculate the number of substitutions, which for arbitrary fixed $y_i \in Y$ have cycle $(y_i, y_{j\neq i}, y_{u\neq i,j})$. In an arbitrary substitution $s \in S_4$, there can be no more than one such cycle, i.e. cases with k>1 are impossible. Each cycle of length $L=3$ in the substitution decomposition is combined with a cycle of length 1, i.e. all eight of these substitutions are given in Table 3. We will calculate the number of substitutions which for arbitrary fixed $y_i \in Y$ necessarily contain a cycle $(y_i, y_{j\neq i}, y_{u\neq i,j})$. In total, there are exactly $C_{n=4}^{kL=3}=4$ ways to simultaneously select values $y_i, y_{j\neq i}, y_{u\neq i,j} \in Y$. But for each $y_i \in Y$ there are exactly $C_{n-1=3}^{kL-1=2}=3$ ways to choose of values $y_{j\neq i}, y_{u\neq i,j} \in Y$. That is, the number of substitutions, which for an arbitrary fixed value $y_i \in Y$ necessarily have a cycle $(y_i, y_{j\neq i}, y_{u\neq i,j})$, is defined as $8 \cdot \frac{C_{n-1=3}^{kL-1=2}}{C_{n=4}^{kL=3}} = 6$. For example, for $y_1 \in Y$ these are 6 substitutions (№ 9, 12, 13, 16, 20, 21) with cyclic decompositions (see Table 3): (y_1, y_2, y_3) (y_4), (y_1, y_2, y_4) (y_3), (y_1, y_3, y_2) (y_4), (y_1, y_3, y_4) (y_2), (y_1, y_4, y_2) (y_3) and (y_1, y_4, y_3) (y_2).

Consequently, at randomly equal probable selection of substitutions from S_4 the probability that in it for arbitrary fixed $y_i \in Y$ will be observed cycle $(y_i, y_{j\neq i}, y_{u\neq i,j})$ of length $L=3$ is equal to 6/24 = 1/4.

Estimation of Probability of Occurrence of a Cycle $(y_i, y_{j\neq i}, y_{u\neq i,j}, y_{v\neq i,j,u})$

In any substitution $s \in S_4$ there can be only one cycle of length $L=4$. Such substitutions are given in Table 5.

Table 5 – Substitutions containing 1 cycle of length 4

№	Result of substitution				Decomposition of substitution to cycles
	$s(y_1)$	$s(y_2)$	$s(y_3)$	$s(y_4)$	
10	y_2	y_3	y_4	y_1	(y_1, y_2, y_3, y_4)
11	y_2	y_4	y_1	y_3	(y_1, y_2, y_4, y_3)
14	y_3	y_1	y_4	y_2	(y_1, y_3, y_4, y_2)
18	y_3	y_4	y_2	y_1	(y_1, y_3, y_2, y_4)
19	y_4	y_1	y_2	y_3	(y_1, y_4, y_3, y_2)
23	y_4	y_3	y_1	y_2	(y_1, y_4, y_2, y_3)

Obviously, all such substitutions necessarily have in their single cycle all elements from set $Y=\{y_1, y_2, y_3, y_4\}$, i.e. for each $y_i \in Y$ in each substitution of Table 5 there will be a cycle $(y_i, y_{j\neq i}, y_{u\neq i,j}, y_{v\neq i,j,u})$. Check the above formula: $\frac{C_{n-1=3}^{kL-1=3}}{C_{n=4}^{kL=4}}=1$, indeed, all substitutions from Table 5 will necessarily contain a cycle $(y_i, y_{j\neq i}, y_{u\neq i,j}, y_{v\neq i,j,u})$ for each arbitrary fixed $y_i \in Y$. Consequently, the probability of a cycle $(y_i, y_{j\neq i}, y_{u\neq i,j}, y_{v\neq i,j,u})$ in a randomly selected substitution $s \in S_4$ is equal to 6/24 = 1/4.

6. Interpretation of the received results to the properties of BSC

The obtained analytic expressions (15) and (16) allow us to estimate the number of substitutions from the symmetric group, which for a certain element of the set of transformations necessarily contain a cycle of a certain length with this element, and the corresponding probability to randomly select substitution with such cycle.

We use these formulas to study periodic properties of OFB mode. In this case, we assume that the probabilistic properties of substitutions generated by the encryption function correspond to certain properties of random substitution, i.e. they correspond to our representations of such "ideal" BSC, which at any given encryption key randomly and equally compares any encrypt text to any open text. In this way, the l-bit BSC will implement a subset of the symmetric group of substitutions of degree 2^l, selecting a particular substitution s from S_{2^l} associated with the entered encryption key. On the all set of cipher keys we can choose substitution, which for an arbitrary fixed $y_i = S \in Y = \{y_1, y_2, ..., y_{2^l}\}$ necessarily has a cycle $(y_i, s_i(y_i), s_i^2(y_i), ..., s_i^{L-1}(y_i))$ of length $L = l_i \in \{1, 2, ..., n\}$. The probability of this event is determined by (16).

In practice this means that the probability of a cycle of any length in randomly chosen substitution from a symmetric group S_{2^l} for an arbitrary fixed element of a set does not depend on either this element or the length of the cycle. It depends only on the order $n = 2^l$ of the substitutions of the symmetric group S_n and is defined as the inverse value, that is equal to 1 / n. For any fixed value of the introduced initialization vector $y = S$, the probability that the corresponding output block $\gamma_i, i = 0,1,..,n-1$ formed in the OFB mode will have a period of length $L = l_i \in \{1, 2, ..., n\}$ does not depend on either the value of this initialization vector or the length of the period. It is determined only by the degree of substitution, that is, in this case, the digit of the cipher and it is equal to 2^{-l}.

Determine the probability that the period of formed output blocks will be not less than 2^m blocks, i.e. the probability of such an event, when for fixed value of the initialization vector $y_i = S$ the corresponding output blocks will not be repeated during 2^m iterations by the formulas (1) and (3) when forming the output blocks γ_i:

$$P(\forall i, j \in \{1, 2, ..., 2^m\} : \gamma_i \neq \gamma_j \big|_{i \neq j}) = 1 - \sum_{L=1}^{2^m} \sum_{k=1}^{[2^l/L]} P(\chi_{2^l, L} = k) \frac{C_{2^l-1}^{kL-1}}{C_{2^l}^{kL}} = \sum_{L=2^m+1}^{2^l} \sum_{k=1}^{[2^l/L]} P(\chi_{2^l, L} = k) \frac{C_{2^l-1}^{kL-1}}{C_{2^l}^{kL}}. \quad (17)$$

Taking into account (16) we obtain:

$$P(\forall i, j \in \{1, 2, ..., 2^m\} : \gamma_i \neq \gamma_j \big|_{i \neq j}) = 1 - \sum_{L=1}^{2^m} 2^{-l} = \sum_{L=2^m+1}^{2^l} 2^{-l} = 1 - 2^{m-l}. \quad (18)$$

Thus, when the assumption about the correspondence of certain probabilistic properties of the cipher to the properties of a random substitution is correct, the probability of non-repetition of output block at a certain length is a function of this length. This fact determines the main limitation of the use of the OFB mode, it is directly derived from the results of the research. The main limitation on the use of the OFB mode for BSC "Kalyna" [10,11] is specified in Appendix G.2 "Limit on the total length of messages protected by the use of one key" namely:

- when the block size is equal to 128 bits, it is recommended to limit the number of blocks protected by the single key to value 2^{60} (16 million TB);
- when the block size is equal to 256 bits, it is recommended to limit the number of blocks protected by the single key to value 2^{124};
- when the block size is equal to 512 bits, it is recommended to limit the number of blocks protected by the single key to value 2^{251}.

Since, as shown in Section 2, the essence of protecting an informational message according to

the OFB mode specification is in addition of output blocks to it, then the restrictions specified in appendix G.2 relate to the restrictions on the length of output blocks, which are formed by multiple encryption of the same non-secret initialization vector by the formulas (1), (3). That is, the implementation of the restrictions recommended by the specification of the national standard provides certain probabilistic indicators of non-periodic output blocks, namely:

- when the block size is l = 128 bits, and when performing the recommended limitation of the number of blocks protected by a single key with the size $2^m = 2^{60}$, the probability of non-repetition of the output blocks $1-2^{m-l} = 1-2^{-68} > 1-2^{-64}$ will be ensured;
- when the block size is l = 256 bits, and when performing the recommended limitation of the number of blocks protected by a single key with the size $2^m = 2^{124}$, the probability of non-repetition of the output blocks $1-2^{m-l} = 1-2^{-132} > 1-2^{-128}$ will be ensured;
- when the block size is l = 512 bits, and when performing the recommended limitation of the number of blocks protected by a single key with the size $2^m = 2^{251}$, the probability of non-repetition of the output blocks $1-2^{m-l} = 1-2^{-261} > 1-2^{-256}$ will be ensured.

More often, in the theory of information security, the inverse value is used, it is the probability that a formed output blocks with a length that does not exceed a certain limit will have at least one repetition. Taking into account (17) and (18), this probability will be determined as:

$$P_{l,m} = 1-P(\forall i, j \in \{1,2,...,2^m\} : \gamma_i \neq \gamma_j \big|_{i \neq j}) = \sum_{L=1}^{2^m} \sum_{k=1}^{[2^l/L]} P(\chi_{2^l,L} = k) \frac{C_{2^l-1}^{kL-1}}{C_{2^l}^{kL}} = 2^{m-l}. \qquad (19)$$

Figure 2 shows the dependence $P_{l,m}$ and m for different l ($\gamma_i, i = 0,1,..,n-1$ *with the length not more than* $2^m = 2^{60}$ *blocks*).

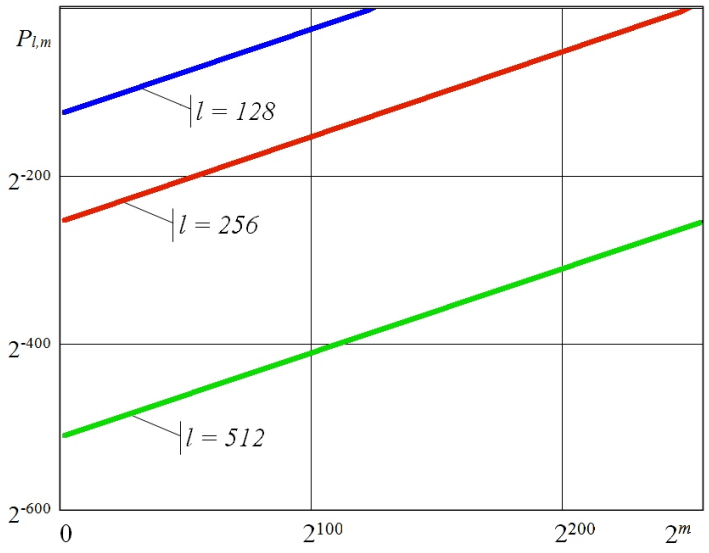

Fig. 2 – The dependence of the probability that there will be at least one repetition in output blocks

From the dependencies shown in Fig. 2, it is evident that increasing the length of the output blocks leads to an increase in the probability of any number of repetitions of the output blocks. These graphs can be used to justify certain restrictions, for example, if you want to reduce the probability of any number of repetitions of the output blocks, you must reduce its length.

7. Conclusions

Based on the obtained results, we can do conclusions that are important in practical terms.

1. Properties of modern symmetric cryptotransformations depend not only on the characteristics of BSC, but also on the mode of application. Therefore the National Standard "Information technology. Cryptographic protection of information. The algorithm of symmetric block transformation" provides 10 modes of cryptotransformations: simple substitution (Electronic Codebook - basic transformation), Counter, Cipher Feedback, Symmetric Key Block Cipher-Based Message Authentication Code, Cipher Block Chaining, Output Feedback, Galois/Counter Mode and Galois Message Authentication Code, Counter with Cipher Block Chaining-Message Authentication Code, XOR Encrypt XOR (XEX) Tweakable Block Cipher, Key Wrapping.

2. In OFB mode, which is used to provide a privacy service, the output message is protected by

addition of output blocks, which are formed by multiple encryption of the same non-secret initialization vector. If we assume that the properties of the cipher correspond to certain properties of random substitution, then the periodicity of the output blocks will be determined by the presence of cycles in randomly selected substitutions from the symmetric group, and the selection of the substitution is set to the value of the secret key.

3. Investigation of the properties of randomly selected substitution s from the symmetric group S_n has shown that the probability of cycle $s_i = (y_i, s_i(y_i), s_i^2(y_i), ..., s_i^{l_i-1}(y_i))$ of any length $L = l_i$ for an arbitrary fixed element y_i from the set $Y = \{y_1, y_2, ..., y_n\}$ does not depend on either this element y_i or the length $L = l_i$ of the cycle. This probability depends only on the order *n* of the substitutions of the symmetric group S_n and is defined as an inverse value, that is equal to 1 / n.

4. Thus, the periodic properties of the output blocks in OFB mode are determined by the distribution of the probabilities of the number of cycles of random substitution. The selection of a secret key that parameterizes the encryption function corresponds to the selection of a particular substitution from the symmetric group; selecting the initialization vector value corresponds to the selection of an element y_i from the set of elements $Y = \{y_1, y_2, ..., y_n\}$ over which substitution occurs. But neither the actual value of the initialization vector nor the length of the output blocks period has any effect on the probability of obtaining an output blocks of a certain period. This probability is determined only by the degree $n = 2^l$ of substitution, that is, by the size l of the basic cipher transformation.

5. From the point of view of the practical application of symmetric cryptographic transformations to output blocks, the requirements of homogeneity are proposed at a length not exceeding the established limit. The probability of such event is determined by $1-2^{m-l}$ where 2^m is the length restriction of the output blocks. For example, for a 128-bit cipher "Kalyna", when we have limiting the length of a output blocks to 2^m in the OFB mode, the probability that the gamma blocks never coincide equals to $1-2^{m-l} = 1-2^{-68}$, i.e. it is much more than $1-2^{-64}$. The probability that at length no more 2^m blocks of output blocks in the OFB mode will coincide at least once, will equal $P_{l,m} = 2^{m-l}$. This dependence can be used to substantiate the restrictions on the length of the output blocks when the upper limit of probability $P_{l,m}$ is set.

6. The specification of BSC "Kalyna" [10,11] recommended certain restrictions on the total length of messages protected by the use of one key. As for OFB mode such restrictions should be considered as requirements for the maximum length of output blocks, which with a certain probability will not be repeated. The above recommendations are fundamental because the occurrence of output blocks repetition is the most dangerous case when using the OFB mode, since in this case, the attacker will almost certainly violate the established privacy mode of the messages. For example, if the probability of a repetition of the output blocks is equal to 2^{-64}, then the length of output blocks for 128-bits BSC "Kalyna" should not exceed 2^{64} blocks (in the standard this restriction is more stringent and equal to 2^{60}).

7. The estimations of the probability of forming the output blocks with given period can be considered as a criterion for selection of cryptographic primitives, or criterion of the statistical test. Indeed, if the studied cryptographic primitive in OFB mode with equal probability forms output blocks with any period and this probability is determined by inverse to the degree of substitution, then by the cyclical properties this cryptographic primitive responsible to probabilistic properties of random substitution and by this criterion can be adopted for use. Actually such studies, particularly on nonlinear replacement nodes or reduced BSC models are promising direction for further work.

References

[1] Sachkov V.N. Introduction to combinatorial methods of discrete mathematics/ V.N. Sachkov. – Moskow: Nauka; Ed. Ph.-math. Lit., 1982. – 384 p.
[2] Tronin S.N. Introduction to the theory of groups/ S.N. Tronin. – Kazan: Kazan State University, 2006. – 100 p.
[3] Alexandrov P.S. Introduction to the theory of groups/ P.S. Alexandrov. – Moskow: Nauka, 1980. – 145 p.

[4] Menezes Alfred J. Handbook of Applied Cryptography/ Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. – CRC Press, 1997. – 794 p.
[5] Dolgov V.I. Analysis of cyclic properties of block ciphers/ V.I. Dolgov, I.V. Lisitskaya, V.I. Ruzhentsev// Applied radio electronics . – 2007. – Vol.6. – №2. – P. 257–263.
[6] Kuznetsov A.A. Linear properties of block symmetric ciphers presented to the Ukrainian competition / A.A. Kuznetsov, I.V. Lisitskaya, S.A. Isaev //Applied radio electronics. – 2001. – Vol. 10. – № 2. – P.135–140.
[7] Soroka L.S. Investigation of the differential properties of block-symmetric ciphers/ L.S. Soroka, A.A. Kuznetsov, I.V. Moskovchenko, S.A. Isaev // Information Processing Systems. – 2010. – Vol. 6 (87). – P. 286–294.
[8] Dolgov V.I. Block symmetric ciphers are random substitutions. Combinatorial indices/ V.I. Dolgov, M.Yu. Rodinko //Applied radio electronics. – 2013. – Vol.12. – № 2. – P. 236–239.
[9] Kuznetsov O.O. Analysis of collision properties of Galois Message Authentication Code with selective Counter/ O.O. Kuznetsov, D.V. Ivanenko, Ie.P. Kolovanova // Bulletin of V. Karazin Kharkiv National University. Series "Mathematical Modelling. Information Technology. Automated Control Systems". – 2014. – № 1097. – Issue 23. – P. 55–71.
[10] Information Technology. Cryptographic protection of information. Symmetric block algorithm transformation: DSTU. – Kyiv: Ministry of Economic Development of Ukraine, 2015. – 238 p.
[11] Gorbenko I.D. Development of a new symmetric block cipher: Report on the first phase of research "Algorithm" (intermediate) / I.D. Gorbenko :in 4 t. – T. 4. – Kharkiv: JSC «IIT», 2014. – 304 p.

Рецензент: Сергей Толюпа, д.т.н., проф., Киевский национальный университет имени Т. Шевченко, Киев, Украина.
E-mail: tolupa@i.ua

Поступила: Май 2017.

Авторы:
Александр Кузнецов, д.т.н., проф., академик Академии наук прикладной радиоэлектроники, ХНУ имени В.Н. Каразина, Харьков, Украина.
E-mail: kuznetsov@karazin.ua

Евгения Колованова, к.т.н., ст. преподаватель, ХНУ имени В.Н. Каразина, Харьков, Украина.
E-mail: e.kolovanova@gmail.com

Татьяна Кузнецова, научный сотрудник каф. безопасности информационных систем и технологий (БИСТ), ХНУ имени В.Н. Каразина, Харьков, Украина.
E-mail: kuznetsova.tatiana17@gmail.com

Периодические свойства шифргаммы в режиме Output Feedback.

Аннотация: Исследуются свойства режима гаммирования с обратной связью по шифргамме (анг. – Output Feedback). С применением математического аппарата теории подстановок исследуются периодические свойства гаммы, в частности, проводится оценка вероятности появления гаммы определенного периода при условии соответствия свойств шифра определенным свойствам случайной подстановки. Разрабатываются практические рекомендации по применению режима гаммирования с обратной связью по шифргамме, обосновываются требования и ограничения, вытекающие из полученных оценок периодических свойств гаммы.

Ключевые слова: режим шифрования, периодичность гаммы, случайная подстановка, Output Feedback.

Рецензент: Сергій Толюпа, д.т.н., проф., Київський національний університет імені Т. Шевченка, Київ, Україна.
E-mail: tolupa@i.ua

Надійшло: Травень 2017.

Автори:
Олександр Кузнецов, д.т.н., проф., академік Академії наук прикладної радіоелектроніки, ХНУ імені В.Н. Каразіна, Харків, Україна.
E-mail: kuznetsov@karazin.ua

Євгенія Колованова, к.т.н., ст. викладач, ХНУ імені В.Н. Каразіна, Харків, Україна.
E-mail: e.kolovanova@gmail.com

Тетяна Кузнецова, науковий співробітник каф. безпеки інформаційних систем і технологій (БІСТ), ХНУ імені В.Н. Каразіна, Харків, Україна.
E-mail: kuznetsova.tatiana17@gmail.com

Періодичні властивості шифргами у режимі Output Feedback.

Анотація: Досліджуються властивості режиму гамування зі зворотнім зв'язком за шифргамою (анг. – Output Feedback). Із застосуванням математичного апарату теорії підстановок досліджуються періодичні властивості гами, зокрема проводиться оцінка ймовірності появи гами певного періоду за умови відповідності властивостей блокового симетричного шифру певним властивостям випадкової підстановки. Розробляються практичні рекомендації щодо застосування режиму гамування зі зворотнім зв'язком за шифргамою, обгрунтовуються вимоги та обмеження, що випливають із отриманих оцінок періодичних властивостей гами.

Ключові слова: режим шифрування, періодичність гами, випадкова підстановка, Output Feedback.

UDC 681.142.01

THE CONCEPT OF PROCESSING INTEGER DATA REPRESENTED IN THE SYSTEM OF RESIDUE CLASSES

Viktor Krasnobayev[1], Sergey Koshman[2], Artem Moskalenko[3]

[1] V. N. Karazin Kharkiv National University, Svobody sq.,4, Kharkiv, 61022, Ukraine
krasnobaev@karazin.ua
[2] Kharkiv Petro Vasylenko National Technical University of Agriculture, Rizdviana st., 19, Kharkiv, 61052, Ukraine
s_koshman@ukr.net
[3] Poltava Institute of Business Academician Yuri Bugay International Science and Technical University, Sinna st., 7
Poltava, 36039, Ukraine
moskalenko_artem@ukr.net

Reviewer: Vyacheslav Kharchenko, Doctor of Sciences (Eng), Full Prof., Academicians of the Academy of Applied Radioelectronics Sciences, N.Ye. Zhukovskiy National Aerospace University – Kharkiv Aviation Institute (KhAI), 17 Chkalov St., Kharkiv, 61070, Ukraine.
v_s_kharchenko@ukr.net

Received on May 2017

Abstract: *The coding of residues number witch submitted the appropriate modules of residual classes system (RCS), made with data from complete system of the smallest non-negative residues (CSSNR) was show in the article. In this aspect, CSSNR is the basis for the construction of non-positional code structure in RCS. Possible field of science and engineering, where there is an urgent need for fast, reliable, and high-precision integer calculations were clarified and systematized in the paper. On the basis of studies of the properties of RCS were examined the advantages and disadvantages of using modular arithmetic (MA). Using the results of the analysis of problems of integer data and a set of positive attributes of MA, the classes of problems and algorithms, which using RCS, much more efficient binary positional numeral systems were defined in the article.*

Keywords: *residual classes system, modular arithmetic, positional numeral systems, complete system of the smallest non-negative residues, computer system and a data processing means witch represented in integer form, residual classes.*

1 Introduction

At present time there is a number of fields and directions of science and technology, where a need in fast, reliable and highly precise integer arithmetic calculations exists. We can say, that in almost all fields of science the integer arithmetic calculations are used. First of all, they are such fields of science as mathematics, physics, astronomy, technical science, geodesy and meteorology, seismology etc. Let's note the following directions in science and technology, where there exists the necessity in fast, reliable and highly precise integer arithmetic calculations: arithmetic operations with integer numbers and polynomials; integer linear programming; operations with numbers and sets, the solution of the multidimensional NP-complete problems; implementation of routing algorithms *(algorithms for finding the shortest path)*; problems of ways and matrix multiplication; problems of fast Fourier transform and it's applications; the creation of artificial intelligence systems *(neural network data processing system)*; tasks for military purposes; digital signal processing, digital image processing; cryptographic transformation; highly-precise integer arithmetic; the solution of problems related to the space research; highly-precise digital-to-analog and analog-to-digital conversions and so forth.

The results of the researches conducted during last few decades in the field of information technologies by different groups of scientists and engineers of methods of productivity improvement, reliability, survivability, and reliability of computer systems calculations and data processing means presented as integers (CSIDPM), showed that within the positional numeral systems (PNS), it is practically impossible to achieve it [1-3]. First of all, it's caused by the main disadvantage of modern CSIDPM that operate in PNS: the presence of inter-bits links between the processed operands.

