ISSN 2519-2310

COMPUTER SCIENCE AND CYBERSECURITY

ISSUE 3(3) 2016

V. N. Karazin Kharkiv National University Publishing

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

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

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

Issue 3(3) 2016

Заснований 2015 року

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

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

Journal is published quarterly.
Approved for placement on the Internet by Academic Council of the Karazin Kharkiv National University (December 26, 2016, 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(3) 2016

UDC 004.056.55

METHODS AND RESULTS OF ELECTRONIC SIGNATURES WITH APPENDIX AND MESSAGE RECOVERY COMPARATIVE ANALYSIS

I. Gorbenko, M. Yesina, N. Kovaleva

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

Reviewer: Irina Lisitska, Dr., Full Professor, V.N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine;
lisitska@karazin.ua

Received on August 2016

Abstract. *The paper deals with the comparative analysis methods of electronic signature mechanisms properties. The existing methods of comparative analysis of electronic signatures based on expert estimations methods – analytic hierarchy process and variations of weight indices methods are investigated and analyzed