These links significantly impact the architecture of the calculator and methods of implementation of arithmetic operations, implemented by CSIDPM; complicate the apparatus and limit the speed of the arithmetic operations of addition, subtraction and multiplication. In this regard, improving above mentioned characteristics of CSIDPM in PNS, is carried out, first of all, by increasing the clock frequency, development and application of methods and means of parallel data processing as well as by using different types of redundancy. This circumstance led to the need of finding the ways of increasing the effectiveness of CSIDPM functioning, for example, through the use of new architectural solutions by applying non-positional machine arithmetic, in particular, on the basis of non-positional numeral systems use in residual classes (NSRC). The well-known Chinese remainder theorem (*the task of restoring the original number A_k by the aggregating of its remains (deductions)* $\{a_i\}$ *by dividing it into a series of natural numbers m_1, m_2, ..., m_n (modules) of NSRC*), which was previously interpreted as a structural theorem of abstract algebra, guaranteed the specified parallelism in the calculations over integers, under the conditions that the result of ring operations belongs to the range of integers, defined by models product of NSRC. The results of conducted researches of the implementation of arithmetic operations methods in NSRC led to the creation of new machine arithmetic. Having its ideological roots of the classical works of Euler, Gauss and Chebyshev on the theory of comparisons, NSRC introduced new ideas in the development of creation methods of highly-productive and ultra reliable CSIDPM [1,4,5].

2 The main part

For the first time the results of theoretical studies devoted to the possibility of practical application of NSRC as a numeral system (NS) of CSIDPM, were published in 1955-1957 in the scientific works of Czech scientists M. Valaha and A. Svoboda. Non-positional number system in NSRC is a NS where integers are presented as a set of non-negative deductions (residues) in the group of mutually pairwise prime numbers which are called bases or modules of NSRC. In this case there are no inter-bits relations between processed numbers residues, that gives opportunity to perform arithmetic operations excluding bit relations between numbers residues. The use of NSRC-based machine arithmetic allowed to create actually operating CSIDPM. In the 60s of the past century the team of scientists and engineers headed by the doctor of technical sciences, professor D.I. Yuditskii, created A-340A the world's first experimental computer and T-340A serial computers, functioning in NSRC. These computers were intended for regular polygon version of Dunay-3UP radar, which was the part of the USSR A-35 missile defense system. In the 70s of the past century for radar stations there were created such CSIDPM in NSRC as "Diamond" and 5E53 supercomputers.

However in the 80s of the past century due to a number of objective and subjective reasons the interest to modular arithmetic (MA) is significantly reduced. It was primarily due to the death of the Director of the Microelectronics Center, developing the general theory and practical creation of a computer in NSRC located in Zelenograd, Moscow Region, the Director and the chief initiator of project Lukin Fedor Victorovich and therefore, the complete termination of practical works, connected with the use of MA. But then this direction was restrained by the imperfection of the existing at that time element base of computers, as well as the existing methodology of computer systems and components designing, principally focused at that time only on the binary system calculation.

Now the interest to the use of NSRC is increasing again. Ultimately it is caused by:

- the emergence of the numerous scientific and theoretical publications devoted to the theory and practice of the computer systems and components creating in NSRC;
- wide distribution of mobile processors that require high speed data processing at low energy consumption; the lack of inter-bits transfers during arithmetic operations of addition and multiplication of numbers in NSRC allows to reduce energy consumption;
- strong interest to NSRC is being shown by the banking structures, where it is necessary in real time to handle large amount of data safely and reliably, i.e. they are required highly-productive means for highly reliable computing with errors self-correction, that is typical to the NSRC codes;
- the elements density increasing on a single chip doesn't always allow to perform a complete

and qualitative testing; in this case there is an increasing importance of providing failover operation of CSIDPM;

– the need for the use of the specialized CSIDPM to perform a large number of operations on vectors, which require high-speed performance of integer addition and multiplication operations *(matrix multiplication problems, the problems of the scalar product of vectors, Fourier transformation, etc.)*;

– the widespread introduction of microelectronics into all spheres of human activity significantly increased relevance and importance of previously rare, and now so massive scientific and practical problems, as a digital signal and image processing, image recognition, cryptography, multi-bit data processing and storage, etc.; this circumstance requires enormous computing resources being in excess of the existing possibilities;

– the current level of microelectronics development is coming to its limits from the point of view of productive provision and reliability of existing and future computer systems and components of large data sets processing in real time;

– taking it over nanoelectronics, molecular electronics, micromechanics, bioelectronics, optical, optoelectronic and photonic computers and others are still rather far from the real industrial production and employment.

– the modern development of integrated circuit technology allows to have a fresh look at the principles of devices construction with modular arithmetic employment and provides wide opportunities to use new design techniques *(such as the methodology of systems design on a chip-SOC)* both in the development of individual computing units, and computer systems in general; integral technology enables more flexible design of computer systems and components and allows us to implement NSRC-based devices as effectively as on the basis of the binary system; furthermore at present in order to improve the effectiveness of computer devices development, automated design systems (ADS) are widely used; in this respect, the design of computer systems and components based on NSRC does not differ from the working with the help of ADS data of binary data-blocks in PNS;

– unfortunately, Ukraine today in contrast to the theoretical development, technologically is behind the foreign microelectronics of some leading countries; in this case, it is advisable to use the existing theoretical achievements and practical experience in the creation of effective computer systems and components in NSRC.

In [1] it is given a definition of NSRC. In this case NSRC is considered a generalized version of NS, in which any natural number *A*, including zero, is represented as a set of the smallest positive residues *(deductions)* of the division of the original A number on preset m_1, m_2, … m_n natural numbers, called bases or NSRC modules. In literature it is often not entirely fair the term NSRC is identified with "residue class". In some cases, this circumstance can interfere the analysis of the results of solving the data processing problems presented in MA. In this regard it is important to consider the correlation between the notion of NSRC and RC. We'll give a definition to the notion "residue class". Let's consider the set {*A*} of all natural numbers, including zero. From the set of natural numbers we choose an arbitrary number *(module)* m_i. While dividing any natural number on m_i module we can get the following set of residues: 0 *(A number is divided into the m module integrally)*, 1, 2 … $m_i - 2$ and $m_i - 1$. All the set of natural numbers including zero, can be divided into m_i (0, 1, 2, ... m_i -2 and m_i -1) of different groups of numbers *(residue classes)*, including in each RC the numbers which, while dividing into the module m_i, give the same remainder. It is considered, that these numbers are comparable with each other on module m_i.

The residue class modulo m_i of NSRC can be denoted by the symbol $RC_j^{(i)}$, where i – the number of the base of orderly ($m_i < m_{i+1}$) NSRC ($i = \overline{1, n}$); j – the RC number in the system of residues for a given module m_i ($j = \overline{0, m_i - 1}$). In the general case, the residue class of $RC_j^{(i)}$ modulo m_i we will call the set of all integers, including zero, which while dividing into the modules m_i give the same positive balance. Taking into account the well-known correlation

$(-A) \bmod m_i = (m_i \cdot k - A) \bmod m_i (k = 1, 2, 3, ...)$, all RC on arbitrary module m_i of NSRC can be represented in the form of

$$\begin{aligned}
RC_0^{(i)} &= \overline{0} \ \{ ..., -2 \cdot m_i, \quad -m_i, \quad 0, \ m_i, \quad 2 \cdot m_i, \quad 3 \cdot m_i, \quad ... \}, \\
RC_1^{(i)} &= \overline{1} \ \{ ..., -(2 \cdot m_i - 1), -(m_i - 1), \ 1, \ m_i + 1, \ 2 \cdot m_i + 1, \ 3 \cdot m_i + 1, \ ... \}, \\
RC_2^{(i)} &= \overline{2} \ \{ ..., -(2 \cdot m_i - 2), -(m_i - 2), \ 2, \ m_i + 2, \ 2 \cdot m_i + 2, \ 3 \cdot m_i + 2, ... \}, \\
RC_3^{(i)} &= \overline{3} \ \{ ..., -(2 \cdot m_i - 3), -(m_i - 3), \ 3, \ m_i + 3, \ 2 \cdot m_i + 3, \ 3 \cdot m_i + 3, ... \}, \\
&\vdots \qquad\qquad\qquad\qquad\qquad\qquad \vdots \\
RC_j^{(i)} &= \overline{j} \ \{ ..., -(2 \cdot m_i - j), -(m_i - j), \ j, \ m_i + j, \ 2 \cdot m_i + j, 3 \cdot m_i + j, ... \}, \\
&\vdots \qquad\qquad\qquad\qquad\qquad\qquad \vdots \\
RC_{m_i-2}^{(i)} &= \overline{m_i - 2} \{ ..., \ -(m_i + 2), \ -2, \ m_i - 2, \ 2 \cdot m_i - 2, \ 3 \cdot m_i - 2, \ 4 \cdot m_i - 2, \ ... \}, \\
RC_{m_i-1}^{(i)} &= \overline{m_i - 1} \{ ..., \ -(m_i + 1), \ -1, \ m_i - 1, \ 2 \cdot m_i - 1, \ 3 \cdot m_i - 1, \ 4 \cdot m_i - 1, \ ... \}.
\end{aligned} \tag{1}$$

If one arbitrary residue is taken from each RC, then such set of m_i integers will be called a complete residue system (CRS) modulo m_i. Having taken one specific residue from each RC, draw up some possible options for CRS modulo m_i: 0, 1, 2, 3, …, $m_i - 1$ – is a complete system of the smallest non-negative residues (CSSNR); m_i, 1, 2, 3, …, $m_i - 1$ – is a complete system of the smallest positive residues (CSSPR); 0, 1, 2, -2, …, -1 – is a complete system of the smallest in absolute value residues (CSSAVR). As within each module they operate only with natural numbers, including zero, for the formation of NSRC with the $m_1, m_2, ..., m_n$ bases it is necessary to use n CSSNR from each set of RS. In this case all possible RC ($C^{(1)}$) for the first m_1, for the second ($C^{(2)}$) m_2 and the last ($C^{(n)}$)m_n of NSRC modules, have been represented respectively by the expressions (2), (3) and (4). For the first NSRC m_1 module we have the following set of RC

$$\begin{aligned}
RC_0^{(1)} &= \overline{0} \ \{ \ 0, \quad m_1, \quad 2 \cdot m_1, \quad 3 \cdot m_1, \quad ... \}, \\
RC_1^{(1)} &= \overline{1} \ \{ \ 1, \quad m_i + 1, \quad 2 \cdot m_1 + 1, \ 3 \cdot m_1 + 1, \ ... \}, \\
RC_2^{(1)} &= \overline{2} \ \{ \ 2, \quad m_1 + 2, \quad 2 \cdot m_1 + 2, \ 3 \cdot m_1 + 2, \ ... \}, \\
&\vdots \\
RC_{m_1-2}^{(1)} &= \overline{m_1 - 2} \{ \ m_1 - 2, \ \ 2 \cdot m_1 - 2, \ 3 \cdot m_1 - 2, \ 4 \cdot m_1 - 2, ... \}, \\
RC_{m_i-1}^{(1)} &= \overline{m_1 - 1} \{ \ m_1 - 1, \ \ 2 \cdot m_1 - 1, \ 3 \cdot m_1 - 1, \ 4 \cdot m_1 - 1, \ ... \}.
\end{aligned} \tag{2}$$

Obviously, for the module m_1 of NSRC the CSSNR will consist of residues:

$$0, 1, 2, ..., m_1 - 1.$$

For the second m_2 module of NSRC we have the following set of RC

$$\begin{aligned}
RC_0^{(2)} &= \overline{0} \ \{ \ 0, \quad m_2, \quad 2 \cdot m_2, \quad 3 \cdot m_2, \quad ... \}, \\
RC_1^{(2)} &= \overline{1} \ \{ \ 1, \quad m_2 + 1, \quad 2 \cdot m_2 + 1, \quad 3 \cdot m_2 + 1, \ ... \}, \\
RC_2^{(2)} &= \overline{2} \ \{ \ 2, \quad m_2 + 2, \quad 2 \cdot m_2 + 2, \quad 3 \cdot m_2 + 2, \ ... \}, \\
&\vdots \\
RC_{m_2-2}^{(2)} &= \overline{m_2 - 2} \ \{ \ m_2 - 2, \ 2 \cdot m_2 - 2, \quad 3 \cdot m_2 - 2, \quad 4 \cdot m_2 - 2, \ ... \}, \\
RC_{m_2-1}^{(2)} &= \overline{m_2 - 1} \ \{ \ m_2 - 1, \ 2 \cdot m_2 - 1, \quad 3 \cdot m_2 - 1, \quad 4 \cdot m_2 - 1, \ ... \}.
\end{aligned} \tag{3}$$

For the module m_2 of NSRC the CSSNR will consist of residues: $0, 1, 2, ..., m_2 - 1$.

For the last NSRC m_n module we have

$$\begin{aligned}
RC_0^{(n)} &= \overline{0} \quad \{\ 0, \quad m_n, \quad 2\cdot m_n, \quad 3\cdot m_n, \quad ...\ \},\\
RC_1^{(n)} &= \overline{1} \quad \{\ 1, \quad m_n+1, \quad 2\cdot m_n+1, \quad 3\cdot m_n+1, \quad ...\ \},\\
RC_2^{(n)} &= \overline{2} \quad \{\ 2, \quad m_n+2, \quad 2\cdot m_n+2, \quad 3\cdot m_n+2, \quad ...\ \},\\
&\qquad\qquad \vdots\\
RC_{m_n-2}^{(n)} &= \overline{m_n-2} \quad \{m_n-2, \quad 2\cdot m_n-2, \quad 3\cdot m_n-2, \quad 4\cdot m_n-2, \quad ...\ \},\\
RC_{m_n-1}^{(n)} &= \overline{m_n-1} \quad \{m_n-1, \quad 2\cdot m_n-1, \quad 3\cdot m_n-1, \quad 4\cdot m_n-1, \quad ...\ \}.
\end{aligned} \tag{4}$$

For the module m_n the CSSNR will consist of residues: $0, 1, 2, ..., m_n - 1$.

Thus, the NSRC is characterized by using of n, the number of bases of CSSNR.

Here is an example of CRS definition for the module $m_i = 5$ of NSRC. Residue classes modulo five can be represented in general form

$$\begin{aligned}
&\overline{0} \ \{ \dots -10, \quad -5, \quad 0, \quad 5, \quad 10, \quad \dots \},\\
&\overline{1} \ \{ \dots -9, \quad -4, \quad 1, \quad 6, \quad 11, \quad \dots \},\\
&\overline{2} \ \{ \dots -8, \quad -3, \quad 2, \quad 7, \quad 12, \quad \dots \},\\
&\overline{3} \ \{ \dots -7, \quad -2, \quad 3, \quad 8, \quad 13, \quad \dots \},\\
&\overline{4} \ \{ \dots -6, \quad -1, \quad 4, \quad 9, \quad 14, \quad \dots \}.
\end{aligned}$$

Taking one residue from each RC, we compose all the variants of the complete residues systems modulo five: 0,1,2,3,4 – CSSNR; 5,1,2,3,4 – CSSPR and 0,1,2,-2,-1 – CSSAVD. According to the definition, CSSNR 0,1,2,3,4 is used in NSRC.

Actually, there is an opinion [3], that it is possible for NSRC not to be called a number system. Indeed, NSRC bases are connected to each other so, that they are selected in a certain way and secured by the permanent modules for the given NS. Each residue modulo is informationally independent on other residues, however, during the implementation of arithmetic operations within each residue unitary or binary NS is generally used. Thus NSRC may be determined not as the number system, but as a special design code numeric data structure, that is specially encoded block of numerical data.

It should be noted that in the proposed approach the NSRC is not opposed to binary PNS, and serves as its extension that allows to solve effectively a certain class of problems. Therefore, the most effective in this case, is an approach that unites the use of a combined MA and binary PNS notation in constructing the control systems. Upon that, for example, control of the entire system can be carried out by the conventional binary commands and blocks; and data processing is performed on the basis of a modular representation of numbers. Thus, the use of the advantages and benefits of NSRC, along with the traditional binary method of control systems constructing can lead to the productivity increase of CSIDPM in general.

To answer the question of whether to use NSRC it's necessary to investigate the influence of the MA basic properties on the structure and operation principles of CSIDPM. Possible logical algorithm research diagram of NSRC effective application can be represented as follows:

– to indentify the areas and directions of science and technology where integer calculations are necessary; to show in which tasks and algorithms *(specifically, to name and show the most important ones)* integer calculations are used; first of all the tasks and algorithms, which include such operations as arithmetic operations of addition, subtraction and multiplication in a positive and negative number ranges, as well as arithmetic operation and algebraic comparisons of numbers;

– to justify the relevance requirements and the need to increase the speed of integer calculations, i.e. to justify the need to increase CSIDPM productivity in order to (to increase the speed of integer calculations it's necessary to create CSIDPM of increased *(in comparison to the existing ones)*) productivity;

– to consider the existing and advanced methods for production increase of CDIDPM, operating in the PNS; possible conclusion: the existing and advanced methods of performance improving of CDIDPM in PNS do not always satisfy the increasing demands to the improved performance implementation of integer calculations *(denote the main reason)*;

– to consider one of the possible *(referred to in modern literature)* options for creation of highly productive CDIDPM on the basis of NSRC; on the basis of the analysis of the NSRC properties and the results of the previous and up-to-date researches of theoretical and practical developments in the application field of non-positional number system, to justify the possibility of its effective application in order to improve the CSIDPM performance.

If the proposed algorithm research scheme is adopted, then the theoretical researches, devoted to the CSIDPM production increase on the basis of NSRC implementation can be carried out. Methods, models and data processing algorithms in NSRC are being developed. Comparative analysis of the achieved results are being conducted.

Before defining a class of tasks and algorithms for which the mathematical apparatus of the numbers theory is effectively applied, it is necessary, on the basis of the results of the NSRC properties researches, to analyze the advantages and disadvantages of the MA use.

3 The properties of the residual classes system

Let's consider the influence of the NSRC basic properties on the CSIDPM structure and principles of functioning [6-9].

1. The independence of residuals. This property gives the opportunity to build CSIDPM in the form of a set of independent, parallel working separate computational paths of information processing, functioning independently from each other according to their specific module m_i. Thus, CSIDPM functioning in NSRC has a modular design, that allows to carry out technical service and elimination of failures and malfunctions of computational paths by their simple replacement without interrupting computational task solving. Arithmetic operations realization time in CSIDPM is determined by the time of operation realization in computing path over the NSRC greatest m_i basis.

Besides, the mistakes arising due to binary bits schemes refusals *(failures)* in any CSIDPM computing path, are not *"multiplied"* in the neighboring tracts they *(remain within one residue)*, that gives the chance to increase the calculations accuracy in NSRC. At that it doesn't matter whether there had been single or multiple errors or multitude of errors with the length of no more than $[\log_2(m_i-1)]+1$ binary bits. An error, occurred in the CSIDPM computing path on the base of m_i is stored in this path until the end of the calculations or is self-destructed in the process of the further calculations. This property of NSRC allows you to create a unique errors control and correction system in the dynamics of the CSIDPM computational process *(without stopping the process of calculation)* at the introduction of the minimum code redundancy that is essential for the data processing systems operating in real-time.

2. The residues equality. We can note that there is a close connection between the arithmetic codes in NSRC and arithmetic AN-codes in PNS. Arithmetic codes in RNS are a futher development of the known positional arithmetic noise-combating multiresidual AN-code. In general terms multiresidual AN-codes is represented in the form of

$$A'_k = (A_k, A_k(\mathrm{mod}\, m_1), A_k(\mathrm{mod}\, m_2), \ldots \\ \ldots, A_k(\mathrm{mod}\, m_i), \ldots, A_k(\mathrm{mod}\, m_{n-1}), A_k(\mathrm{mod}\, m_n)) \quad (5)$$

i.e.

$$A'_k = (A_k, a_1, a_2, \ldots, a_n), \quad (6)$$

where $a_i = A_k - [A_k / m_i]m_i$.

When performing a ratio $\prod_{i=1}^{n} m_i \geq A_k$ the set of residuals $\{a_i\}$ uniquely determines the number A_k. In this case, in the expression structure (5) the value A_k can be excluded. Then a multiresidual code (5) in PNS takes the form of the NSRC code $A'_k = (a_1, a_2, ..., a_n)$ (6), that allows to realize modular arithmetical operations on certain independent computing paths, operating only with residuals $\{a_i\}$.

Based on the procedure of numbers formation in NSRC, it's obviously, that any residual a_i of number $A = (a_1, a_2, ..., a_n)$ carries all the information about the original A number, that gives the opportunity by using the programming methods to replace the refused computing path m_i modulo on the operable path m_j modulo (under the condition that $m_i < m_j$) without interrupting the task solution. Thus, CSIDPM functioning in NSRC and having, for example, two control bases, ensure self operation in case of any two computing path failure. In case of failures in the third or fourth paths CSIDPM continues the computing program execution under some dilution of computing precision i.e. CIDPM in NSRC has the property of a gradual degradation. This property defines a specific difference of the CSIDPM functioning in NSRC: the computer system depending on the requirements imposed to it can have different reliability, computing accuracy and high-speed performance in the calculating process dynamics. Thus, during the tasks solution course, it is possible to vary CSIDPM reliability, computing validity, accuracy and speed. Really, let data be determined by the numerical code presented by the set of bases $\{m_i\}$ ($i = \overline{1, n+k}$) of NSRC. It is known that the time of arithmetic operations execution and decision accuracy depends on the amount of n information bases, and reliability of CSIDPM functioning and validity of calculations depends on the amount of k control bases of NSRC. Let in the process of calculations there was a necessity to enhance the reliability of CSIDPM functioning and (or) validity of calculations. In this case, in real time, without interrupting the calculations, there is a redistribution of NSRC bases $\{m_i\}$ as follows $i = \overline{1, n'+k'}$, and $n' < n$, $k' > k$. At that $n + k = n' + k' = const$. In this case accuracy of calculation is diminished and it is increased the speed of arithmetic operations, that are determined by the amount of information bases n'. If there is a necessity to increase accuracy of decision on the separate section of the computed program, then the redistribution of the program is carried out in the following way: $i = \overline{1, n''+k''}$ ($n + k = n'' + k'' = const$). In this case with the increasing of calculation accuracy ($n'' > n$), CSIDPM reliability (validity of calculations) and the speed of the given task execution is diminished.

Non-module operations *(operation of control, correction, comparison, etc)* in NSRC are carried out in the same way. The time necessary for the execution of non-module operations in NSRC is proportional to the number of n information bases, i.e. to the number of bases, determining the accuracy of calculations. Transition to the calculations with less accuracy allows to increase the speed of CSIDPM. If the ordered ($m_i < m_{i+1}$) NSRC is expanded by the addition of l bases, each of which is bigger than the previous base of the initial NSRC, then the minimum code distance $d_{\min}$ is increased automatically on the value of l. One can obtain the same by diminishing the information bases number of n, i.e. passing to the calculations with less accuracy. Therefore, there is some back proportional dependence between the correcting possibilities of codes in NSRC and the accuracy of calculations. Being applied to PNS the described property, having the possibility to change a correlation between the number of information and control bases in the process of problem solving is based on the well-known method of variable scaling, allowing to diminish the amount of bits in the presentation of numerical information in PNS. Due to it we can introduce the additional bits to organize hardware operative control while having limitations to the increase of weight, dimensions and cost of CSIDPM. Upon that one can vary the accuracy, speed and reliability of calculations. However the specific character of PNS creates the following limitations to the variable scaling method:

- before each timing period of the program implementation it is necessary to make the addi-

tional operations of data transfer, reducing the real speed of CSIDPM on 10 %;

– prior to the preparation of the variable scaling program it is expected to do more theoretical work on the definition of rational scaling coefficient;

– scaling should be applied only for a certain class of problems;

– the given method is generally inexpedient for CSIDPM operating in real time.

Sharing the first and the second properties of NSRC causes the existence of three types of redundancy simultaneously in CSIDPM: structural, information and functional. Based on the idea of the structural redundancy, the sharing of the first and second properties allows to synthesize a model of CSIDPM reliability in NSRC, corresponding to the model of the dynamic redundancy in the PNS. In this case, the information paths $m_1 \div m_n$ of CSIDPM play the role of the working elements and path $m_{(n+1)} \div m_{(n+k)}$ – the role of reserve elements, where k is the number of control *(backup)* NSRC bases.

3. The low-bit of residues. This characteristic allows significantly improve the reliability of CSIDPM and the speed of arithmetic operations both by the low-bit of CSIDPM computing paths and through the ability to use *(unlike PNS)* table arithmetic where arithmetic operations of addition, subtraction and multiplication are performed in one step virtually. In particular the low-bit of residues in representation of the numbers in modular arithmetic gives possibility of a wide choice of options for engineering solutions while implementing modular arithmetic operations based on the following principles:

– summation principle *(based on low-bit binary adders)*;

– table principle *(based on the use of ROM of small size)*;

– direct logical principle of arithmetic operations implementation, based on the modular operations description at the level of switch functions systems of Boolean algebra;

– ring shear principle based on the use of ring shear registers.

On the base of the analysis of the possible use of these three main characteristics *(independence, equal rightness and low-bit of residues, defining non-positional code structure in MA)* non-positional arithmetic in NSRC, compared with the PNS, has the following significant advantages:

– the possibility of calculations parallelization at the level of decomposition of operands, which greatly improves their high-speed performance;

– the possibility of spatial separation of data elements with the possibility of their following asynchronous independent processing;

– the possibility of table *(matrix)* execution of a basic set of arithmetic operations and polynomial functions with single-cycle sampling of modular operation results;

– the possibility of establishing a system of CSIDPM control and correction with the effective detection and correction of faults and failures;

– the possibility to control and correct the errors in the dynamics of the CSIDPM computing process;

– the possibility to use effectively passive and active failsoft on the base of the operational reconfiguration of the CSIDPM structure;

– -less computing and time complexity for the separate classes *(types)* of integer problems;

– demonstration of the special property of the CSIDPM structure in NSRC, ensuring the lack of error expansion effect when implementing arithmetic operations of addition, subtraction and multiplication;

– adaptation of the CSIDPM structure in NSRC for the rapid diagnostics of calculator blocks and points;

– the possibility to increase the CSIDPM reliability in NSRC as a result of the effective simultaneous use of both passive and active failsoft.

– Along with the mentioned benefits of modular arithmetic we can emphasize the number of advantages regarding to the integrated form devices implemented with the MA means [10,11]:

– independent operation of each computing channel of CSIDPM in NSRC according to the

corresponding modules provides significant flexibility in the topological design and layout of the crystal;

– trace interconnections are distributed only within a separate channel for each module of NSRC, which excludes the availability of long routes and, as a result, provides some reduction of power consumption and reduction of signals time delays over critical paths;

– tracing of clock frequency circuits within the data processing channels for each module of NSRC is being improved, that in turn reduces the peak emission in drive circuits;

– implementation of the computing devices on the base of PLD possessing less gating resources, can be easily planed and placed in a few crystals, the possibility of using the table methods of multi-bit numbers processing on a single chip, under the condition that the chip area is not critical;

– introduction of additional redundant channels to design fail-soft systems without full duplication of each computing path of CSIDPM in PSRC.

The represented peculiarities of the integrated devices based on the modular representation indicate that while analyzing and comparing them with conventional positional one, we can not be limited by only usual comparison of speed and occupied space. It is also necessary to take into account the given indicated factors, as they are very important in the development of highly-productive systems, among them the operating in real time ones. Let's note that when writing program in the PNS programmers have difficulties when they have to use large numbers in the program (2^{24}-2^{128} bits).

Let's consider the main drawbacks inherent to NSRC:

– by the type of number in NSRC its quantitative value can not be determined;

– one of the major practical problems is the complexity of the division operation execution; ratio of A/B may not be an integer number, and if it is integer one, in general case, it is impossible to find its exact modular presentation, computing a_i / b_i modulo m_i for each value of i;

– it's also difficult to perform comparison operations for a variety of modular representations $\{a_1, a_2, \ldots, a_p\}$ and $\{b_1, b_2, \ldots, b_p\}$; that leads to the problem of overflows control *(i.e., checking output results beyond the numerical range* $0 \div M-1$*)*;

– to ensure compatibility with the existing binary PNS *(binary representation of data)* CSIDPM in NSRC should have, respectively, the forward converter in modular representation and inverter in the binary number system; converters can also make a significant contribution in both hardware costs and speed of such devices;

– the basic modular operations are more complicated in the technical implementation and more expensive in terms of a chip occupied space and speed than similar binary ones.

Shortcomings listed above limit the scope of the MA, so computer components in the NSRC are rarely implemented in general-purpose machine blocks. But it is possible to allocate a number of specific applications, the implementation of which with the use of the MA is believed to be the most effective. Computer devices where the main calculation share is on multiplication operations combined with addition and subtraction, or computer systems of increased reliability belong to these applications.

Correction of the NSRC disadvantages expands the modular arithmetic applicable scope. In particular, the simplification of the comparison operation implementation and the development of the effective methods and numbers division algorithms will make it possible to apply NSRC in general-purpose computers for solving a wider range of tasks.

The results of the tasks analysis of the data integer processing and accounting for the whole positive properties of NSRC defines the following classes of problems and algorithms, in which the non-positional number system is essentially more effective than PNS:

– cryptographic and module transformations;

– signals digital processing *(image compression, algorithms implementation of Fourier rapid and discrete transformations, etc.)*;

– integer processing in real time and large bits storage (2^{32} - 2^{128} bit);

– vector and matrix processing of large data files;
– neurocomputing information processing;
– optoelectronic tabular data processing;
– monitoring, diagnostics and jam-resistant data coding in CSIDPM;
– using of CSIDPM in NSRC as a computer arithmetic expanders or a general-purpose computing system, performing modular operations of addition, subtraction and (or) multiplication.

4 Conclusions

In the present article it has been shown that the number residues coding, submitted by the respective NSRC bases, is performed by the data from CSSNR. Thus, CSSNR is the basis for the constructing of the non-positional data code structure in NSRC. This is on the one hand. On the other hand the residue classes for each module of NSRC are the basis for the CSSNR formation. Within this framework, strongly mathematically, the notions NSRC and RC cannot be identified. However, experts in the field of MA often use vernacular term RC, having in mind the NSRC.

In the paper there have been specified and systematized the possible fields of science and technology, where there is an urgent need for fast, reliable and high precision integer calculation. There have been shown, that to reach essential "breakthrough" in that direction in PNS is nearly impossible. In fact, the PNS employment in electronics has reached its potential, that is defined by the impossibility to eliminate the inter-bits links between the processed operands in CSIDPM. There is no such drawback in CSIDPM, functioning in NSRC. On the basis of the results of the NSRC properties research, there have been analized the advantages and disadvantages of the MA use. Having used the results of the analysis of the data integer processing tasks and a set of MA positive properties, in the paper there have been formulated tasks and algorithms classes, for which the NSRC use is essentially more efficient than PNS.

References

[1] Akushskii I. Ya. Mashinnaya arifmetika v ostatochnykh klassakh / I. Ya. Akushskii, D. I. Yuditskii. – Moskva: Sov. radio, 1968. – 440 s.
[2] Siora A. A. Otkazoustoichivye sistemy s versionno-informatsionnoi izbytochnost'yu v ASU TP: monografiya / A. A. Siora, V. A. Krasnobaev, V. S. Kharchenko. – Khar'kov: MON, NAU im. N. E. Zhukovskogo (KhAI), 2009. – 320 s.
[3] Morgado M. Modular arithmetic [Electronic Resource] / Matthew Morgado. – Way of access: http://math.uchicago.edu/~may/REU2014/REUPapers/Morgado.pdf. – Title from the screen.
[4] Stewart I. Concepts of Modern Mathematics / Ian Stewart. – Dover Publications: Amazon Digital Services, Inc, 2012. – 352 p.
[5] Lance S. A survey of primality tests [Electronic Resource] / Stefan Lance. – Way of access: http://math.uchicago.edu/~may/REU2014/REUPapers/Lance.pdf. – August 27, 2014. – Title from the screen.
[6] Krasnobaev V. A. Osnovnye svoistva nepozitsionnoi sistemy schisleniya / V. A. Krasnobaev, S. V. Somov, A. S. Yanko // Systemy upravlinnja, navigacii' ta zv'jazku. – 2013. – Vyp. 1 (25). – S. 110–113.
[7] Grandini D. Notes on Modular Arithmetic [Electronic Resource] / Daniele Grandini. – Way of access: http://math.unm.edu/~daniele/Notes%20on%20 Modular%20Arithmetic.pdf. – Spring 2013. – Title from the screen.
[8] 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.
[9] Barsov V. I. Metodologiya parallel'noi obrabotki informatsii v modulyarnoi sisteme schisleniya: monografiya / V. I. Barsov, L. S. Soroka, V. A. Krasnobaev. – Khar'kov: MON, UIPA, 2009. – 268 s.
[10] Kornilov A. I. Printsipy postroeniya spetsializirovannykh vychislitelei s primeneniem modulyarnoi arifmetiki / A. I. Kornilov, M. Yu. Semenov, O. V. Lastochkin, V. S. Kalashnikov // Institut problem proektirovaniya v mikroelektronike RAN. – 2010. – S. 346–355.
[11] 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.

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

Надійшло: Травень 2017.

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

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

Артем Москаленко, к.т.н., доцент, Полтавський інститут бізнесу Міжнародного науково-технічного університету імені академіка Юрія Бугая, Полтава, Україна.
E-mail: moskalenko_artem@ukr.net

Концепція обробки цілочисельних даних, що представлені у системі залишкових класів.

Анотація. Показано, що кодування залишків числа, що представлено відповідними основами системи залишкових класів (СЗК), виконується даними з повної системи найменших невід'ємних лишків (ПСННЛ). У цьому аспекті ПСННЛ є основою для побудови непозиційної кодової структури даних у СЗК. У статті уточнені і систематизовані можливі сфери та напрямки науки і техніки, де є гостра необхідність у швидких, надійних і високоточних цілочислових обчислень. На основі результатів досліджень властивостей СЗК, проаналізовано переваги і недоліки використання модулярної арифметики (МА). Використовуючи результати аналізу завдань цілочислової обробки даних і сукупності позитивних властивостей МА, у статті визначені класи задач і алгоритмів, для яких використання СЗК істотно ефективніше ніж двійкова позиційна система числення.

Ключові слова: система залишкових класів, модулярна арифметика, позиційна система числення, повна система найменших невід'ємних лишків, комп'ютерна система і засоби обробки даних, що представлені у цілочисловому вигляді, клас лишків.

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

Поступила: Май 2017.

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

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

Артём Москаленко, к.т.н., доцент, Полтавский институт бизнеса Международного научно-технического университета имени академика Юрия Бугая, Полтава, Украина.
E-mail: moskalenko_artem@ukr.net

Концепция обработки целочисленных данных, представленных в системе остаточных классов.

Аннотация. Показано, что кодирование остатков числа, представленного соответствующими основаниями системы остаточных классов (СОК), производится данными из полной системы наименьших неотрицательных вычетов (ПСННВ). В этом аспекте ПСННВ является основой для построения непозиционной кодовой структуры данных в СОК. В статье уточнены и систематизированы возможные области и направления науки и техники, где есть острая необходимость в быстрых, надежных и высокоточных целочисленных вычислений. На основе результатов исследований свойств СОК, проанализированы преимущества и недостатки использования модулярной арифметики (МА). Используя результаты анализа задач целочисленной обработки данных и совокупности положительных свойств МА, в статье определены классы задач и алгоритмов, для которых использование СОК существенно эффективнее двоичной позиционной системы счисления.

Ключевые слова: система остаточных классов, модулярная арифметика, позиционная система счисления, полная система наименьших неотрицательных вычетов, компьютерная система и средства обработки данных, представленных в целочисленном виде, класс вычетов.

УДК 004.652

МОДЕЛЬ ДАННЫХ «ОБЪЕКТ-СОБЫТИЕ»: ТРЕБОВАНИЯ И СИНТЕЗ МОДЕЛИ

Виталий Есин

Харьковский национальный университет имени В.Н. Каразина, пл. Свободы, 4, г. Харьков, 61022, Украина
v.i.yesin@karazin.ua

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

Поступила в июне 2017

Аннотация. *Исходя из необходимости нахождение новых решений актуальной задачи своевременного создания, модернизации в рамках запланированного бюджета баз данных, обладающих требуемыми качествами, формулируются требования, предъявляемые к разрабатываемой модели данных. В соответствии со сформулированными требованиями и общим подходом к проблеме семантического моделирования, предложенным К. Дейтом, синтезируется модель данных, получившая название – «объект-событие».*

Ключевые слова: *модель данных, семантическое (концептуальное) моделирование, база данных.*

1 Введение

Развитие технологии баз данных (БД) привело к созданию весьма мощных и удобных в эксплуатации информационных систем (ИС), возрастание роли которых в современных условиях является объективной реальностью, обусловленной необходимостью предоставления своевременной и достоверной информации, как одного из наиболее важного ресурса общества, для принятия оптимального решения практически во всех сферах деятельности человека. Анализ ключевых проблем, современного состояния и развития технологий баз данных показал, что основные происходящие сегодня изменения в данной области, обусловленные различными факторами, в том числе, повышенным интересом к организации хранения и обработке больших объемов структурированных и неструктурированных данных, располагающихся во всевозможных источниках, потребностью постоянного совершенствования действующих ИС, путем их адаптации к изменениям внешней среды вне зависимости от конкретной области применения, расширяющимися требованиями потребителей информационных продуктов, вызваны необходимостью решения новых научно-практических задач. Одной из таких актуальных задач является задача адаптации действующих БД информационных систем организационного управления (ИСОУ) к новым условиям функционирования.

Устойчивая тенденция необходимости постоянного совершенствования действующих БД ИСОУ, путем их адаптации к изменениям в предметной области и требованиям бизнес-процессов, ведет к росту востребованности проектов модернизации, интеграции, замены существующих систем. А именно проектов по: разработке новых БД ИСОУ и их интеграции с существующими БД информационных систем; разработке новых БД ИСОУ с целью замены существующих БД информационных систем; модернизации существующих БД ИСОУ, суть которых – реинжиниринг действующих баз данных информационных систем. С реинжинирингом БД ИСОУ в работе связываются такие достаточно широко используемые в различных источниках понятия, как: эволюция баз данных информационных систем, миграция, модернизация, реструктуризация, прямой, обратный инжиниринг и т. д. Деятельность, соотносимая с этими понятиями, подразумевает ее рассмотрение либо как одну из форм, либо как подпроцесс процесса реинжиниринга БД ИСОУ. При этом одним из важных требований, предъявляемых к процессу реинжиниринга существующих БД ИСОУ, является своевременность завершения соответствующих проектов в рамках запланированного бюджета с заданными характеристиками качества, которое, к сожалению, как показывают результаты анали-

за IT-проектов, проведенного международными организациями экспертов, не всегда выполняется. Достаточно большое число проектов (более 60%) были провалены или завершены с опозданием, причем с гораздо большими затратами, чем планировалось [1,2].

Налицо существование нерешенной проблемы, связанной с необходимостью своевременного создания, модернизации в рамках запланированного бюджета информационных систем, обладающих требуемыми качествами, и ограниченностью возможностей существующих методов проектирования. В отношении реляционных баз данных (РБД), как получивших наибольшее распространение в ИС рассматриваемого класса, указанная ограниченность возможностей обусловлена ориентацией традиционной методологии их проектирования, используемой при реинжиниринге БД ИСОУ, на итерационную, достаточно сложную и трудоемкую процедуру создания уникальных концептуальной модели, логической и физической схем при разработке новой БД, либо на существенное их преобразование при модернизации. Что часто влечет за собой значительные, не всегда прогнозируемые объективные затраты временных и финансовых ресурсов. В результате возникает объективная необходимость в пересмотре существующих подходов, методологий и технологий реинжиниринга баз данных. А именно потребность в проведении исследований, направленных на создание таких универсальных моделей и методов обеспечения адаптируемости реляционных баз данных к изменениям в предметной области (ПрО), которые позволят избавиться от необходимости затратной политики выполнения лишних работ при реинжиниринге БД ИСОУ.

Проведенный анализ известных «расширенных» моделей (термин, введенный К. Дейтом [3], для обозначения моделей, используемых при семантическом моделировании): ERM *(entity-relationship model),* EERM *(enhanced entity-relationship model),* HERM (higher-order entity-relationship model) [4-6], ORM (object role modeling) [7-12], объектной [13-16], семантической бинарной [17,18], семантических сетевых [19,20], инфологической [17, 21-23], онтологической [24-27], а также реляционной модели [28,29], систем доступа к данным, основанным на онтологиях [30], позволил сделать предположение о возможности синтеза таких моделей и методов, если соответствующим образом интегрировать в них подходы и решения, присущие перечисленным выше моделям и системам.

Для доказательства (проверки) справедливости этой гипотезы в первую очередь необходимой стала разработка одной из таких ключевых, востребованных моделей – модели класса «расширенных».

2 Требования, предъявляемые к модели

В технологиях баз данных концептуальное *(семантическое)* моделирование ПрО, как отмечается в работе [31], решает две важные задачи: во-первых, обеспечивает представление ПрО на таком уровне абстракции, благодаря которому оно становится достаточно выразительным для аналитиков, разработчиков, экспертов ПрО, программистов и конечных пользователей; во-вторых, дает возможность проектировщикам БД специфицировать ее структурную и поведенческую организацию в виде, независимом от технических особенностей СУБД.

При этом возможности отображения семантики ПрО в концептуальных моделях в значительной мере связаны со свойствами выразительных средств, используемых для их представления: какие понятия принимаются в качестве предопределенных, что представляет собой атомарный факт, каковы используемые для описания ПрО механизмы абстракций, описания поведения сущностей и т.д. [31]. В случае расхождения языка формализации со складом мышления специалиста, реализация системы обработки данных может стать слишком сложной или вообще неразрешимой проблемой [24]. С другой стороны, решая проблему разностороннего и многоуровневого представления данных, необходимо не только учитывать взгляды пользователей, но и аспекты дальнейшей компьютерной организации и управления данными.

Таким образом, на основании результатов анализа существующих достижений в области

семантического моделирования и перспективных направлений ее развития, исходя из необходимости нахождение решений обозначенной проблемы, связанной с необходимостью своевременного создания, модернизации в рамках запланированного бюджета баз данных, обладающих требуемыми качествами, опираясь на приведенные выше заключения, были сформулированы требования, предъявляемые к разрабатываемой модели:

а) модель должна обладать достаточной общностью с тем, чтобы ее средства позволяли обеспечивать прозрачное для всех участников проекта адекватное, комплексное представление данных моделируемой ПрО, их структуры и ограничений целостности;

б) разрыв между создаваемой моделью и реляционной моделью данных, на основе которой в дальнейшем реализовывается БД ИСОУ, приспособленная к динамичным изменениям предметных областей, не должен быть большим. Более того состав и структура набора формальных объектов создаваемой модели и реляционной модели данных должны быть близкими, чтобы при отображении концептуальной схемы ПрО в даталогическую среду можно было легко воспользоваться заранее известными правилами преобразования структур, ограничений целостности из одной модели в другую и не утратить семантики ПрО;

в) возможность комплексного использования модели, как на соответствующем этапе проектирования БД *(в качестве инструмента концептуального моделирования ПрО),* так и на стадии функционирования РБД ИСОУ, как основы пользовательских интерфейсов.

3 Синтез модели «объект-событие»

Синтез модели, удовлетворяющей сформулированным требованиям, проведем в соответствии с общим подходом, изложенным К. Дейтом [3], и включающим четыре основных этапа:

1) выявление некоторого множества semantic concepts* *(словосочетание, применяемое автором в оригинальном тексте своей монографии [36])*, которые будут использоваться для описания «реального мира» (* – в переводной монографии [3] словосочетание semantic concepts определяется как множество семантических концепций или понятий, хотя корректнее было бы вместо термина концепция использовать термин концепт; поэтому далее по тексту будет использоваться либо непереводимый оригинал автора, либо термины концепт, понятие, базовое понятие);

2) определение набора формальных объектов, которые могут использоваться для представления описанных понятий;

3) определение формальных правил поддержки целостности данных;

4) определение формальных операторов.

Известно, что информация о реальном мире (рассматриваемой ПрО) дается через восприятие. При этом само восприятие достаточно сложно и состоит из множества взаимосвязанных фактов [17]. Системный подход к познанию ориентирует аналитика на рассмотрение любой ПрО с позиций закономерностей системного целого и взаимодействия составляющих его частей, исходя из многоуровневой иерархической организации любой сущности, когда все объекты, процессы и явления с одной стороны уместно рассматривать как множество более мелких подмножеств *(признаков, деталей)*, а с другой – любые объекты разумно рассматривать как элементы более высоких классов обобщений [24]. Если исходить из того, что предлагаемая «расширенная» модель должна обеспечивать возможность правильного представления наших восприятий, то при выборе способа представления элементов ПрО, целесообразно руководствоваться принципами, в соответствии с которыми такое представление человек, в первую очередь, строит для себя на естественном языке. В виду того, что все процессы реального мира протекают в пространстве и времени (в большинстве случаев моделируемая ПрО представляет собой динамическую систему, состоящую из определенной последовательности состояний, конечность множества которых, определяется в каждый момент времени), человек, как правило, отмечается в [17], описывает элементарные факты на естественном языке в терминах объектов, свойств объекта *(связей объектов)*, значений свойств и

времени наступления события. Поэтому описание моделируемой ПрО целесообразно осуществлять именно в этих терминах, несколько расширив и дифференцировав их набор, который в итоге будет включать следующие понятия (выделенные курсивом):

– *объект*, связываемый с различными выделенными частями моделируемой ПрО, *свойство* (*характеристика*) *объекта* (при этом абстракция обобщения позволяет соотнести множество объектов (подклассов) и их свойств с одним общим *классом*);

– *событие* (определенного *класса*), происходящее с объектом, *свойство* (*характеристика*) *события*, *время* наступления события;

– *значение характеристики объекта* и *события*,

выделяя при необходимости в качестве особых характеристик объектов изменяемые во времени признаки (*параметры*, относящиеся к определенным классам), а также некоторые другие данные (содержательное описание, графическое изображение, аудио-, видеоинформацию).

Эти понятия являются неформальными *semantic concepts* создаваемой модели, как ее неотъемлемый элемент, согласно общему подходу к разработке «расширенных» моделей, предложенному К. Дейтом. Более подробно, с формализацией, эти базовые понятия будут рассмотрены ниже.

Следует заметить, что основополагающими *semantic concepts*, давшими название создаваемой модели, являются базовые понятия «объект» и «событие». Объект как нечто, представляющее интерес, может существовать независимо от того, определены или нет его свойства и связи с другими объектами. Объект возникает, когда субъект начинает проявлять к нему интерес, и исчезает, когда этот интерес утрачивается. При этом единственное свойство, с которым следует соотносить существование объекта – это время его возникновения, исчезновения и изменения, связанное с событиями с ним происходящими [17].

В соответствии с определением модели данных, как совокупности правил описания и структурирования данных, допустимых операций над ними и видов ограничений целостности, которым они должны удовлетворять, модель «объект-событие» ($\mathfrak{M}$) в формализованном виде можно представить как кортеж:

$$\mathfrak{M} = \langle \mathrm{S}(\mathfrak{A}, \mathbb{R}, \mathbb{F}),\ \mathrm{P},\ \mathrm{L} \rangle, \tag{1}$$

где $\mathrm{S}(\mathfrak{A}, \mathbb{R}, \mathbb{F})$ – множество правил описания и структурирования данных ПрО; $\mathfrak{A}$ – множество базовых понятий модели (некоторые из которых приведены в таблице 1); $\mathbb{R}$ – множество отношений между базовыми понятиями модели; $\mathbb{F}$ – множество функций интерпретации, заданных на базовых понятиях (глоссарий, составленный для множества понятий $\mathfrak{A}$) и отношениях; P – множество ограничений целостности; L – язык модели данных.

Таблица 1 – Перечень базовых понятий модели

Базовое понятие	***Определение***	***Условное обозначение***
Раздел	– некоторая выделенная и уникально поименованная часть предметной области.	Раздел
Класс объектов	– совокупность типов объектов, объединяющих экземпляры объектов, выделенные по нескольким значительным качественным признакам, и идентифицируемая именем.	КлассО
Тип объектов	– совокупность схожих по нескольким значительным качественным признакам экземпляров объектов, идентифицируемая именем.	ТипО
Экземпляр объекта *(объект)*	– однозначно идентифицируемый объект из набора объектов, принадлежащих некоторому типу и классу объектов.	ЭкзО

Продолжение таблицы 1

Базовое понятие	***Определение***	***Условное обозначение***
Характеристика типа объектов	– один поименованный признак (качество, свойство) из всей совокупности признаков, описывающих тип объектов определенного класса.	ТипХОп
Фактическая характеристика объекта	– один поименованный признак (качество, свойство) из всей совокупности признаков, описывающих экземпляры объектов определенного класса.	ТипХОф
Значение характеристики объекта	– значение, присвоенное характеристике экземпляра объекта.	ЗначХО
Класс событий	– совокупность событий (экземпляров событий), выделенных по некоторым качественным признакам, которые могут происходить с экземплярами объектов определенного класса в некоторый момент или интервал времени, и идентифицируемая именем.	КлассС
Событие (экземпляр события)	– факт или действие, которое происходит (произошло, будет происходить) с некоторым объектом в определенный момент или интервал времени. Идентифицируется временем и объектом, принадлежит некоторому классу событий. С одним экземпляром объекта в один и тот же момент (интервал) времени может происходить только одно событие одного класса (при допустимости нескольких событий разных классов).	ЭкзС
Характеристика события	– один поименованный признак (качество, свойство) из всей совокупности признаков, описывающих событие определенного класса.	ТипХС
Значение характеристики события	– значение, присвоенное характеристике экземпляра события, которое произошло с конкретным экземпляром объекта.	ЗначХС
Класс параметров объектов	– совокупность характеристик параметров объектов, выделенных по некоторым качественным признакам, идентифицируемая именем.	КлассПО
Характеристика параметра объекта	– изменяемый во времени один поименованный признак (качество) из всей совокупности признаков, описывающих экземпляры объектов определенного класса.	ТипХПО
Единица физической величины	– символьное обозначение единиц физической величины.	ЕдИзмер
Документ	– структурированные или неструктурированные данные, необходимые для дополнения, детализации описания существенных свойств (признаков, качеств), связываемых с основными базовыми понятиями модели.	Документ
Папка документов	– поименованная совокупность документов, выделенных по каким-либо признакам.	Папка

Каждое из базовых понятий (далее в работе часто вместо их полных названий используются условные обозначения) множества $\mathfrak{A}$:

$$\mathfrak{A} = \{\text{Раздел, КлассО, ТипО, ЭкзО, ТипХОф, ТипХОп, ЗначХО, КлассПО, ТипХПО, ТипЗнПО, ЗначХПО, КлассС, ЭкзС, ТипХС, ЗначХС, Документ, Папка, ЕдИзмер}\} \quad (2)$$

соотносится с одноименным множеством (рассматривается как имя некоторого множества), являющимся основным компонентом некоторого формального объекта, требующего определения в соответствии с указанным выше подходом к синтезу модели. Например, базовое понятие «Раздел» соотносится с множеством, имеющим имя *Раздел*, базовое понятие «КлассО» соотносится с множеством, имеющим имя *КлассО*, и т. д.

При описании моделируемой ПрО каждое из этих множеств будет содержать в качестве элементов конкретные разделы, классы объектов, событий, параметров объектов, типы объектов, соответствующие характеристики и т. д., имена *(названия)* которых будут либо заимствованы из словарей терминов рассматриваемой ПрО, либо получены в результате неформального соглашения между разработчиками и пользователями. Тогда множество отношений между базовыми понятиями модели «объект-событие» $\mathbb{R}$ – есть множество отношений между одноименными множествами, соотносимыми с этими понятиями, и их элементами, как математических структур (формальных объектов), позволяющих описывать свойства различных элементов моделируемой ПрО и их взаимосвязи (взаимодействия).

В модели «объект-событие» было определено конечное множество таких отношений. Среди них:

– математические отношения, позволяющие формально описывать, так называемые, классификационные отношения (отношения классификации) [24,32], определяющие тип взаимодействия между элементами предметной области. А именно, отношения, фиксирующие связи между элементами «владельцами» и «подчиненными» соответствующих множеств *Раздел, КлассО, КлассС, КлассПО, ЭкзО, Папка* (данный тип взаимосвязи между элементами множеств, обобщающий типы классификационных отношений «род-вид», «класс-подкласс», «целое-часть», назван в модели – «владелец-подчиненный»):

$$R \subseteq Раздел \times Раздел = Раздел^2 = \{(P_i, P_j) \mid P_i, P_j \in Раздел\}, \quad (3)$$

где R – бинарное отношение на множестве *Раздел*; роли упорядоченных элементов кортежей отношения R распределяются следующим образом: P_i – «подчиненный», P_j – «владелец» ($i, j \in Ix$; $Ix = \{1,...,|Раздел|\}$ – некоторое множество индексов; $|Раздел|$ – мощность множества *Раздел*.

Аналогичные формы записи для остальных отношений этой группы:

$$C \subseteq КлассО \times КлассО = КлассО^2 = \{(Кл_{o_k}, Кл_{o_l}) \mid Кл_{o_k}, Кл_{o_l} \in КлассО\}; \quad (4)$$

$$O \subseteq ЭкзО \times ЭкзО = ЭкзО^2 = \{(Экз_{o_r}, Экз_{o_s}) \mid Экз_{o_r}, Экз_{o_s} \in ЭкзО\} \quad (5)$$

и т. д.;

– отношения, позволяющие формально описывать, так называемые признаковые [24,32] отношения, приписывающие различные качественные признаки понятиям, которые используются для обозначения элементов моделируемой ПрО. Ниже приведены некоторые *n*-арные отношения с типами взаимодействия между определенными множествами, соответствующими одноименным базовым понятиям, и их элементами, названными в модели – «иметь характеристику», «иметь документ», «иметь значение характеристики»:

- «иметь характеристику», например, характеристику события (для класса событий), которая «имеет меру»:

$$X \subseteq ТипХС \times ЕдИзмер \times КлассС = \{(Т_{хс}, Ед_{ф}, Кл_{с}) \mid Т_{хс} \in ТипХС \wedge Ед_{ф} \in ЕдИзмер \wedge Кл_{с} \in КлассС\}, \quad (6)$$

- «иметь документ» (для основных базовых понятий модели):

$$D \subseteq Документ \times Папка \times \mathfrak{A} = \{(d, f, u) \mid d \in Документ \wedge f \in Папка \wedge u \in \mathfrak{A}\}; \quad (7)$$

- «иметь значение характеристики», например, для фактической характеристики объекта:

$$Z_{H_ф} \subseteq ЗначХО \times ЕдИзмер \times ТипХОф \times ЭкзО = \{(Зн_{хоф}, Ед_ф, Т_{хоф}, Экз_о \mid Зн_{хоф} \in ЗначХО \wedge Ед_ф \in ЕдИзмер \wedge Т_{хоф} \in ТипХОф \wedge Экз_о \in ЭкзО\}; \quad (8)$$

– математическое отношение $ЭкзС$, позволяющее формально описывать факты или действия, которые происходят *(произошли или произойдут)* с некоторыми объектами в определенный момент или интервал времени, и определяющее тип взаимосвязи между соответствующими базовыми понятиями, названный в модели – «иметь событие»:

$$ЭкзС \subseteq КлассС \times ВремяНС \times ВремяКС \times ЭкзО = \{(Кл_с, Вр_{нс}, Вр_{кс}, Экз_о) \mid Вр_{нс} \in ВремяНС \wedge Вр_{кс} \in ВремяКС \wedge Кл_с \in КлассС \wedge Экз_о \in ЭкзО\}, \quad (9)$$

где $ВремяНС$ – множество времен начала событий; $ВремяКС$ – множество времен окончания событий (допускается отсутствие – неопределенное значение (*null*) элемента $Вр_{кс} \in ВремяКС$).

Множество функций $\mathbb{F}$. В модели «объект-событие» кроме декларативных функций интерпретации, приведенных в виде глоссария, составленного для множества понятий $\mathfrak{A}$ (см.табл. 1), были определены следующие виды функциональных отношений, как специальный вид отношений:

– отношение, определяющее тип взаимодействия между соответствующими базовыми понятиями модели «образуют тип»:

$$f : ЭкзО \times TunXOn \to TunO \Leftrightarrow ЭкзО \times TunXOn \xrightarrow{f} TunO, \quad (10)$$

где для любой упорядоченной пары $(Экз_о, T_{хоп})$ из $ЭкзО \times TunXOn$ $(Экз_о \in ЭкзО; T_{хоп} \in TunXOn)$ существует не более одного элемента $T_о \in TunO$, такого, что $(Экз_о, T_{хоп}, T_о) \in f$, тогда: $T_о = f(Экз_о, T_{хоп})$.

– отношение, определяющее тип взаимодействия между соответствующими базовыми понятиями модели *Раздел* и *КлассО*. Это отношение агрегации – «целое-часть» («*Раздел* включает *КлассО*»):

$$\rho : КлассО \to Раздел \Leftrightarrow КлассО \xrightarrow{\rho} Раздел. \quad (11)$$

Использование именно отношения «целое-часть» в данном случае обусловлено его примечательной особенностью – такие отношения могут быть установлены между сущностями различных семантических типов: физическими объектами, процессами и действиями, географическими регионами, свойствами и состояниями, коллекциями и множествами, абстрактными сущностями и т.д. [33]. Это соответственно в определенной степени упрощает описание некоторых элементов ПрО;

– отношения, определяющие тип взаимодействия между соответствующими базовыми понятиями модели «образуют класс» (например, класс объектов):

$$\alpha : \Psi \to КлассО \Leftrightarrow \Psi \xrightarrow{\alpha} КлассО, \quad (12)$$

где $\Psi \subseteq TunO \times TunXOф$ и т. д.

Представленные множества базовых понятий модели «объект-событие» *(как множества определенных «полезных» semantic concepts)*, отношений $\mathbb{R}$ и функций $\mathbb{F}$ *(как набор формальных объектов)*, определяют правила описания и структурирования данных ПрО.

Полученный набор формальных объектов, как математических структур, несложно реализовать в рамках реляционной модели, которая в своем большинстве случаев [34], вполне до-

статочна для моделирования различных ПрО. Это позволяет выполнить предъявляемое к модели требование по обеспечению близости (согласованности) состава и структуры ее набора формальных объектов, с базисом отношений реляционной модели данных, на основе которой реализуется БД ИСОУ, адаптированная к изменениям предметных областей.

Множество ограничений целостности P. Как известно [17], ограничения вводятся в модели данных в целях повышения их семантичности и расширения возможностей поддержки целостности данных. В модели, в соответствии с классификацией, приводимой в различных авторитетных источниках [17,35], специфицируются следующие типы ограничений целостности данных: - явные (семантические ограничения целостности); - неявные (внутренние, поддерживаются самой структурой модели данных). Ряд явных ограничений целостности в модели относится к характеристикам объектов, событий, параметров объектов. Прежде всего, это множества допустимых значений для соответствующих характеристик (ограничения на допустимые значения):

$$
\begin{aligned}
&D = \{D_1, D_2, D_3\};\ D_1 = \{D_1^1, ..., D_1^{K_1}\};\ D_2 = \{D_2^1, ..., D_2^{K_2}\};\ D_3 = \{D_3^1, ..., D_3^{K_3}\};\\
&D_1^i = dom(T_{xo}^{i_{спис}});\ i = 1...K_1;\ T_{xo}^{i_{спис}} \in TunXO^{спис} \subseteq (TunXOф \bigcup TunXOn);\\
&D_2^j = dom(T_{xc}^{j_{спис}});\ j = 1...K_2;\ T_{xc}^{j_{спис}} \in TunXC^{спис} \subseteq TunXC;\\
&D_3^k = dom(T_{xno}^{k_{спис}});\ k = 1...K_3;\ T_{xno}^{k_{спис}} \in TunXПО^{спис} \subseteq TunXПО,
\end{aligned}
\qquad (13)
$$

где $dom(T_{xo}^{i_{спис}})$, $dom(T_{xc}^{j_{спис}})$, $dom(T_{xno}^{k_{спис}})$ – домены соответствующих характеристик объектов ($T_{xo}^{i_{спис}}$), событий ($T_{xc}^{j_{спис}}$), параметров объектов ($T_{xno}^{k_{спис}}$) моделируемой ПрО, принадлежащих к так называемому перечисляемому (списочному) типу (значения для них выбираются из заранее сформированного списка); K_1, K_2, K_3 – число соответствующих характеристик объектов, событий, параметров объектов списочного типа.

Следует отметить, что в достаточно многих ПрО, (автопром, авиапром, военно-промышленный комплекс), необходимо учитывать ограничения, накладываемые на конкретные экземпляры объектов. Например, комплектующие к некоторым изделиям (объектам) должны пройти процедуру соответствующей приемки, сертификации. После чего только они (при соответствующей идентификации), а никакие другие элементы, могут быть установлены в нужное изделие. Человек может понять нечто только в конкретном контексте [17]. Поэтому определение множества допустимых экземпляров объектов, задаваемых в модели в виде домена: $dom(Экз_o^{огр})$, является также неотъемлемой и востребованной частью описания ПрО ($Экз O_{o_z} \in dom(Экз_o^{огр}) \subseteq ЭкзO$), т.к. впоследствии позволяет уменьшить количество потенциальных ошибок.

Следующим ограничением, выражаемым в модели, является ограничение, накладываемое на используемые единицы физических величин характеристик объектов, событий, параметров объектов рассматриваемой ПрО, в виде задания домена: $dom(Ed_ф)$.

Модель «объект-событие» позволяет представить ограничение по существованию, заключающееся в том, что для существования элемента в отношении S_1 необходимо, чтобы он был связан с элементом в отношении S_2 ($S_1 \to S_2$: каждый элемент S_1 отображен в один элемент S_2). Например, в модели без конкретного класса объекта, не может быть его типов, характеристик, экземпляров и событий с ними происходящими и т.д. При удалении класса объектов, удаляются все его типы, характеристики, экземпляры, события и все «подчиненные» ему классы объектов, а также их типы, характеристики, экземпляры, события и т.д. Аналогично для классов событий и параметров объектов, разделов, экземпляров объектов и событий.

Как внутренние ограничения следует рассматривать требования возможности выражения принадлежности элементов моделируемой ПрО к множествам отношений модели «объект-

событие», а также к множеству значений с помощью предикатов. При этом сами предикаты могут быть заданы явно, как в случае выражения ограничений:

– на максимальное количество экземпляров объектов для определенного класса объектов:

$$C = \{(Кл_{o_k}, Кл_{o_l}, c_{obj}) \mid Кл_{o_k}, Кл_{o_l} \in КлассО \wedge c_{obj} \in \mathbb{N}^+\}, \quad (14)$$

где c_{obj} – элемент упорядоченной тройки отношения (14), определенный на множестве натуральных положительных чисел $\mathbb{N}^+$, ограничивающий число экземпляров объектов ($|ЭкзО| \le c_{obj}$) для класса объектов $Кл_{o_k}$;

– на максимальное количество значений, которые могут быть присвоены определенной характеристике события для экземпляра события заданного класса:

$$X = \{(T_{xc}, Ед_{ф}, Кл_{c}, x_{ce}) \mid T_{xc} \in ТипХС \wedge Ед_{ф} \in ЕдИзмер \wedge Кл_{c} \in КлассС \wedge x_{ce} \in \mathbb{N}^+\}, \quad (15)$$

где x_{ce} – элемент упорядоченной четверки отношения (15), определенный на множестве натуральных положительных чисел $\mathbb{N}^+$, ограничивающий количество значений, которые могут быть присвоены характеристике события T_{xc} для экземпляра события класса $Кл_{c}$ и т.д.

При этом выделение в отдельную компоненту базового понятия «событие», напрямую связанного со временем, усиливает контроль за непротиворечивостью данных – ограничением их целостности, обеспечивая сохранение сведений о свойствах или связях, которые либо являются на текущий момент достоверными – состояние ПрО, либо их утратили.

Уникальная идентификация элементов множеств, соотнесенных с одноименными базовыми понятиями модели, достигается уникальностью именования, в том числе: для элементов множеств $Раздел$, $КлассО$, $КлассС$, $КлассПО$, $Папка$, $ЭкзО$ – уникальностью соответствующих имен в иерархиях «владелец-подчиненный» (иерархических имен) в рамках рассматриваемой ПрО; для элементов множеств $ТипХОф$, $ТипХОп$, $ТипХС$, $ТипХПО$, $ТипЗнПО$ – уникальностью имен характеристик конкретных классов и типов объектов, классов событий и параметров объектов соответственно.

Ссылочная целостность, предполагающая обязательное наличие объекта, на который ссылается другой объект, в модели обеспечивается благодаря существующим типам взаимодействия между элементами множеств $Раздел$, $КлассО$, $КлассС$, $КлассПО$, $Папка$, $ЭкзО$ – «владелец-подчиненный» (выражения (3)-(5) и им подобные).

Основными операциями в модели «объект-событие» являются: операция создания (вставки) элементов множеств, одноименных базовым понятиям модели $\mathfrak{A}$, и их связей между собой в соответствии с $\mathbb{R}$ и F; операция изменения указанных элементов множеств, одноименных базовым понятиям модели; операция удаления указанных элементов множеств, одноименных базовым понятиям модели, а также зависимых от них (в соответствии с $\mathbb{R}$ и F) элементов других множеств; операция выборки в соответствии с указанными условиями элементов из множеств, одноименных базовым понятиям модели.

Информационные запросы могут быть выражены в понятиях операций над множествами. Однако для неподготовленного специалиста теоретико-множественная модель является непростой для ее восприятия и понимания. Поэтому для достижения простоты и гибкости практического использования модели «объект-событие» был разработан специальный язык L – язык модели данных (ЯМД), сочетающий ясность и простоту использования его операторов для участников проекта, а также полноту представления данных моделируемой ПрО.

Более детально язык модели данных, близкий к некоторому подмножеству естественного языка, а также его возможности рассмотрены в работах [37,38].

4 Выводы

1. В результате анализа достижений в области семантического моделирования и перспективных направлений его развития, а также исходя из необходимости нахождения решений проблемы, связанной с потребностью своевременного создания и модернизации, в рамках запланированного бюджета, баз данных, обладающих требуемыми качествами, сформулированы требования, предъявляемые к разрабатываемой модели.

2. В соответствии с представленными требованиями синтезирована модель «объект-событие», которая содержит определенные подходы и решения, апробированные в известных «расширенных» моделях: ERM, EERM, HERM, ORM, объектной, семантических сетевых, онтологической, инфологической, основанной на логике предикатов с расширенной поддержкой концепции времени.

3 В процессе создания модели «объект-событие» были определены: множество базовых понятий модели, которые используются для описания реального мира; множество отношений между базовыми понятиями модели и множество функций интерпретации, заданных на базовых понятиях и отношениях (как набор формальных объектов, необходимых для представления базовых понятий модели); множество ограничений целостности; множество допустимых операций над данными и специальный язык модели данных, сочетающий в себе понятность и простоту использования его операторов для участников проекта, а также полноту представления данных моделируемой ПрО.

4. Применение средств разработанной модели «объект-событие» позволяет:

- обеспечить комплексное представление данных моделируемой ПрО, их структуры и ограничений целостности;
- упростить процесс преобразования концептуальной модели ПрО в схему реляционной БД;
- реализовать возможность использования модели, как на этапе концептуального проектирования БД, так и на стадии функционирования РБД ИСОУ.

Ссылки

[1] Chaos Manifesto 2013: Think Big, Act Small online version. The Standish Group [Electronic Resource]. – Way of access: http://www.versionone.com/assets/img/files/ChaosManifesto2013.pdf. – Title from the screen.

[2] Standish Group 2015 Chaos Report – Q&A with Jennifer Lynch [Electronic Resource]. – Way of access: https://www.infoq.com/articles/standish-chaos-2015. – Title from the screen.

[3] Deit K. Dzh. Vvedenie v sistemy baz dannykh / K. Dzh. Deit; per. s angl. – [8-e izd.]. – Moskva : Izdatel'skii dom "Vi-l'yams", 2005. – 1328 s.

[4] Chen P. P. S. The entity-relationship model – toward a unified view of data / P. P. S. Chen // ACM Transactions on Database Systems (TODS). – 1976. – Vol.1. – № 1. – P. 9 – 36.

[5] Teorey T. J. Database modeling and design: logical design / T. J. Teorey, S. S. Lightstone, T. Nadeau. – Elsevier, 2006. – 282 p.

[6] Thalheim B. Entity-relationship modeling: foundations of database technology / B. Thalheim. – Berlin; Heidelberg: Springer-Verlag, 2000. – 639 p.

[7] Halpin T. Business roles and object-role modeling / T. Halpin // DBP&D. – 1996. – № 10. – P. 66–72.

[8] Halpin T. Conceptual schema and relational database design / T. Halpin. – [2nd edition] . – Sydney, Australia: Prentice-Hall of Australia Pty. Ltd., 1995. – 500 p.

[9] Halpin T. Entity Relationship modeling from an ORM perspective: Part 1 / T. Halpin // Journal of Conceptual Modeling. – 2000. – № 13. – P. 1 – 10.

[10] Halpin T. Using object role modeling to design relational databases: Interview / T. Halpin // DBMS. – 1995. – № 8 (9). – 38 p.

[11] Nijssen G. M. The Entity-Relationship Data Model Considered Harmful / G. M. Nijssen, D. J. Duke, S. M. Twine // Proc. 6th Symposium on Empirical Foundations of Information and Software Sciences. – Atlanta, Ga., 1988. – P. 109–130.

[12] Nijssen G. M. Conceptual Schema and Relational Database Design: a fact oriented approach / G. M. Nijssen, T. A. Halpin. – Prentice-Hall, Inc., 1989. – 342 p.

[13] Kalinichenko L. A. Standart sistem upravleniya ob"ektnymi bazami dannykh ODMG-93: kratkii obzor i otsenka sosto-yaniya / L. A. Kalinichenko // SUBD. – 1996. – №1. – S. 102–109.

[14] Object-Oriented Database System Manifesto / M. Atkinson, F. Bancilhon , D. DeWitt and other // Proc. 1st Int. Conf. Deductive and Object-Oriented Databases. – Kyoto, Japan, 1989. – P. 40–57.

[15] The object database standard: ODMG – 93 / [Ed. by R. G.G. Cattell]. – Burlington, USA: Morgan Kaufmann Publ., 1994. – 169 p.
[16] The object data standard: ODMG 3.0. / [Ed. by R.G.G. Cattel, Douglas K. Barry]. – Burlington, USA: Morgan Kauffmann Publ., 2000. – 280 p.
[17] Tsikritzis D. Modeli dannykh / D. Tsikritzis, F. Lokhovski: per. s angl. – Moskva: Finansy i statistika, 1985. – 344 s.
[18] Abrial J. R. Data semantics / J. R. Abrial // Data Base Management: [Ed. by J. W. Klimbie and K. L. Koffeman]. – North-Holland, Amsterdam, 1974. – P. 1–59.
[19] Mylopoulos J. Information System Design at the Conceptual Level – the TAXIS Project / J. Mylopoulos, A. Borgida, S. Greenspan, H.K.T. Wong // IEEE Database Engineering Bulletin. – 1984. – Vol. 7. – № 4. – P. 4–9.
[20] Roussopoulos N. Using semantic networks for data base management / N. Roussopoulos, J. Mylopoulos // Proceedings of the 1st International Conference on Very Large Data Bases. – ACM. – 1975. – P. 144–172.
[21] Bubenko J. Data Models and their Semantics / J. Bubenko // Data Design. Infotech State of the Report Series. – 1980. – Vol. 8. – № 4. – P. 107–136.
[22] Langefors B. Infological model and information user views / B. Langefors // Information Systems. – 1980. – № 5. – P.17–32.
[23] Sundgren B. Conceptual foundation of the infological approach to data bases / B. Sundgren // Data Base Management: [Ed. by J. W. Klimbie and K. L. Koffeman]. – North-Holland, Amsterdam, 1974. – P. 61–96.
[24] Palagin A. V. Ontologicheskie metody i sredstva obrabotki predmetnykh znanii: monografiya / A. V. Palagin, S. L. Kryvyi, N. G. Petrenko. – Lugansk: Izd-vo VNU im. V. Dalya, 2012. – 323 s.
[25] Gruber T. R. A translation approach to portable ontology specifications / T. R. Gruber // Knowledge acquisition. – 1993. – Vol. 5. – № 2. – P. 199 – 220.
[26] Gruber T. R. Toward principles for the design of ontologies used for know ledge sharing / T. R. Gruber // International journal of human-computer studies. – 1995. – Vol. 43. – № 5. – P. 907–928.
[27] Guarino N. Formal Ontology and Information Systems / N. Guarino // Formal Ontology in Information Systems: Proceedings of FOIS'98, 6–8 June 1998, Trento, Italy. – Amsterdam: IOS Press, 1998. – P. 3–15.
[28] Codd E. F. A relational model of data for large shared data banks / E. F. Codd // Communications of the ACM. – 1970. – Vol. 13. – № 6. – P. 377–387.
[29] Codd E. F. Extending the database relational model to capture more meaning / E. F. Codd // ACM Transactions on Database Systems (TODS). – 1979. – Vol. 4. – № 4. – P. 397–434.
[30] Kogalovskii M. R. Sistemy dostupa k dannym, osnovannye na ontologiyakh / M. R. Kogalovskii // Programmirovanie. – 2012. – № 4. – S. 55–77.
[31] Kogalovskii M. R. Kontseptual'noe modelirovanie v tekhnologiyakh baz dannykh i ontologicheskie modeli / M. R. Kogalovskii, L. A. Kalinichenko // Ontologicheskoe modelirovanie: trudy simpoziuma. – Moskva : IPI RAN, 2008. – S. 114–148.
[32] Pospelov D. A. Situatsionnoe upravlenie: teoriya i praktika / D. A. Pospelov. – Moskva : Nauka; Gl. red. fiz.-mat. lit., 1986. – 288 s.
[33] Lukashevich N. V. Tezaurusy v zadachakh informatsionnogo poiska / N. V. Lukashevich. – Moskva: Izdatel'stvo Moskovskogo universiteta, 2011. – 512 s.
[34] Kuznetsov S. D. Osnovy baz dannykh / S. D. Kuznetsov. – Moskva: Internet-Universitet Informatsionnykh Tekhnologii; BINOM. Laboratoriya znanii, 2007. – 484 s.
[35] Tal'khaim B. Obzor semanticheskikh ogranichenii dlya modelei baz dannykh / B. Tal'khaim [Elektronnyi resurs]. – Rezhim dostupa : www.intsys.msu.ru/magazine/archive/v3(3.../thalheim-307-351.pdf. – Zagl. s ekrana.
[36] Date C. J. An Introduction to Database Systems / C. J. Date: [8th Edition]. – Pearson: Addison-Wesley, 2004. – XXVII, 983, I – 22 p.
[37] Esin V. I. Yazyk dlya universal'noi modeli dannykh / V. I. Esin, M. V. Esina // Systemy obrobky informacii'. – 2011. – № 5(95). – S. 193–197.
[38] Esin V. I. Yazyk opisaniya i manipulirovaniya dannymi, khranyashchimisya v BD s UMD / V. I. Esin, M. V. Esina // Komp'yuternoe modelirovanie v naukoemkikh tekhnologiyakh (KMNT-2010): tezisy dokl. mezhdunar. nauch.-tekhn. konf., 18-21 maya 2010 g. – Khar'kov: Khar'kovskii natsional'nyi universitet im. V.N. Karazina, 2010. – Chast' 2. – S. 104–108.

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

Received: June 2017

Authors:
V. Yesin, Doctor of Sciences (Engineering), Department of Information Systems and Technologies Security, V.N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: v.i.yesin@karazin.ua

The data model "object-event": requirements and synthesis of the model.

Abstract. Requirements imposed to the developed data model are formulated based on the need to find new solutions of the actual problem of timely creation, modernization within the planned budget of databases that have the required qualities. The data model, called "object-event", is synthesized in accordance with the formulated requirements and the general approach to the problem of semantic modeling proposed by C. Date.

Key words: data model, semantic (conceptual) modeling, database.

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

Надійшло: Червень 2017.

Автори:
Віталій Єсін, д.т.н., каф. безпеки інформаційних систем і технологій, Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: v.i.yesin@karazin.ua

Модель даних «об'єкт-подія»: вимоги та синтез моделі.

Анотація. Виходячи з необхідності знаходження нових рішень актуальної задачі своєчасного створення, модернізації в рамках запланованого бюджету баз даних, що володіють необхідними якостями, формулюються вимоги, що висуваються до розроблюваної моделі даних. Відповідно до сформульованих вимог і загального підходу до проблеми семантичного моделювання, запропонованого К. Дейтом, синтезується модель даних, що отримала назву – «об'єкт-подія».

Ключові слова: модель даних, семантичне (концептуальне) моделювання, база даних.

UDC 004 056 55

RESEARCH OF USAGE POSSIBILITY AND POST-QUANTUM ALGORITHMS ADVANTAGES DEPEND ON APPLICATION CONDITIONS

Ivan Gorbenko, Vladimir Ponomar, Marina Yesina

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

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

Received on June 2017

Abstract: *We established the need for comparative analysis and evaluation of the possibility to use asymmetric post-quantum cryptographic mechanisms. In order to compare, a procedure for evaluation was selected based on integral assessments of unconditional and conditional criteria. An analysis was conducted among the algorithms that fulfilled general unconditional criteria. As conditional criteria, we chose numerical characteristics of algorithms. In addition, additional unconditional criteria were put forward that differed depending on the conditions of use. The relevance of present research is associated with the emergence of a quantum computer. Previous studies have already proved that the existing cryptographic algorithms are vulnerable to the methods of quantum cryptanalysis. That is why, at present, leading organizations in the standardization of crypto algorithms conduct research and comparisons for selecting the post-quantum standard of cryptography. As a result of present research, we found a lack of a universal post-quantum cryptographic algorithm. It is proposed to separate three variants in the application of post-quantum algorithms: for lightweight cryptography, for the use by standard automated systems and use in a cloud-based environment. For all conditions of use, a separate evaluation of benefits in the cryptographic algorithms was carried out. Deficiencies in the leading candidate were detected. That is why the recommendations were given to employ these algorithms as the basic ones in the transition period. And, if the suspicion is confirmed, then we proposed alternatives. Results of present research allow us to understand current state in the development of post-quantum crypto algorithms and to predict their possible further development. The practical value of the research consists in obtaining the evaluation for post-quantum algorithms, depending on the conditions of their application.*

Keywords: *post-quantum cryptographic algorithms, comparative assessment of crypto algorithms, comparison criteria of crypto algorithms.*

1 Introduction

Due to the development of technologies for quantum computing and the introduction of quantum computer, there is a threat to the current state of protection of cryptographic systems with a public key [1]. With an advent of quantum computer that would have the volume of register required for the methods of quantum cryptanalysis, the stability of existing crypto algorithms will significantly degrade [2, 3]. This necessitates the creation of algorithms resistant to the methods of quantum cryptanalysis. The European project "New European Schemes for Signatures, Integrity, and Encryptions " (NESSIE) and the National Institute of Standards and Technologies (NIST) of the USA announced a start of recruiting the applicants for the contest of post-quantum algorithms whose standards are planned to be adopted over 2020–2022 [4,5].

A peculiarity of this task is that the contest will accept the algorithms whose cryptographic transformations are based on the latest information or insufficiently tested mathematical methods that will require considerable time to prove their stability in terms of quantum cryptanalysis. That is why the choice of the new standard will affect not only the algorithm that will be employed but also further development of the post-quantum cryptography.

Another feature is that the universal algorithms are lacking that can be used both for electronic signature (ES) and the encryption. Therefore, it is necessary for each of the security services to select its particular algorithm. A possible exception is the use of isogenies by the Jao-Soukharev algorithm, but a special feature of the ES mechanism by this algorithm is that it requires interactivity and full trust from a third party [6].

A relevant task is the comparative analysis and evaluation of a possibility to use the post-quantum mechanisms, which are represented by the algorithms that already exist, depending on the

conditions of applying them. At present, only the possibility of using the appropriate crypto transformations over a post-quantum period is being examined, but the analysis of advantages of one over another has not been run yet. In addition, it is necessary to evaluate the very possibility to use such algorithms taking into account those constraints that are imposed by the existing information systems.

2 Literature review and problem statement

As a confirmation of necessity to develop the post-quantum algorithms, article [1] should be brought here. It notes that in August 2015, the National Security Agency (NSA) of the US Government came up with a broad statement about the need for devising the standards for post-quantum cryptography. This article analyzed the risk of applying quantum computers for modern crypto algorithms and proposed the mechanisms for crypto transformations that are resistant to the cryptanalysis of different types (Table 1).

Table 1 – Types of crypto transformations that are resistant to quantum cryptanalysis

Lattice-based primitives	Cryptographic resistance (protection) depends on the complexity of solving the equation on algebraic grids
Multivariate primitives	Cryptographic resistance (protection) depends on the complexity of solving a system of multivariate polynomial equations
Code-based primitives	Cryptographic resistance (protection) depends on the complexity of fulfilling the task on decoding a linear code
Hash-based primitives	Cryptographic resistance (protection) depends on the complexity of finding collisions or prototypes in the cryptographic hash-functions
Isogeny-based key primitives	Cryptographic resistance (protection) depends on the complexity of finding an unknown isogeny between a pair of supersingular elliptic curves

The algorithms given in Table 2 were proposed by the task force of the European Telecommunications Standards Institute (ETSI) [5] for further research and study as possible candidates for quantum-protected algorithms.

Table 2 – List of post-quantum algorithms and their characteristics, proposed by ETSI

Type	**Scheme**	**Resistance** [bits]	**Public key** [bytes]	**Signature** [bytes]
Lattice	Lyubashevsky	–	1 664	2 560
	NTRU-MLS	128	988	988
	Aguilar et al	128	1 082	1 894
	Guneysu te al	80	1 472	1 120
	BLISS	128	896	640
	Ducas et al	80	320	320
	HIMMO	128	32	-----
MQ	Quartz	80	72 237	16
	Ding	123	142 576	21
	UOV	128	413 145	135
	Cyclic-UOV	128	60 840	135
	Rainbow	128	139 363	79
	Cyclic-Rainbow	128	48 411	79

Each of the quantum-resistant types of cryptographic transformations is under examination and there are already algorithms for ES and directed encryption (DE or E2EE) that are based on these transformations [5-7]. There are preliminary results of comparing these algorithms to the existing standardized ones [7].

Continuation of Table 2

Type	Scheme	Resistance [bits]	Public key [bytes]	Signature [bytes]
Code	Parallel-CFS	120	503 316 480	108
	Cayrel et al	128	10 920	47 248
	Cyclic-Cayrel et al	128	208	47 248
	RankSign	130	7 200	1 080
	Cyclic RankSign	130	3 538	1 080
Hash	Merkle	128	32	1 731
	Leighton-Micali	128	20	668
	XMSS	256	64	8 392
	SPHINCS	256	1 056	41 000
Isogeny	Jao-Soukharev	128	768	1 280
	Sun-Tian-Wang	128	768	16

An analysis of scientific literature [1, 4-7] revealed that comparisons between potentially possible post-quantum mechanisms are still lacking, as well as information about the possibilities of their use depending on the conditions and the environment. At the same time, it is the choice of the most promising cryptographic transformations for the post quantum application, which is extremely important, as it defines future direction in the development of cryptography – asymmetric cryptography.

At [5-7] note that post-quantum algorithms, compared with others, in addition to the resistance to quantum cryptanalysis, demonstrate other advantages, as well as shortcomings. Thus, the algorithms based on multivariate transformations have a very small size of the signature. However, in contrast, for the required stability they demand key data of such large size that it makes their widespread use and application problematic. The algorithms based on the use of algebraic codes display a similar flaw, but their benefit is high performance speed.

The disadvantage of algorithms based on hashes is the large size of the crypto transformation result. In addition, to reduce the threat of attack of the "replay" type, additional information must be stored together with a private key.

The disadvantage of using algorithms based on elliptic curves isogenies is the high complexity in crypto transformations.

However [5-7] do not focus on these shortcomings. There is no analysis for a possibility to employ algorithms with such properties into existing systems. And there is no analysis of their advantages and shortcomings in comparison to other post-quantum algorithms. Nevertheless, this very analysis is particularly important. Since the need for a standard post-quantum asymmetric algorithm has been already defined [1, 4-5], it is necessary to choose the most suitable one to the requirements of the existing information systems.

3 The aim and tasks of the research

The aim of present research is to evaluate and to conduct comparative analysis of the existing methods for post-quantum crypto transformations of algorithms depending on the requirements put forward and conditions for their application. This will allow us, first, to select the algorithms that are most likely to become future post-quantum standards, second, to predict the future direction in the development of asymmetric cryptography.

To achieve the set aim, we solved the following tasks in the course of research:

– to select a technique, which will enable conducting an assessment and comparative analysis of post-quantum algorithms depending on the requirements put forward and conditions of application;

– to choose and analyze methods and algorithms that are based on different mathematical methods but meet unconditional (basic) requirements put forward to the candidates for post-quantum

standards (proved correctness and resistance, tested protection, exact assessment of parameters and complexity of implementation);

– to make up proposals and recommendations regarding the use of the examined algorithms when adopting the post-quantum standards of asymmetric crypto transformations.

4 Materials and methods for examining a possibility and advantages of using post-quantum algorithms depending on conditions

4.1 Substantiation of the choice of technique for comparing the cryptographic algorithms

One of the most important issues in the process of holding a contest is the application of objective methods and technique for the evaluation and comparative analysis of cryptographic primitives. Paper [8] described methods and techniques for comparative analysis of symmetric and asymmetric crypto primitives. They are based on the system of unconditional and conditional partial and integral criteria, as well as indicators that allow assessment of the degree of satisfying the requirements put forward to a candidate. The main task of such techniques is [8-10]:

– formalization of decision-making processes regarding the execution of requirements put forward to them;

– consideration of advantages and shortcomings in the cryptographic primitives that are candidates for the post-quantum standard;

– reducing the impact of subjective factors on decision making.

Under the criterion we shall understand an attribute, based on which the assessment is made, or determining or categorization of anything, that is, in essence, we shall understand it as an evaluation measure.

Previous studies [7,10] allowed drawing a conclusion that the comparison of cryptographic primitives can be carried out using two clusters of criteria: unconditional and conditional. This approach makes it possible to assess and compare those crypto transformations that are the candidates in 2 stages. This approach is based as well on accounting for or utilizing the expert evaluations.

At the first stage, they verify the appropriateness of crypto transformation for the system of partial unconditional criteria, and then for each crypto primitive, based on the partial ones, an unconditional integral criterion is computed.

At the second stage they receive appropriate assessments using first the system of partial conditional criteria, and then, based on them, an integral conditional criterion is calculated. The application of partial conditional criteria, and then, based on them, of integral conditional criterion, allow obtaining a more accurate estimate. Such assessment is obtained from the normalization of overall estimates of characteristics of crypto transformations and makes it possible to compare crypto primitives, which are the candidates for a post-quantum algorithm.

4.2 Examining the mechanisms of cryptographic transformations by the totality of unconditional criteria

It is by using the unconditional and conditional criteria that it becomes possible to compare different cryptographic transformations by the integral conditional and general criteria.

Further, by the conformity of one or another mechanism to the unconditional criteria we shall understand that expert assessments by the unconditional criteria are positive, in other words, they are satisfied unequivocally. We shall assign to the unconditional criteria those criteria whose fulfillment for cryptographic transformations is compulsory, that is, unconditional.

Thus, under condition of positive assessment by the integral unconditional criterion, further comparison and evaluation can be carried out based on determining and comparing the conditional criteria and an integral conditional criterion.

The general unconditional criteria are:

$W_{\delta 1}$ – reliability of mathematical base that is used in the cryptographic transformations;

$W_{\delta 2}$ – practical protection of cryptographic transformations from known quantum attacks;

$W_{\delta 3}$ – real protection from all known and potentially possible cryptanalytic attacks;

$W_{\delta 4}$ – statistical safety of cryptographic transformation;

$W_{\delta 5}$ – theoretical protection of cryptographic transformation;

$W_{\delta 6}$ – absence of weak private keys for cryptographic transformation or the existence of a proven mechanism to identify/verify such keys;

$W_{\delta 7}$ – complexity of direct and inverse cryptographic transformations regarding ES does not exceed a polynomial character.

1. Under the reliability of mathematical base, we shall understand practical absence of intruder's capabilities to carry out attacks of the "universal disclosure" type due to the imperfection of mathematical apparatus that is used, or weaknesses that can be predetermined by the specific properties of general parameters and keys. In this case, the criterion for estimating the reliability of mathematical base is the fact that the complexity of the attack "universal disclosure" is exponential in nature, and the criterion of unreliability is the subexponential or polynomial complexity.

2. Under the practical protection of crypto transformations, we shall understand protection from power and analytic attacks, which is achieved by selecting the size of general parameters and keys, as well as the means for their generation. In other words, the criterion of practical protection of crypto transformations is determined by a dependence of the complexity of attack on the size of general parameters and keys. There must exist such parameters, for which complexity of the attack considerably (*by the required number of orders*) exceeds the existing capacity of cryptanalytic systems in the technologically advanced states (*third level offender*). Including those that take into account a forecast for increase in the capacity of cryptanalytic systems due to the development of mathematical provision and software, as well as hardware and software means. In the present study, we considered future application of the means based on quantum computing. Since the emergence of such means necessitates introduction of new cryptographic algorithms.

3. Real protection from all known and potentially possible cryptanalytic attacks. Such protection refers to the fact that all known cryptanalytic attacks of the "full disclosure" type have exponential complexity. And the criterion of vulnerability – subexponential and lower character of complexity of the attack "full disclosure".

4. Statistical safety of cryptographic transformation, which we shall understand as a statistical independence of the result of cryptographic transformation from the input block that is encrypted (EP-signed), and a private key that is used.

5. Theoretical protection of cryptographic transformation. A crypto transformation is estimated when using general parameters with the appropriate properties and lengths. There should not exist (*unidentified*) theoretical analytical attacks whose complexity is lower than the complexity of attack of the "full disclosure" type.

6. Absence of weak key pairs, including private keys. Weak keys are the keys with which complexity of cryptanalytic attacks of the "full disclosure" and "universal disclosure" types is lower than the complexity of attack "full disclosure" for other (*not weak*) private keys. It is allowed to accept a mechanism, which has weak key pairs, but the probability of their generation is low and there is a proven algorithm for the validation of key pair on weakness of (*if all such key pairs have been already discovered*).

7. A complexity of the direct and inverse cryptographic transformations, as well as the generation or deployment of keys, has a polynomial character and does not exceed permissible magnitudes.

When using the given unconditional criteria, we chose the following algorithms (Table 3) under condition of applying the following parameters (*minimum values*) [7,8,10]:

1) $I_{res.}$ – cryptographic resistance;

2) $l_{pub.k.}$ – length of the public key;

3) $l_{pr.k.}$ – length of private key;

4) $l_{t.res.}$ – length of the result of cryptotransformation;

5) $T_{dir.}$ – speed of direct crypto transformation;

6) $T_{inv.}$ – speed of inverse crypto transformation.

Characteristics of algorithms from this Table. Among these algorithms, Jao-Soukharev is

highlighted because it can be used both for the encryption and for ES, but a signature requires interactivity.

Table 3 – Comparison of characteristics of post-quantum algorithms

Algorithms	$\mathbf{I_{res.}}$	$\mathbf{l_{pub.k.}}$	$\mathbf{l_{pr.k.}}$	$\mathbf{l_{t.res.}}$	$\mathbf{T_{dir.}}$	$\mathbf{T_{inv..}}$
NTRU	128	988	256	988	0,5	0,02
BLISS	128	896	256	640	0,02	0,01
Quartz	80	72237	3000	16	2	0,05
XMSS	128	1700	280	2048	2	0,2
SPHINCS	128	1024	1024	41000	0,5	0,02
RankSign	130	7200	21600	1080	0,02	0,02
Jao-Soukharev	128	768	768	1280	5	5

Note: Cryptographic resistance is given in bits, data size in bytes, and the speed of transformations in the form of coefficient relative to the speed of the corresponding transformation of the RSA algorithm with a key length of 4096 bits.

Among the indicated algorithms, we used a comparison by the unconditional criteria for various areas of application. The criteria are:

W_{s1} – $l_{pub.k.}$ – length of the public key;

W_{s2} – $l_{pr.k.}$ – length of private key;

W_{s3} – $l_{t.res.}$ – length of the result of crypto transformation;

W_{s4} – interactivity of algorithm.

These criteria are different for the following cases:

1) Lightweight cryptography is due to the use of smart cards, hardware electronic keys. A peculiarity of lightweight cryptography is:

– limited amount of internal storage;

– low computing capacities for satisfying which it is possible to reduce resistance;

– the use in combination with an extensive system of another type (such as an object of multifactor authentication in the internal network).

The criteria are:

W_{s1} – $l_{pub.k.}$ <=2048;

W_{s2} – $l_{pr.k.}$<=768;

W_{s3} – $l_{t.res.}$<=2048;

W_{s4} – interactivity is prohibited.

2) Cryptography in the standard automated systems (AS). Compared to the lightweight cryptography, the requirements to the size of the key data are reduced while requirements for resistance are increased. However, at the same time, such AS can be employed as servers. This predetermines a large amount of concurrent operations and storing, accordingly, a large volume of public-key certificates *(that includes a public key and its signature by the key of the certificate authority (CA))*. The criteria are:

W_{s1} – $l_{pub.k.}$ <=8192;

W_{s2} – $l_{pr.k.}$<=2048;

W_{s3} – $l_{t.res.}$<=8192;

W_{s4} – interactivity is prohibited.

3) Cryptography in a cloud-based environment:

Special conditional criteria are absent, that is, all algorithms from Table 3 can be applied.

Evaluation of the potential to use crypto transformation W_s under these conditions can be represented in the form:

$$W_s = W_{s1} \wedge W_{s2} \wedge W_{s3} \wedge W_{s4}. \quad (1)$$

Tables 4 and 5 give the results of comparing the crypto algorithms by formula (1) for the conditions of applying in lightweight cryptography and standard AS, respectively.

Table 4 – Conformity of algorithms to the unconditional criteria of light cryptography

Criterion / Algorithm	W_{s1}	W_{s2}	W_{s3}	W_{s4}	W_s
NTRU	1	1	1	1	1
BLISS	1	1	1	1	1
Quartz	0	0	1	1	0
XMSS	1	1	1	1	1
SPHINCS	1	0	0	1	0
RankSign	0	0	1	1	0
Jao-Soukharev DH	1	1	1	1	1
Jao-Soukharev Sign	1	1	1	0	0

Table 5 – Conformity of algorithms to the unconditional criteria of cryptography for standard AS

Criterion / Algorithm	W_{s1}	W_{s2}	W_{s3}	W_{s4}	W_s
NTRU	1	1	1	1	1
BLISS	1	1	1	1	1
Quartz	0	0	1	1	0
XMSS	1	1	1	1	1
SPHINCS	1	1	0	1	0
RankSign	1	0	1	1	0
Jao-Soukharev DH	1	1	1	1	1
Jao-Soukharev Sign	1	1	1	0	0

That is, for the conditions of light cryptography and cryptography of standard AS, we shall compare algorithms for ES BLISS and XMSS and the encryption algorithms NTRU and the Diffie-Hellman scheme for the Jao-Soukharev algorithm.

4.3 Examining the mechanisms of cryptographic transformations by the totality of conditional criteria

Studies have demonstrated that qualitative and quantitative comparison of cryptographic transformations can be conducted using a generalized conditional benefit criterion or an integral conditional criterion [10,11].

As the basic partial conditional criteria, it is proposed to use numerical characteristics of the algorithms that are listed in Table 3.

When applying the chosen partial conditional criteria, it is important to select a method for the convolution of partial conditional criteria into a conditional integral criterion.

Conducted analysis, as well as practical study, has demonstrated that as the methods for the convolution of partial conditional criteria, it is possible to choose the hierarchy analysis method based on pairwise comparisons and the ranking method.

When using the hierarchy analysis method based on pairwise comparisons, the obtained judgments are expressed by integers. These numbers *(ratings)* are selected by a 9-point scale *(Table 6, in the explanation column: interpretation of the score in our comparison is recorded)*. The validity of this scale is proved theoretically when compared to many other scales. When using the specified relation scale, comparing two objects in the sense of achieving the goal, which is located at the highest level of hierarchy. It is necessary to match this comparison with a number in the interval between 1 and 9, or the inverse value of numbers.

Table 6 – Scale of expert estimations of the pairwise comparison method

Degree of significance	Definition	Explanation
1	Equal significance	Two characteristics have the same significance.
3	Some advantage of one action over another (weak significance)	Characteristic in the numerical value is 2 times better, has some advantage qualitatively
5	Essential or strong significance	Characteristic in the numerical value is 4 times better, has a distinct advantage qualitatively
7	Obvious or very strong significance	Characteristic in the numerical value is 32 times better, has a considerable advantage qualitatively
9	Absolute significance	Characteristic in the numerical value is more than 32 times better, the other characteristic can be neglected qualitatively
2, 4, 6, 8	Intermediate values between two adjacent judgments	The situation needs a compromise solution
Inverse magnitudes of the non-zero magnitudes shown above	If action i when compared to j is assigned with one of the non-zero numbers defined above, then action j when compared to action is assigned with the inverse value	If the coherence was postulated when obtaining N numeric values for the formation of matrix

Thus, a comparison of cryptographic transformations can be carried out by using a generalized conditional benefit criteria or a conditional integral criterion. In this case, as the methods for the convolution of partial conditional criteria, one may choose the hierarchy analysis method based on pairwise comparisons and the ranking method.

Since the algorithms are compared by the determined numeric characteristics, then it is possible by the scale from Table 6 to receive their accurate assessment. However, determining the significance of each characteristic for the selected conditions cannot be performed with the same accuracy as determining the weight coefficients has a qualitative character. Therefore, in order to determine them, it is necessary to apply the method of expert evaluations [12].

4.4 Methods of expert evaluation

The expert evaluations are understood as a complex of logical and mathematical procedures aimed at obtaining information from specialists, its analysis and generalization in order to prepare and develop rational decisions [12].

Methods of expert evaluations are the methods for organizing work with specialists-experts and processing of expert opinions.

The essence of methods of expert evaluations – underlying the decision made, or forecast, or opinion, is the specialist's opinion or of a team of experts, based on their knowledge and practical professional experience.

Stages of expert evaluation [12]:

1) statement of purpose of the research;
2) selection of form of research, defining the budget of project;
3) preparation of information materials, forms, moderator of the procedure;
4) selection of experts;
5) conducting the survey;
6) analysis of results *(processing expert assessments)*;

7) preparation of the report with results of the expert evaluation.

There are the following methods of expert evaluations *(ways to work out both collective and individual expert assessments)*:

− method of association: based on studying the object similar in properties with another object;

− method of pairwise comparisons: based on the comparison by an expert of alternative choices among which the most significant is to be chosen;

− method of benefit vectors: an expert analyses the whole set of alternatives, chooses the most significant;

− method of focal objects: based on assigning the attributes of randomly selected analogues to the examined object;

− individual expert survey: a survey in the form of an interview in the form of analysis of expert assessments;

− the midpoint method: two alternative variants of solution are stated, one of which has a lower benefit. After that, the expert has to select a third alternative variant whose estimate is between the values of the first and second alternatives;

− method of simple ranking: each expert should position the attributes in order of benefits;

− method for assigning the weighting coefficients: all attributes are assigned with certain weighting coefficients;

− method of sequential comparisons (all the attributes are arranged by the decrease in their significance; the first attribute is assigned with value 1, others are assigned with weighting coefficients in fractions of a unity; the value of the first attribute is compared to the sum of all of the subsequent ones);

− method of assigning the points: experts, depending on the significance of the indicator *(attribute)* assign points (0–10), and are permitted to evaluate the significance of the indicator in decimal values, as well as different indicators can be assigned with equal points.

Common opinion displays a larger accuracy than the individual opinions of each of the experts. This method is used to obtain quantitative estimates of qualitative characteristics and properties.

Thus, there are collective and individual expert assessments. As far as each of the groups of scores is concerned, there are appropriate methods for defining such estimates. The given methods are selected according to the conditions of evaluation, degree of complexity and the required accuracy of assessment, etc. Each of the methods has also its own advantages and shortcomings.

In the case when all characteristics of the cryptographic algorithms have a precise numeric value, the role of experts is to determine the weighting coefficients of the significance of characteristics. These coefficients vary depending on the area of application. That is why the chosen experts were specialists in their relevant fields.

4.5 Establishing a degree of coherence among expert opinions

If several experts participate in a survey, then the differences in their assessments are unavoidable, however, the magnitude of such discrepancy is important. Group evaluation can be considered sufficiently reliable only under condition of a good degree of coherence among the responses from individual experts [12].

For the analysis of variability and coherence in the assessments, they apply statistical characteristics – a measure of spread or statistical variance.

The means of computing a measure of spread:

1) Variance spread:

$$R = x_{\max} - x_{\min},$$

where x_{max}, x_{min} are the maximal and minimal value of indicator (attribute), respectively.

2) Mean linear deviation:

$$a = \frac{1}{n}\sum_{i=1}^{n}\left|x_i - \bar{x}\right|,$$

where n is the number of expert estimates of characteristic *(number of experts)*, x_i is the estimate of the *i*-th expert, i=1,..., n, $\bar{x}$ is the mean value of estimate of characteristic.

3) The root mean square deviation:

$$\sigma = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})^2}.$$

4) Dispersion:

$$\sigma^2 = \frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})^2.$$

As a reliability measure of the degree of reliability of a given survey, the method of pairwise comparisons employs the values of variation in the estimates of a characteristic:

$$\beta_j = \frac{\sigma_j}{\bar{x}_j},$$

where σ_j is the root mean square deviation of the *j*-th characteristic, $\overline{x_j}$ is the mean value of assessment of the *j*-th characteristic. The closer a variance coefficient to zero, the more coherent experts' estimates are. If the value of variance is larger than 0,33, the opinion of experts is considered to be unsatisfactorily coherent, 0,17 - 0,33 – satisfactorily coherent, 0,17 – coherent enough. The total variance (that is, coherence among the assessments of all characteristics) can be selected by the maximax criterion – maximum value of the variance. Another variant is to perform the evaluation for the variance of variance, that is, to repeat calculations, but, instead of the values of estimates, to apply the values of variance.

For the method of pairwise comparisons, the mean value of a characteristic's estimate will become a weight coefficient for this characteristic.

For the ranking method, they use a different method to evaluate coherence among the opinions of experts – a method for determining the coefficient of concordance:

1) d experts estimate n attributes by the ranking method, r_{ij} is the estimate of the *i*-th attribute by the *j*-th expert.

2) the sum of ranks of the attribute is determined:

$$r_{is} = \sum_{j=1}^{d} r_{ij}, \quad i = \overline{1,n.}$$

3) the average sum of the ranks is determined:

$$\bar{r}_s = \frac{1}{n}\sum_{i=1}^{n} r_{is}.$$

4) the coefficient of deviation is determined:

$$S = \sum_{i=1}^{n}(r_{is} - \bar{r}_s)^2.$$

5) the coefficient of concordance is determined:

$$W = \frac{12}{d^2(n^3 - n)}S.$$

The closer coefficient of concordance to 1, the more coherent is the opinion of experts. It is believed that at W > 0,5, the coherence of opinions is satisfactory.

4.6 The hierarchy analysis method based on pairwise comparisons and the peculiarities of its application for the evaluation of algorithms

In order to apply the hierarchy analysis method, it is necessary to select a system of conditional criteria. By using such a set of indicators, by applying the conditional criteria, it is possible to calculate the values of integral conditional criterion and, as a consequence, to compare cryptographic algorithms by the conditional integral criterion [8,10,12].

The method for pairwise comparison of elements can be described in the following way. We construct a set of matrices of paired comparisons. Paired comparisons are represented in terms of dominance of one element over another. At pairwise comparison, expert compares examined objects by their significance in pairs, establishing the most important in each pair of objects. All possible pairs of objects are represented by an expert in the form of record of each of the combinations (object 1 – object 2, object 2 – object 3, etc.) or in the form of a matrix. The method of pairwise comparisons is very simple and allows examining a larger number of objects (in comparison, for example, with the ranking method) and with a better accuracy.

Assume E_1, E_2,... ,E_n is the multitude of n elements (*alternatives*) and v_1 ,v_2,..., v_n are, respectively, their weight or intensity. Let us compare in pairs the weight, or intensity, of each element to the weight, or intensity, of any other element in the set relative to a property or goal common to them (*relative to the element "father"*). In this case, the matrix of pairwise comparisons [E] takes the form of Table 7.

Table 7 – Representation of matrix of pairwise comparisons

Criteria	**E_1**	**E_2**	**…**	**E_n**
E_1	ν_1 / ν_1	ν_1 / ν_2	…	ν_1 / ν_n
E_2	ν_2 / ν_1	ν_2 / ν_2	…	ν_2 / ν_n
…	…	…	…	…
E_n	ν_n / ν_1	ν_n / ν_2	…	ν_n / ν_n

The matrix of pairwise comparisons has a property of inverse symmetry, that is, $a_{ij}=1/a_{ji}$, where $a_{ij}=v_i/v_j$. When conducting the pairwise comparisons, one should answer the following questions: which of the two compared elements is more important or exerts a larger influence, which is more probable and which has a larger benefit. When comparing the criteria, they usually ask which of the criteria is more important; when comparing the alternatives relative to the criteria – which of the alternatives has a larger benefit, or is more likely. When constructing a matrix of pairwise comparisons for all criteria, it is necessary to determine a relation of coherence for each of the criteria in the following way. The estimate of component of the natural vector will be calculated by formula (2):

$$q_i = (W_{yi} \times W_{yi+1} \times \ldots \times W_{yn})^{\frac{1}{n}}. \quad (2)$$

The normalized estimate of the priority vector will be calculated by formula (3):

$$r_i = q_i \div z, \quad (3)$$

where z is the ratio of consistency of the matrix, which is calculated by expression (4):

$$z = \sum_{i=1}^{n} q_i. \quad (4)$$

The value of relation in the consistency of the matrix is in the range of $[0, \sum_{i=1}^{n} q_{i\max}]$, where $q_{i\max}$ is the maximal possible value of the estimate of component of the natural vector for the chosen case. Therefore, the hierarchy analysis method based on the pairwise comparisons demonstrates both advantages and disadvantages. The main shortcoming is a sufficiently strong influence of the subjective opinion of an expert on the outcome of the assessment. One of the benefits is a simple mathematical apparatus used.

4.7 Methods for determining the weight coefficients

In the case, when get information about parameters comparable systems importance using informal methods is not possible, necessary to use formalized methods. Among them are methods based on determining the weight indices. Let us consider the general problem formulation for cryptographic primitives evaluation technique based on the determining the weight indices method. Let there are:

1) *k* systems *(cryptoprimitives)*, which is necessary to evaluate;
2) *m* indicators, according to which systems are evaluated;
3) *n* experts, that carry out the evaluation.

For the evaluation, you can use the following weight indices determining methods: using the Fishburn scale; based on the ranking method; based on the points attribution method; based on the numerical method. Let us consider these methods more detail hereafter. The cryptographic primitives estimation in this article are done only with using method for determining the weight coefficients based on the ranking method and hierarchy analysis method based on pairwise comparisons.

4.7.1 Method for determining the weight coefficients using the Fishburn scale

Let we have *m* indicators and *n* experts, that estimate the importance of these indicators for some system. To each indicator x_i, $i = 1,...,m$ the estimate of their importance is put on accordance. After that the weight system are built by the next way

$$\begin{cases} \sum_{i=1}^{m} a_i = 1, \\ a_i \geq 0, i = 1,....,m \end{cases}, \quad (5)$$

where a_i – i-th indicator weight; i – indicator number; m – indicators amount. Indicators are ranging by the significance increasing: $x_1 \succ x_2 \succ x_3 \succ ... \succ x_i \succ ... \succ x_m$.

Let we define weight indices by using the Fishburn scale:

$$a_i = \frac{2 \cdot (m - i + 1)}{m \cdot (m + 1)}. \quad (6)$$

Values of weight indices and their average value are brought under the table (Table 8).

$\overline{a_i}$ – average value of weight indices for i-th indicator; $w_i = \overline{a_i}$ – weight indices values.

Table 8 – Weight indices values and their average value

Indicators / Experts	x_1	x_2	...	x_m
1	a_{11}	a_{12}	...	a_{1m}
2	a_{21}	a_{22}	...	a_{2m}
...	...	...	...	...
n	a_{n1}	a_{n2}	...	a_{nm}
w_i	w_1	w_2	....	w_m

4.7.2 Method for determining the weight coefficients based on the ranking method

The ranking method – one builds a matrix of evaluations of the attributes by experts, where each expert assigns a rank to each attribute. Assume there is n of partial indicators and group of d experts who assess the significance of these indicators for a certain system. The most important indicator is matched by rank (*score*) n, the next one – by (n–1), etc.; the rank equal to 1 is the least important. Then, the weighting coefficients are determined by formula (7) [8-10]:

$$w_j = \frac{r_j}{\sum_{j=1}^{n} r_j}, \quad j = 1,...,n. \tag{7}$$

Table 9 – Table of expert estimates by the ranking method

Indicators / Experts	x_1	x_2	…	x_n
1	r_{11}	r_{12}	…	r_{1n}
2	r_{21}	r_{22}	…	r_{2n}
…	…	…	…	…
d	r_{d1}	r_{d2}	…	r_{dn}
$r_j = \sum_{i=1}^{n} r_{ij}$	r_1	r_2	…	r_n
w_j	w_1	w_2	….	w_n

Notes: x_n is the n-th indicator, r_j is the j-th rank (estimate), d is the number of experts, n is the number of indicators.

Results of a survey of experts are compiled in a table (Table 9). The penultimate line of this table contains a record of the sum of the ranks (*estimates*) that were assigned by the experts, and the last line of the table contains a record of values of weighting coefficients of the indicators.

4.7.3 Method for determining the weight coefficients based on the points attribution method

Let we have *m* indicators and *n* experts, that estimate the importance of these indicators for some system. Experts according to indicator significance put points from 0 to 10, herewith it's allow to estimate the importance of indicator by the fractional values, and also to the different indicators we can charge off similar points. After that it's defined weights of each indicator that is calculated by each expert:

$$r_{ij} = \frac{h_{ij}}{\sum_{j=1}^{m} h_{ij}}; \ \sum_{j=1}^{m} r_{ij} = 1, \tag{8}$$

where r_{ij} – weights of j-th indicator, that are defined by i-th expert; h_{ij} – point of i-th expert, that are put to the j-th indicator; *n* – amount of experts; *m* – amount of indicators.

All received data are brought under the table (Table 10). The finale weight indices of indicators are defined by the formula:

$$w_j = \frac{\sum_{i=1}^{n} r_{ij}}{\sum_{j=1}^{m}\sum_{i=1}^{n} r_{ij}}; \ \sum_{j=1}^{n} w_j = 1. \tag{9}$$

Besides experts estimates for define weight indices we can use some formal methods, which take into the consideration values of indicators itself.

Table 10 – Weight indices values

Indicators (j) / Experts (i)	x_1	x_2	…	x_m	$\sum_{j=1}^{m} h_{ij}$	Indicators weights			
						r_{i1}	r_{i2}	…	r_{im}
1	h_{11}	h_{12}	…	h_{1m}	$\sum_{j=1}^{m} h_{1j}$	$r_{11}=\frac{h_{11}}{\sum_{j=1}^{m} h_{1j}}$	$r_{12}=\frac{h_{12}}{\sum_{j=1}^{m} h_{1j}}$	…	$r_{1m}=\frac{h_{1m}}{\sum_{j=1}^{m} h_{1j}}$
2	h_{21}	h_{22}	…	h_{2m}	$\sum_{j=1}^{m} h_{2j}$	$r_{21}=\frac{h_{21}}{\sum_{j=1}^{m} h_{2j}}$	$r_{22}=\frac{h_{22}}{\sum_{j=1}^{m} h_{2j}}$	…	$r_{2m}=\frac{h_{2m}}{\sum_{j=1}^{m} h_{2j}}$
…	…	…	…	…	…	…	…	…	…
n	h_{n1}	h_{n2}	…	h_{nm}	$\sum_{j=1}^{m} h_{nj}$	$r_{n1}=\frac{h_{n1}}{\sum_{j=1}^{m} h_{nj}}$	$r_{n2}=\frac{h_{n2}}{\sum_{j=1}^{m} h_{nj}}$	…	$r_{nm}=\frac{h_{nm}}{\sum_{j=1}^{m} h_{nj}}$
					$\sum_{i=1}^{n} r_{ij}$	$r_1=\sum_{i=1}^{n} r_{i1}$	$r_2=\sum_{i=1}^{n} r_{i2}$	…	$r_m=\sum_{i=1}^{n} r_{im}$
					w_j	$w_1=\frac{r_1}{\sum_{j=1}^{m} r_j}$	$w_2=\frac{r_2}{\sum_{j=1}^{m} r_j}$	…	$w_m=\frac{r_m}{\sum_{j=1}^{m} r_j}$

4.7.4 Method for determining the weight coefficients based on the numerical method

For each indicator the coefficient of relative spreading is calculated by the formula:

$$\delta_i = \frac{x_{i\max} - x_{i\min}}{x_{i\max}}, \tag{10}$$

where $x_{i\max}$, $x_{i\min}$ – maximum and minimum values of i-th indicator accordingly, m – indicators amount.

Values of indicators itself can find by the any above mentioned methods. Weight indices take the greatest value for that indicators, which relative spreading are the most significant

$$w_i = \frac{\delta_i}{\sum_{i=1}^{m} \delta_i}. \tag{11}$$

All received data are brought under the table (Table 11).

Table 11 – Weight indices values

Indicators / Estimation	x_1	x_2	…	x_m
$x_{i\min}$	$x_{1\min}$	$x_{2\min}$	….	$x_{m\min}$
$x_{i\max}$	$x_{1\max}$	$x_{2\max}$	….	$x_{m\max}$
δ_i	δ_1	δ_2	….	δ_m
w_i	w_1	w_2	….	w_m

5 Results of examining the comparative evaluation of the application of post-quantum cryptographic algorithms

Table 12 gives the result of determining the weight coefficients by expert estimates for the mechanisms of ES for lightweight cryptography.

The level of consistency in the assessments is 0,156 that meets the requirements. After conducting evaluations of characteristics for the algorithms (Table 3) that were selected by unconditional criteria (Table 4), by the scale of Table 6, the BLISS algorithm has the level of 0,709, XMSS – 0,291.

Table 12 – Weight coefficients of the ES mechanisms criteria by expert estimates for lightweight cryptography by the method of pairwise comparisons

Indicators / Experts	$I_{res.}$	$l_{pub.k.}$	$l_{pr.k.}$	$l_{t.res.}$	$T_{dir.}$	$T_{inv..}$
1	0,235	0,124	0,235	0,124	0,235	0,045
2	0,218	0,096	0,286	0,129	0,218	0,053
3	0,242	0,084	0,242	0,135	0,242	0,056
4	0,264	0,098	0,264	0,137	0,186	0,050
5	0,275	0,092	0,275	0,155	0,155	0,047
W	0,247	0,099	0,260	0,136	0,207	0,050

Table 13 gives the result of determining the weight coefficients by expert estimates for the encryption mechanisms for lightweight cryptography.

The level of consistency in the assessments is 0,108 that meets the requirements. After conducting evaluations of characteristics for the algorithms (Table 3) that were selected by unconditional criteria (Table 4), by the scale of Table 6, the NTRU algorithm has the level of 0,704, Jao-Soukharev – 0,296.

Table 13 – Weight coefficients of the encryption mechanisms criteria by expert estimates for lightweight cryptography by the method of pairwise comparisons

Indicators / Experts	$I_{res.}$	$l_{pub.k.}$	$l_{pr.k.}$	$l_{t.res.}$	$T_{dir.}$	$T_{inv..}$
1	0,079	0,137	0,079	0,187	0,259	0,259
2	0,087	0,114	0,076	0,241	0,241	0,241
3	0,082	0,133	0,064	0,240	0,240	0,240
4	0,089	0,123	0,089	0,233	0,233	0,233
5	0,071	0,119	0,071	0,199	0,269	0,269
W	0,081	0,125	0,076	0,220	0,249	0,249

Table 14 gives the result of determining the weight coefficients by expert estimates of the ES mechanisms for the cryptography of standard AS. The level of consistency in the assessments is 0,310 that meets the requirements. After conducting evaluations of characteristics for the algorithms (Table 3) that were selected by unconditional criteria (Table 5), by the scale of Table 6, the BLISS algorithm has the level of 0,763, XMSS - 0,237.

Table 15 gives the result of determining the weight coefficients by expert estimates of the encryption mechanisms for the cryptography of standard AS.

The level of consistency in the assessments is 0,176 that meets the requirements. After conducting evaluations of characteristics for the algorithms (Table 3) that were selected by unconditional criteria (Table 5), by the scale of Table 6, the NTRU algorithm has the level of 0,705, Jao-Soukharev – 0,295.

Table 14 – Weight coefficients of the ES mechanisms criteria by expert estimates for the standard AS by the method of pairwise comparisons

Indicators / Experts	$I_{res.}$	$l_{pub.k.}$	$l_{pr.k.}$	$l_{t.res.}$	$T_{dir.}$	$T_{inv..}$
1	0,263	0,181	0,123	0,072	0,181	0,181
2	0,203	0,281	0,065	0,105	0,143	0,203
3	0,138	0,232	0,054	0,083	0,138	0,354
4	0,134	0,229	0,075	0,134	0,075	0,353
5	0,198	0,142	0,068	0,153	0,175	0,264
W	0,187	0,213	0,077	0,109	0,142	0,271

Table 15 – Weight coefficients of the encryption mechanisms criteria by expert estimates for the standard AS by the method of pairwise comparisons

Indicators / Experts	$I_{res.}$	$l_{pub.k.}$	$l_{pr.k.}$	$l_{t.res.}$	$T_{dir.}$	$T_{inv..}$
1	0,100	0,077	0,060	0,254	0,254	0,254
2	0,096	0,096	0,059	0,203	0,273	0,273
3	0,110	0,067	0,067	0,302	0,226	0,226
4	0,123	0,078	0,052	0,335	0,206	0,206
5	0,107	0,107	0,064	0,329	0,196	0,196
W	0,107	0,085	0,061	0,285	0,231	0,231

Table 16 gives the result of determining the weight coefficients by expert estimates of the ES mechanisms for the cryptography in a cloud-based environment.

The level of consistency in the assessments is 0,199 that meets the requirements. After conducting evaluation of characteristics for the algorithms (Table 3), by the scale of Table 6, the BLISS algorithm has the level of 0,267, RankSign – 0,218, Quartz – 0,158, SPHINKS – 0,154, XMSS – 0,123, Jao-Soukharev – 0,11.

Table 16 – Weight coefficients of the ES mechanisms criteria by expert estimates for clouds by the method of pairwise comparisons

Indicators / Experts	$I_{res.}$	$l_{pub.k.}$	$l_{pr.k.}$	$l_{t.res.}$	$T_{dir.}$	$T_{inv..}$
1	0,305	0,068	0,068	0,168	0,168	0,222
2	0,233	0,055	0,082	0,164	0,233	0,233
3	0,329	0,064	0,107	0,107	0,196	0,196
4	0,274	0,058	0,089	0,153	0,153	0,274
5	0,246	0,062	0,062	0,140	0,246	0,246
W	0,277	0,061	0,082	0,147	0,199	0,234

Table 17 gives the result of determining the weight coefficients by expert estimates of the encryption mechanisms for the cryptography in a cloud-based environment.

The level of consistency in the assessments is 0,197 that meets the requirements. After conducting evaluation of characteristics for the algorithms (Table 3), by the scale of Table 6, the NTRU algorithm has the level of 0,685, Jao-Soukharev – 0,315.

Table 17 – Weight coefficients of the encryption mechanisms criteria by expert estimates for clouds by the method of pairwise comparisons

Indicators / Experts	$I_{res.}$	$l_{pub.k.}$	$l_{pr.k.}$	$l_{t.res.}$	$T_{dir.}$	$T_{inv..}$
1	0,319	0,068	0,068	0,182	0,182	0,182
2	0,233	0,055	0,082	0,164	0,233	0,233
3	0,329	0,064	0,107	0,107	0,196	0,196
4	0,242	0,056	0,084	0,135	0,242	0,242
5	0,246	0,062	0,062	0,140	0,246	0,246
W	0,274	0,061	0,081	0,146	0,220	0,220

As in determining the weight coefficients, some attributes were assigned equal estimates, then to define a more accurate estimate we also used the ranking method, in which during expert assessment it was prohibited to assign features with the same rank, and when evaluating the very cryptographic algorithms, the equal rank was assigned only at complete matching of attributes. In Table 3, such matching is only for the resistance and speed of transformations, but in the case of speed of the transformations, we analysed not only the relative performance speed but comparative as well, which allowed us to obtain a more accurate ration for some pairs of algorithms.

Table 18 gives the result of determining the weight coefficients by expert estimates of the ES mechanisms for lightweight cryptography.

The coefficient of concordance is equal to 0,904 that satisfies the requirements. After conducting evaluation of characteristics of the algorithms (Table 3), BLISS has the levels of 0,618, XMSS – 0,382.

An analysis of Tables 12 and 18 reveals that, regardless of the applied methods, the values of weighting coefficients are almost identical. However, XMSS has a higher rating due to the fact that in the ranking method they do not take into account the difference in characteristics, and rank is assigned only. This leads to a decrease in the level of estimates in the case when a small number of objects are estimated. This property is one of the largest differences between these two methods: if, for the method of pairwise comparisons, a larger influence is exerted by the difference in characteristics (*given the weighting coefficients*), then for the ranking method, a larger impact is exerted by the number of characteristics according to which the object has an advantage (*also taking into account the weighting coefficients*).

Table 18 – Weight coefficients of the ES mechanisms criteria by expert estimates for lightweight cryptography by the ranking method

Indicators / Experts	$I_{res.}$	$l_{pub.k.}$	$l_{pr.k.}$	$l_{t.res.}$	$T_{dir.}$	$T_{inv..}$
1	4	2	5	3	6	1
2	4	2	6	3	5	1
3	5	2	6	3	4	1
4	6	2	5	3	4	1
5	6	2	5	3	4	1
W	0,238	0,095	0,257	0,143	0,219	0,048

Table 19 gives the result of determining the weight coefficients by expert estimates of the encryption mechanisms for lightweight cryptography. The coefficient of concordance equals 0,872, which meets the requirements. After conducting evaluation of characteristics of the algorithms (Table 3), the NTRU algorithm has the level of 0,606, Jao-Soukharev – 0,394.

Table 19 – Weight coefficients of the encryption mechanisms criteria by expert estimates for lightweight cryptography by the ranking method

Indicators / Experts	$I_{res.}$	$l_{pub.k.}$	$l_{pr.k.}$	$l_{t.res.}$	$T_{dir.}$	$T_{inv..}$
1	1	3	2	4	6	5
2	2	3	1	4	6	5
3	2	3	1	6	5	4
4	1	3	2	6	5	4
5	1	3	2	4	5	6
W	0,067	0,143	0,076	0,229	0,257	0,229

Table 20 gives the result of determining the weight coefficients by expert estimates of the ES mechanisms for the cryptography in standard AS. The coefficient of concordance is equal to 0,762, which satisfies the requirements. After conducting evaluation of characteristics of the algorithms (Table 3), the BLISS algorithm has the level of 0,619, XMSS – 0,381.

Table 20 – Weight coefficients of the ES mechanisms criteria by expert estimates for standard AS by the ranking method

Indicators / Experts	$I_{res.}$	$l_{pub.k.}$	$l_{pr.k.}$	$l_{t.res.}$	$T_{dir.}$	$T_{inv..}$
1	6	4	2	1	3	5
2	5	6	1	2	3	4
3	4	5	1	2	3	6
4	4	5	1	3	2	6
5	5	2	1	3	4	6
W	0,229	0,210	0,057	0,105	0,143	0,257

Table 21 gives the result of determining the weight coefficients by expert estimates of the encryption mechanisms for the cryptography of standard AS.

The coefficient of concordance equals 0,872, which meets the requirements. After conducting evaluation of characteristics of the algorithms (Table 3), the NTRU algorithm has the level of 0,605, Jao-Soukharev – 0,395.

Table 21 – Weight coefficients of the encryption mechanisms criteria by expert estimates for standard AS by the ranking method

Indicators / Experts	$I_{res.}$	$l_{pub.k.}$	$l_{pr.k.}$	$l_{t.res.}$	$T_{dir.}$	$T_{inv..}$
1	3	2	1	4	5	6
2	2	3	1	4	5	6
3	3	2	1	6	4	5
4	3	2	1	6	5	4
5	3	2	1	6	5	4
W	0,133	0,105	0,048	0,248	0,229	0,238

Table 22 gives the result of determining the weight coefficients by expert estimates of the ES mechanisms for cryptography in clouds.

The coefficient of concordance is equal to 0,954, which satisfies the requirements. After conducting evaluation of characteristics of the algorithms (Table 3), the BLISS algorithm has the level of 0,244, RankSign – 0,203, SPHINKS – 0,168, XMSS – 0,149, Jao-Soukharev – 0,132, Quartz – 0,105.

Table 22 – Weight coefficients of the ES mechanisms criteria by expert estimates for clouds by the ranking method

Indicators / Experts	$I_{res.}$	$l_{pub.k.}$	$l_{pr.k.}$	$l_{t.res.}$	$T_{dir.}$	$T_{inv..}$
1	6	2	1	3	4	5
2	6	1	2	3	5	4
3	6	1	2	3	4	5
4	6	1	2	3	4	5
5	6	2	1	3	4	5
W	0,286	0,067	0,076	0,143	0,200	0,229

Table 23 gives the result of determining the weight coefficients by expert estimates of the encryption mechanisms for cryptography in clouds.

Table 23 – Weight coefficients of the encryption mechanisms criteria by expert estimates for clouds by the ranking method

Indicators / Experts	$I_{res.}$	$l_{pub.k.}$	$l_{pr.k.}$	$l_{t.res.}$	$T_{dir.}$	$T_{inv..}$
1	6	2	1	3	5	4
2	6	1	2	3	5	4
3	6	1	2	3	5	4
4	6	1	2	3	4	5
5	6	2	1	3	4	5
W	0,286	0,067	0,076	0,143	0,219	0,210

The coefficient of concordance equals 0,945, which meets the requirements. After conducting evaluation of characteristics of the algorithms (Table 3), the NTRU algorithm has the level of 0,588, Jao-Soukharev – 0,412.

6 Discussion of results of examining the possibility of using and benefits of post-quantum algorithms depending on conditions

Weight coefficients for the conditions of lightweight cryptography (Tables 12,13,18,19) are determined from the fact that for ES, a complexity of the ES verification is almost non-essential, because the main verification of ES is performed outside the system, not in the smart card. The hardware means conducts the ES verification while performing the following procedures:

– update (*firmware renewal by developer*);

– change in the system critical data (*downloading a new CA or developer's certificate, formatting the card*);

– the process of authentication (*electronic passport, etc.*).

Also important is the size of a private key as the memory capacity is limited. For the encryption, complexity of direct and inverse transformations have the same impact. The size of the result has a big impact since it has to be transferred with every operation, and for encrypting, a public key as well.

For the standard systems (Tables 14,15,20,21), more important is the crypto transformation speed and resistance. In addition, the importance of complex validation of ES is higher than the complexity of ES procedure itself. This is due to the fact that in the public key infrastructure (PKI), the ES validation (*that is, additional check on certificate*) takes place significantly more often than the ES procedure itself.

In the cloud-based environment (Tables 16,17,22,23), the most important is the mechanism re-

sistance and speed of crypto transformations. This is so because resistance characterizes reliability of the systems, and the use of crypto-equipment in the clouds is fee-based. At the same time, storing the public keys is predetermined by the structure of clouds, and storage of private keys is included in the service when using the crypto-equipment in clouds. The size of the result of crypto transformations is more important than the size of the keys, because the result, first, may be stored not in the clouds but in the system, and, second, these messages are transmitted by communications that increase the load on the system.

When applying the methods of pairwise comparisons and ranking, the crypto algorithms estimates do not change significantly and the advantage of these over the others is maintained. But there is an exception in the evaluation of ES algorithms under conditions of cloud environment (*the case in our study, in which we simultaneously compared the largest number of algorithms*). When using the ranking method (Table 22), algorithm Quartz took the last position in contrast to the method of pairwise comparison (Table 16), where this algorithm takes a third place. This was due to the fact that the ranking method does not account for the difference between the values of characteristics, and the main benefit of the Quartz algorithm is a very small size of ES. Therefore, since the ranking method takes into account the existence of a benefit rather than its size, the Quartz algorithm gets a low benefit rank.

The comparative analysis revealed that the best choice for all systems and cases is the choice of lattice-based algorithms (BLISS and NTRU). A shortcoming of these algorithms is that according to the latest research, these algorithms have a reduced complexity for quantum attack of the "meeting in the middle" type [13,14], however, such complexity is satisfactory for minimum requirements. Hence, it follows that these algorithms are the best choice for the transition period, which will permit, by stable algorithms, finding further solutions to improve these algorithms, or searching for other variants.

Among the post-quantum mechanisms for ES, one of the most promising is the hash-based algorithm. These algorithms have a proven resistance to all known methods of quantum cryptanalysis (*in contrast to lattice-based mechanisms*). Their advantage is in that they can be used in all environments and even in the cloud-based environment they are competitive. For the use in clouds, good results were demonstrated by the RankSign algorithm, which is based on the application of mathematical codes. Other algorithms have close estimates and it is recommended to choose an algorithm depending on the structure of the appropriate cloud (*in case the state of optimization and research into protection of these algorithms will not change*).

As far as the encryption algorithms are concerned, then in the case the NTRU vulnerability [13,14] is confirmed, the choice will be limited by the mechanisms that employ isogenies.

7 Conclusions

1. In view of the specific requirements to the post-quantum crypto transformations, it is expediently to use two classes of criteria: conditional and unconditional. Conditional criteria are the criteria whose fulfilment for the examined crypto transformations is compulsory, that is, unconditioned. Conditional criteria are the criteria whose fulfilment for the examined crypto transformations must be carried out only under specified conditions. In a comparative analysis, for the purpose of conducting targeted evaluation, it is necessary to apply precise numerical values for the attributes of characteristic candidates in the post-quantum cryptographic transformations, as well as the defined scale of evaluation. To conduct evaluation of post-quantum algorithms relative to the environment, it is necessary to conduct expert assessment of weighting coefficients of attributes, or their standardization.

2. Results of comparative analysis revealed that in some cases it is possible to employ crypto transformations whose resistance is based on the transformations in the rings of abridged polynomials and lattice-based. The disadvantage of these algorithms (BLISS and NTRU) is in that, according to the latest research, these algorithms have a reduced complexity regarding the quantum attack *"meeting in the middle"*, but this complexity is satisfactory for minimal requirements. The aforementioned allows us to conclude that the crypto transformations whose resistance is based on the

transformations in the rings of abridged polynomials, and lattice-based, can be applied in the transition and the initial post-quantum periods. In the future, it is necessary to continue studies and search for or improve those adopted. Probably, an important alternative is the use of algorithms based on the hash trees of ES and algorithms with the use of isogenies of elliptic curves for encryption. When using the post-quantum crypto transformations in a cloud-based environment, it is possible to apply several candidates that have close evaluation results, which requires further research and substantiation of the choice depending on the type and use of cloud environment by the clients.

3. Depending on the application, the system of criteria may and be refined or changed, for example depending on the environment. Among the selected post-quantum cryptographic mechanisms, all the requirements are satisfied only by the lattice-based algorithms, as well as signature based on hash functions and the encryption using isogenies. Other algorithms meet only the requirements of cloud-based environment.

References

[1] Koblitz N. A riddle wrapped in an enigma / Neal Koblitz, Alfred J. Menezes [Electronic Resource]. – Way of access: https://eprint.iacr.org/2015/1018.pdf. – Title from the screen.

[2] Shor P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer / P. W. Shor // SIAM J. Comput. – 1997. – Issue 26 (5). – P. 1484 – 1509.

[3] Grover L. K. A fast quantum mechanics algorithm for database search / L. K. Grover [Electronic Resource]. – Way of access: http://cds.cern.ch/record/304210/files/9605043.pdf. – Title from the screen.

[4] Moody D. Post-Quntum Cryptography: NIST's Plan for the Future / D. Moody // The Seventh International Conference on Post-Quntum Cryptography, Japan, 2016 [Electronic Resource]. – Way of access: https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf. – Title from the screen.

[5] Mosca M. Setting the Scene for the ETSI Quantum-safe Cryptography Workshop / M. Mosca // E-proceedings of "1st Quantum-Safe-Crypto Workshop", Sophia Antipolis, Sep 26-27, 2013 [Electronic Resource]. – Way of access: http://docbox.etsi.org/Workshop/2013/201309_CRYPTO/eproceedings_Crypto_2013.pdf. – Title from the screen.

[6] Jao D. Isogeny-Based Quantum-Resistant Undeniable Signatures / D. Jao, V. Soukharev // PQCrypto 2014. – P. 160–179.

[7] Postkvantova kryptografija ta mehanizmy i'i' realizacii' / I.D. Gorbenko, O.O.Kuznjecov, O.V.Potij ta in. // Radiotehnika. – 2016. – Vyp. 186. – S. 32–52.

[8] Gorbenko Ju.I. Metody pobuduvannja ta analizu, standartyzacija ta zastosuvannja kryptografichnyh system / Ju. I. Gorbenko: monografija; za zag. red. I. D. Gorbenko. – Harkiv: Fort, 2015. – 959 s.

[9] Lenstra H. W. Analysis and comparison of some integer factoring algorithms, in Computational Methods in Number Theory / H. W. Lenstra, Jr. Tijdeman , R. Tijdeman // Math. Centre Tract 154. – 1982. – P. 89–141.

[10] Yesina M. Methods of cryptographic primitives comparative analysis / Maryna Yesina, Yurij Gorbenko // Inżynier XXI wieku ("Engineer of XXI Century"): the VI Inter University Conference of Students, PhD Students and Young Scientists; University of Bielsko-Biala, Poland, December 02, 2016. – Bielsko-Biała: Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej, 2016. – P. 451–462.

[11] Nogin V. D. Uproshchennyi variant metoda analiza ierarkhii na osnove nelineinoi svertki kriteriev / V. D. Nogin [Elektronnyi resurs]. – Rezhim dostupa: http://www.apmath.spbu.ru/ru/staff/nogin/nogin_p11.pdf. – Zagl. s ekrana.

[12] Ekspertnye otsenki pri razrabotke reshenii [Elektronnyi resurs]. – Rezhim dostupa: http://books.ifmo.ru/file/pdf/817.pdf – 20.05.2016. – Zagl. s ekrana.

[13] Wang H. An efficient quantum meet-in-the-middle attack against NTRU-2005 / H. Wang, M. Zhi, M. ChuanGui // Chinese Science Bulletin. – 2013. – Vol. 58. – № 28–29. – P. 3514–3518.

[14] An Improved MITM Attack Against NTRU / Zhijian Xiong, Jinshuang Wang, Yanbo Wang et al. // International Journal of Security and Its Applications. – 2012. – Vol. 6. – № 2. – P. 269–274.

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

Надійшло: Червень 2017.

Автори:
Іван Горбенко, д.т.н., проф., лауреат Державної премії України, Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: gorbenkoi@iit.kharkov.ua

Володимир Пономар, аспірант, ХНУ імені В.Н. Каразіна, Харків, Україна.
E-mail: laedaa@gmail.com

Марина Єсіна, аспірантка, ХНУ імені В.Н. Каразіна, Харків, Україна.
E-mail: rinayes20@gmail.com

Дослідження можливості використання та переваг постквантових алгоритмів залежно від умов застосування.

Анотація. Встановлена необхідність проведення порівняльного аналізу та оцінки можливості використання асиметричних постквантових криптографічних механізмів. Для порівняння обрано методику оцінювання на основі інтегральних оцінок безумовних і умовних критеріїв. Аналіз проведено серед алгоритмів, що задовольнили загальні безумовні критерії. В якості умовних критеріїв обрано чисельні характеристики алгоритмів. Крім того, висувалися додаткові безумовні критерії, що відрізнялися залежно від умов застосування. Актуальність досліджень пов'язана з прогнозом появи квантового комп'ютера. А в існуючих дослідженнях вже доведено, що поточні криптографічні алгоритми мають вразливості до методів квантового криптоаналізу. Тому вже зараз лідируючі інститути стандартизації криптоалгоритмів проводять дослідження та порівняння для вибору постквантового стандарту криптографії. У результаті досліджень було встановлено відсутність універсального постквантового криптографічного алгоритму. Запропоновано відокремити три варіанти використання постквантових алгоритмів: для легкої криптографії, використання стандартними автоматизованими системами і використання в хмарному середовищі. Для кожних умов застосування проведено окреме оцінювання переваг криптографічних алгоритмів. Виявлені недоліки лідируючого кандидата. Надані рекомендації використовувати ці алгоритми в якості основного на час перехідного періоду. А, якщо підозра підтвердиться, запропоновано альтернативи. Результати досліджень дозволяють зрозуміти поточний стан розвитку постквантових криптоалгоритмів і спрогнозувати можливий їх подальший розвиток. Практичне значення дослідження полягає в отриманні оцінки постквантових алгоритмів в залежності від умов застосування.

Ключові слова: постквантові криптографічні алгоритми, порівняльна оцінка криптоалгоритмів, критерії порівняння криптоалгоритмів.

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

Поступила: Июнь 2017.

Авторы:
Иван Горбенко, д.т.н., проф., лауреат Государственной премии Украины, Харьковский национальный университет имени В. Н. Каразина, Украина.
E-mail: gorbenkoi@iit.kharkov.ua

Владимир Пономарь, аспирант, ХНУ имени В. Н. Каразина, Харьков, Украина.
E-mail: Laedaa@gmail.com

Марина Есина, аспирантка, ХНУ имени В. Н. Каразина, Харьков, Украина.
E-mail: rinayes20@gmail.com

Исследование возможности использования и преимуществ постквантовых алгоритмов в зависимости от условий применения.

Аннотация. Была установлена необходимость проведения сравнительного анализа и оценки возможности использования асимметрических постквантових криптографических механизмов. Для сравнения выбрано методику оценивания на основе интегральных оценок безусловных и условных критериев. Анализ проводился среди алгоритмов, которые удовлетворили общие безусловные критерии. В качестве условных критериев выбрано численные характеристики алгоритмов. Кроме того, выдвигались дополнительные безусловные критерии, которые отличались в зависимости от условий использования. Актуальность данных исследований связана з прогнозом появления квантового компьютера. А в существующих исследованиях уже доказано, что текущие криптографические алгоритмы имеют уязвимости к методам квантового криптоанализа. Поэтому уже сейчас лидирующие институты стандартизации криптоалгоритмов проводят исследования и сравнения для выбора постквантового стандарта криптографии. В результате исследований было установлено отсутствие универсального постквантового криптографического алгоритма. Предложено выделить три варианта использования постквантовых алгоритмов: для легкой криптографии, использование стандартными автоматизированными системами и использование в облачной среде. Для каждых условий применения проведено отдельное оценивание преимуществ криптографических алгоритмов. Выявлены недостатки лидирующего кандидата. Даны рекомендации использовать эти алгоритмы в качестве основного на время переходного периода. А, если угроза подтвердится, предложены альтернативы. Результаты исследований дают понять текущее состояние развития постквантовых криптоалгоритмов и спрогнозировать возможное их дальнейшее развитие. Практическое значение исследования заключается в получении оценки постквантовых алгоритмов в зависимости от условий применения.

Ключевые слова: постквантовые криптографические алгоритмы, сравнительная оценка криптоалгоритмов, критерии сравнения криптоалгоритмов.

UDC 621.327:621.391

МОДИФИЦИРОВАННОЕ ЗОНАЛЬНОЕ КОДИРОВАНИЕ ТРАНСФОРМАНТ МАЛОРЕСУРСНОГО СТЕГАНОАЛГОРИТМА

Дмитрий Морозов, Сергей Малахов

Харьковский национальный университет имени В.Н. Каразина, пл. Свободы, 4, г. Харьков, 61022, Украина
ikurortnik@gmail.com, mailgate@meta.ua

Рецензент: Георгий Кучук, д.т.н., проф., Национальный технический университет «Харьковский политехнический институт», ул. Кирпичова, 21, Харьков, Украина, 61000.
kuchuk56@mail.ru

Поступила в июне 2017

Аннотация. *Представлены результаты моделирования процесса сжатия полутоновых изображений посредством модифицированной зональной селекции коэффициентов преобразования. Для обработки трансформант применены два способа группировки коэффициентов. Реализовано последовательное укрупнение сформированных зон и поэтапное уменьшение количества сохраняемых коэффициентов. Выполнен анализ зависимости искажений от варианта обработки трансформант. Рассмотренные процедуры являются первым этапом малоресурсного стеганоалгоритма.*

Ключевые слова: *видеоданные, кодирование с преобразованием, зональное кодирование, стеганография.*

1 Введение

Задача сокращения объема цифрового описания видеоданных при их передаче, хранении и использовании различных стеганографических методик, сопровождает все этапы развития систем обработки и передачи информации на протяжении всей их эволюции. При этом подавляющее большинство существующих форматов компактного представления видеоданных базируется на использовании внутрикадрового и межкадрового методов кодирования с преобразованием [1-3]. Кодирование с преобразованием относится к группе методов сжатия с частичной потерей качества восстанавливаемых изображений. Однако применяемые в них способы отбора (селекции) значимых коэффициентов преобразования во многих случаях не обеспечивают требуемой детальности восстанавливаемых изображений. Наиболее характерно это проявляется при внутрикадровой обработке полутоновых изображений (256 градаций серого), что обусловлено большей чувствительностью зрительной системы человека к изменениям градаций яркости, нежели градаций цвета [1,3]. Это обстоятельство, в определенной степени, затрудняет задачу инкапсуляции стеганоконтента в изображение - стеганоконтейнер [4]. Поэтому уменьшение величины искажений восстанавливаемых (декодируемых) полутоновых изображений при сохранении высокой степени сжатия исходного массива данных является актуальной задачей и обеспечивает благоприятные условия для успешного встраивания стеганоконтента.

Анализ различных источников, касающихся рассматриваемой тематики, показал, что задача селекции коэффициентов преобразования чаще всего решается путем использования зонального и порогового методов. Каждый из них имеет свои положительные и отрицательные стороны [1,3,5,6]. Так, зональный метод характеризуется: – большей устойчивостью сжатого массива данных к воздействию помех и ошибок, возникающих в каналах связи при их передачи; – относительной простотой реализации кодера и декодера; - постоянной скоростью потока данных на выходе кодера. Поэтому данный метод чаще применяется в системах, функционирующих в масштабе времени, близком к реальному, или системах (устройствах) ориентирующихся на малоресурсную обработку данных *(различные мобильные платформы)*.

В отличие от него пороговый метод обеспечивает улучшенное качество восстановления исходных данных. Однако при его реализации особое внимание следует обратить на

точность позиционирования (адресации) значимых коэффициентов преобразования, вследствие чего несколько возрастает сложность алгоритма обработки и увеличивается объем цифрового описания сжатого массива видеоданных. Кроме того, для поддержания постоянной скорости передачи данных желательно использование буфера. Таким образом, пороговый метод реализует адаптивный к локальной статистике обрабатываемых изображений отбор значимых коэффициентов преобразования, однако проявляет повышенную чувствительность к ошибкам адресации сохраняемых компонент трансформант и несколько сложнее в своей реализации [3].

Анализ профильной тематики и проведенное экспериментальное моделирование позволяют утверждать, что во многих случаях (идентификация объектов динамических изображений в режиме «стоп кадр» или сложная структура передаваемой сцены и др.) зональный метод не обеспечивает достаточной точности восстановленных репродукций и ограничивает возможности по встраиванию стеганоконтента в изображение-контейнер обработанный традиционным образом. С учетом бурного развития мобильных платформ и широким распространением приложений для них представляет практический интерес создание легковесного алгоритма обработки, обеспечивающего улучшенные исходные условия для последующей инкапсуляции стеганоконтента в обработанное соответствующим образом изображение-контейнер.

Целью статьи является представление результатов моделирования процессов модифицированной зональной обработки трансформант полутоновых изображений со сложной структурой при проведении внутрикадрового кодирования с преобразованием. Данную процедуру следует рассматривать как условие для последующей успешной реализации легковесного алгоритма стеганографической обработки изображений *(ориентированного на использование в рамках различных мобильных платформ)*. Таким образом, основную цель проведенных экспериментов можно сформулировать, как минимизация величины искажений восстанавливаемых видеоданных при использовании относительно простых программно-аппаратных решений и сохранении высоких степеней компрессии.

2 Основная часть

Модель селекции коэффициентов преобразования при реализации зонального кодирования заключается в следующем. Если через I_t обозначить адреса передаваемых коэффициентов трансформант ($y_{u,v}$)

$$I_t = \{(u,v); |y_{u,v}| \geq 1\}, \quad (1)$$

то можно определить функцию зонального маскирования (Zonal)

$$m(u,v) = \begin{cases} 1, & где\ u,v \in I_t; \\ 0, & в\ противном\ варианте, \end{cases} \quad (2)$$

которая равна 1 в зоне сосредоточения наибольших значений $y_{u,v}$. Таким образом, реализуется зональная селекция коэффициентов преобразования.

В ходе моделирования исследовалась возможность улучшения качества восстанавливаемых репродукций путем формирования в области трансформант, не охваченных функцией зонального маскирования (2), дополнительных зон (областей селекции - ОС) с заданной конфигурацией [6].

В рамках моделирования рассмотрены два способа формирования областей селекции коэффициентов трансформант (Рис.1). В отличие от известного метода «пирамиды Лапласа» в данном случае обеспечивается пропорциональное присутствие в каждой из формируемых зон контуров деталей изображения, имеющих вертикальную и горизонтальную протяженность, а также постепенное повышение пространственных частот спектра в каждой из зон. В обоих случаях все коэффициенты, формирующие область Zonal (Рис.1), округлялись до це-

лых и сохранялись с соответствующими им знаками. Далее, для каждой из оставшихся областей сохранялось среднее значение амплитуд составляющих ее коэффициентов. При декодировании, эти значения используются для восстановления трансформант.

Следует отметить, что амплитудный спектр содержит информацию о резкости изображения, а информация о наличии и положении световой границы заключена в его фазовом спектре [1,3]. Если искажения фазового спектра будут невелики, т.е. не вызовут исчезновения или появления новых световых границ, то изображение будет узнаваемым. К таким искажениям относятся процедуры дифференцирования *(подчеркивание границ)* и интегрирования *(расфокусировка)* [3]. Если же в результате какого-либо преобразования существенно искажается фазовый спектр изображения, то может произойти полная потеря его узнаваемости. Пример этого случая - воздействие флуктуационного шума большой мощности, что влечет за собой полное «размывание» световых границ. Очевидно, что при передаче видеоданных особое внимание следует уделить точности передачи фазового спектра. Поэтому при проведении экспериментов вся информация о фазовых составляющих сохранялась путем формирования отдельного массива матриц знаков (МЗ).

Уменьшение объема цифрового описания трансформант реализовано путем сокращения объема цифрового описания амплитудных составляющих. Он заключается в поэтапном ограничении количества сохраняемых значений, характеризующих среднюю амплитуду коэффициентов в каждой из зон, и реализуется за счет объединения соседних ОС коэффициентов трансформант (рис.1). При этом в ходе моделирования использовался механизм «высокочастотного» (ВЧ) объединение смежных зон [6]. В соответствии с ним процесс объединения зон инициируется в области группировки гармоник высших порядков и проводится в направлении области трансформант, охваченных функцией зонального маскирования (2), к изменению состава и величины которых наиболее чувствительна зрительная система человека [1,3]. Исходной (базовой) трансформантой $F_N(U;V)$ при проведении экспериментов являлась матрица размером 8×8 элементов. В общем случае, при выборе размера субблоков изображений следует руководствоваться соображениями обеспечения баланса между требуемой степенью сжатия, вычислительной сложностью и текущим уровнем заряда батареи гаджета. При этом для базовой матрицы ($F_7(U;V)$) возможно проведение шести шагов (τ_{max}) по объединению смежных зон. При $\tau = 5$ оба способа формируют трансформанту с одинаковой конфигурацией зон ($F_2(U;V)$). На 6-м шаге формируется матрица $F_1(U;V)$, аналогичная Zonal (Рис.1). При этом чем больше ОС сформировано в базовой трансформанте, тем выше качество восстанавливаемого изображения.

В дополнение к уже введенным обозначениям, описывающим состояние трансформант, необходимо ввести следующее сокращение: $kF_N(U;V)$ следует понимать, как: - трансформанта, сформированная k-м способом; - содержащая N областей селекции.

При восстановлении исходной информации проведение расчетов базовых матриц не требуется, а восстановление трансформант осуществляется в соответствии с информацией, записанной в маркере декодируемого кадра изображения. Очевидно, что процесс перехода от одного варианта к другому в обратном порядке не возможен, т.к. на каждом шаге алгоритма (τ) происходит потеря части информации, содержащейся в исходной базовой трансформанте. При этом среднеквадратичная ошибка (СКО) аппроксимации матрицы изображения X^* (с компонентами x_{ij}), восстановленной посредством проведения модифицированной зональной селекции коэффициентов трансформант по отношению к исходной матрице X, определяется как

$$\varepsilon_a^2 = \mathrm{E}\left\{\left\|X - X^*\right\|^2\right\} = \mathrm{E}\left\{\left\|\sum_{u=1}^{n}\sum_{v=1}^{n} a_{ijuv} y_{uv} - \sum_{u=1}^{n}\sum_{v=1}^{n} a_{ijuv} y^*_{uv}\right\|^2\right\} =$$

$$= \mathrm{E}\left\{\left\|\left(\sum_{u=1}^{n}\sum_{v=1}^{n}\left(y_{uv} - y^*_{uv}\right)\times\left(\sum_{u=1}^{n}\sum_{v=1}^{n} a_{ijuv}\right)\right)\right\|^2\right\} =$$

$$= \mathrm{E}\left\{\left\| \left(\sum_{u=1}^{n}\sum_{v=1}^{n} (\Delta y_{uv}) \right) \times \left(\sum_{u=1}^{n}\sum_{v=1}^{n} a_{ijuv} \right) \right\|^2 \right\}, \quad (3)$$

где a_{ijuv} - компоненты унитарной матрицы, определяемые видом ортогонального преобразования; - y^*_{uv} – коэффициенты, восстановленные одним из рассматриваемых способов;
- y_{uv} - коэффициенты исходной трансформанты, определяемые в результате проведения прямого преобразования

$$y_{uv} = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{uvij}\, x_{ij}, \quad i, j = \overline{1,n}. \quad (4)$$

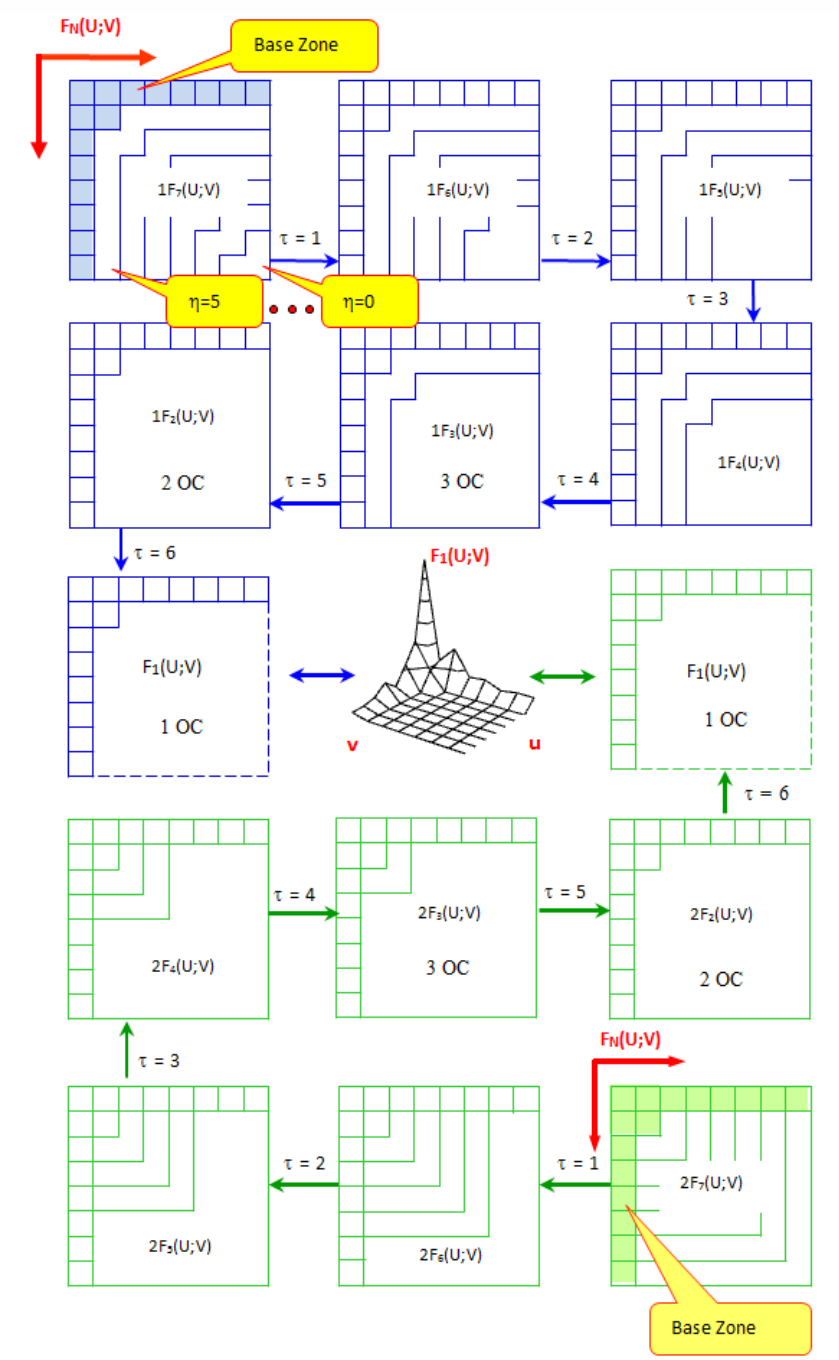

Рис.1 - Порядок объединения смежных зон для матрицы 8×8 элементов

Данное преобразование дает набор из n^2 компонент, каждая из которых представляет собой линейную комбинацию элементов исходного изображения - *X*. Аналогично этому об-

ратное преобразование определяет каждый элемент изображения, как линейную комбинацию всех компонентов

$$x_{ij} = \sum_{u=1}^{n}\sum_{v=1}^{n} a_{ijuv}\, y_{uv}, \quad i,j = \overline{1,n}. \tag{5}$$

Δy_{uv} - определяется из системы:

$$\begin{cases} \Delta y_{uv} = \left| y_{uv} - \lfloor y_{uv} \rfloor \right|, & для\ y_{uv} \in Zonal; \\ \Delta y_{uv} = \left| y_{uv} - \left\lfloor \dfrac{\sum\limits_{u=1}^{\Omega_\eta}\sum\limits_{v=1}^{\Omega_\eta} y_{uv}}{2\Omega_\eta - 1} \right\rfloor \right|, & для\ y_{uv} \notin Zonal, \end{cases} \tag{6}$$

где: $|\ |$ - модуль величины; $\lfloor\ \rfloor$ - округление результата в сторону уменьшения; η - порядковый номер сформированной зоны в каждой из трансформант. Их максимальное число определяется как

$$\eta_{\max} = n - (1+\tau), \qquad \tau = \overline{0, n-1}; \tag{7}$$

Ω_η - количество спектральных компонент в η-ой зоне трансформанты $F_N(U;V)$. Причем

$$\eta = \overline{0, \tau_{\min} - 1}, \tag{8}$$

где $\tau_{\min}$ – оставшееся число шагов алгоритма по объединению смежных зон.

Так для трансформанты 8×8 элементов в зависимости от используемого способа объединения смежных зон, количество спектральных компонент (Ω_η) в каждой из зон определяется из данных табл. 1

Таблица 1 - Количество компонент в зонах для матрицы 8×8

1 спб.	**$1F_7(U;V)$**	**$1F_6(U;V)$**	**$1F_5(U;V)$**	**$1F_4(U;V)$**	**$1F_3(U;V)$**	**$1F_2(U;V)$**
η=0	2n-13+2η	4n-24	6n-33	8n-40	10n-45	12n-48
η>0	2n-13+2η	21-2n+2η	23-2n+2η	25-2n+2η	27-2n+2η	-
2 спб.	**$2F_7(U;V)$**	**$2F_6(U;V)$**	**$2F_5(U;V)$**	**$2F_4(U;V)$**	**$2F_3(U;V)$**	**$2F_2(U;V)$**
η=0	2n-3-2η	4n-8	6n-15	8n-24	10n-35	12n-48
η>0	2n-3-2η	2n-5-2η	2n-7-2η	2n-9-2η	2n-11-2η	-

В ходе моделирования степень отличия восстановленных изображений от их оригинала оценивалась по двум показателям: - СКО (3); - коэффициенту разницы – K_r. Коэффициент разницы связывает взятые по модулю значения разностей яркости элементов исходного и восстановленного блоков изображения ($|\Delta x_{ij}|$) с их количеством:

$$K_r = \sum_{\Delta x_{ij}=5}^{\Delta x_{ij}=max} \frac{n_\Delta}{|\Delta x_{ij}|}, \tag{9}$$

где n_Δ – общее количество элементов восстановленного блока изображения, отличающихся от их оригинала на величину $|\mathbf{\Delta x_{ij}}|$ (*i и j – координаты пикселя в блоке изображения*). Причем, оценка проведена только для визуально фиксируемых изменений яркости, т.е. для случая, когда $|\mathbf{\Delta x_{ij}}| \geq 5$.

На рис. 2 представлены зависимости, полученные по результатам проведенных экспериментов.

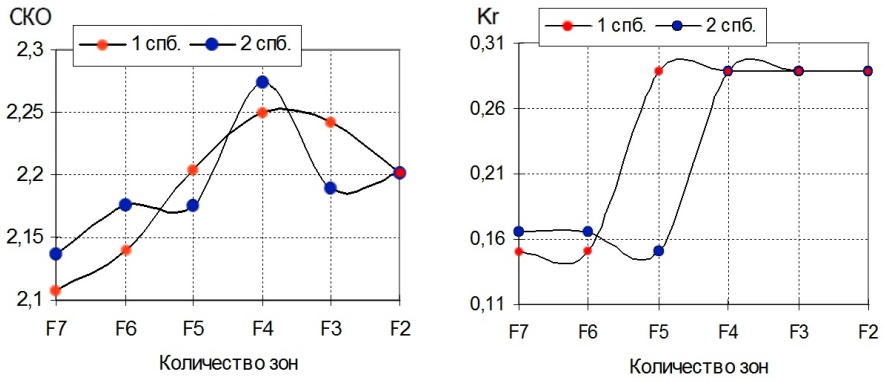

Рис. 2 – Изменение величины СКО и K_r в зависимости от режима обработки ОС

3 Выводы

1. В результате анализа полученных в ходе моделирования зависимостей можно утверждать, что характеристика K_r, по сравнению с СКО, носит более статичный характер, так как показатель K_r обладает меньшей чувствительностью к количеству и величине искажений с малой амплитудой. Это обусловлено тем, что при изменении параметров настроек алгоритма кодирования, увеличение ошибок с малой амплитудой происходит гораздо интенсивнее, чем для $|\Delta x_{ij}| \geq 5$. Однако, сопоставление зависимостей СКО и K_r говорит об одинаковом характере их изменения, что подтверждает правомерность использования показателя K_r для оценки визуально фиксируемой составляющей от общего количества ошибочно восстановленных элементов изображений.

2. Апробирован алгоритм обработки трансформант (10), обеспечивающий плавный рост искажений, ограниченный величиной ошибок, характерных для режима Zonal. В соответствии с ним каждый последующий шаг реализованного алгоритма представляет собой очередное упрощение базовой трансформанты, проводимое путем ВЧ объединения соседних ОС:

$$\begin{aligned} & 1F_7(U;V) \xrightarrow{\tau_a=1} 1F_6(U;V) \xrightarrow{\tau_a=2} 2F_5(U;V) \xrightarrow{\tau_a=3} \dots \\ & \rightarrow 1F_4(U;V) \xrightarrow{\tau_a=4} 2F_3(U;V) \xrightarrow{\tau_a=5} F_2(U;V) \xrightarrow{\tau_a=6} \dots \\ & \rightarrow \frac{F_1(U;V)}{Zonal}. \end{aligned} \qquad (10)$$

3. Рассмотренный порядок обработки трансформант характеризуется простотой реализации, малой вычислительной сложностью и обеспечивает хорошие стартовые условия *(хорошие степень сжатия и СКО)* для последующей инкапсуляции стеганоконтента, обработанного подобным образом *(симметричная схема)*. Для повышения стойкости ко взлому стеганоконтента разработан соответствующий алгоритм генерации масок обфускатора *(вопрос выходит за рамки данной статьи)*, реализующий механизмы межблочного и внутриблочного перемешивания.

Ссылки

1. Zubarev Yu.B. Tsifrovaya obrabotka televizionnykh i komp'yuternykh izobrazhenii / Yu.B. Zubarev, V.P. Dvorkovich. – Moskva: MTsNTI, 1997. – 212 s.
2. Shlikht G.Yu. Tsifrovaya obrabotka tsvetnykh izobrazhenii / G.Yu. Shlikht. – Moskva: EKOM, 1997. – 336 s.
3. Prett U. Tsifrovaya obrabotka izobrazhenii / U. Prett. – M.: Mir, 1985. – 736 s.
4. Gribunin V.G. Tsifrovaya steganografiya / V.G. Gribunin, I.N. Okov, I.V. Turintsev. – Moskva: Solon-Press, 2009. – 265 s.
5. Korolev A.V. Otsenka informativnosti transformant diskretnogo kosinusnogo preobrazovaniya / A.V. Korolev // Sistemi obrobki informatsii. – 2003. – Vip.3. – S. 81–85.
6. Malakhov S.V., Bukhantsov A.D. Zonal'noe kodirovanie izobrazhenii s razlichnym razbieniem prostranstvenno-chastotnoi oblasti / S.V. Malakhov, A.D. Bukhantsov // Sistemi obrobki informatsiї. – 2001. – Vip. 4(14). – S. 121–125.

Reviewer: Georgiy Kuchuk, Doctor of Technical Sciences, Full Professor, Professor of the Department of Computer Science and Programming, National Technical University "Kharkiv Polytechnic Institute", st. Kirpichova, 21, Kharkiv, Ukraine.
E-mail: kuchuk56@ukr.net

Received: June 2017.

Authors:
Dmitriy Morozov, student, Faculty of Computer Science, V. N. Karazin Kharkiv National University, Kharkov, Ukraine.
E-mail: ikurortnik@gmail.com

Sergey Malakhov, Ph.D., Senior Researcher, V. N. Karazin Kharkiv National University, Kharkov, Ukraine.
E-mail: mailgate@meta.ua

Modified zonal coding of transformants of low-resource steganography algorithm.

Abstract. The results of modeling the process of compression of halftone images by means of a modified zonal selection of the transformation coefficients. To process transformants, two methods of grouping the coefficients are applied. Successive consolidation of the formed zones is realized and a phased reduction in the number of stored coefficients. The analysis of the dependence of distortions on the variant of processing transformants is performed. The procedures considered are the first stage of a low-resource steganography algorithm.

Keywords: video data, encoding with conversion, zonal encoding, steganography.

Рецензент: Георгій Кучук, д.т.н., проф., НТУ «ХПІ», Харків, Україна.
E-mail: kuchuk56@ukr.net

Надійшло: Червень 2017.

Автори:
Дмитро Морозов, студент факультету комп'ютерних наук, ХНУ імені В. Н. Каразіна, Харків, Україна.
E-mail: ikurortnik@gmail.com

Сергій Малахов, к.т.н., с.н.с., ХНУ імені В. Н. Каразіна, Харків, Україна.
E-mail: mailgate@meta.ua

Модифіковане зональне кодування трансформант малоресурсного стеганоалгоритма.

Анотація. Представлені результати моделювання процесу стиснення півтонових зображень за допомогою модифікованої зональної селекції коефіцієнтів перетворення. Для обробки трансформант застосовані два способи угруповання коефіцієнтів. Реалізовано послідовне укрупнення сформованих зон і поетапне зменшення кількості збережених коефіцієнтів. Виконано аналіз залежності викривлень від варіанту обробки трансформант. Розглянуті процедури є першим етапом малоресурсного стеганоалгоритму.

Ключові слова: відеодані, кодування з перетворенням, зональне кодування, стеганографія.

Статті пройшли внутрішнє та зовнішнє рецензування.

Наукове видання

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА

Випуск 3(7) 2017

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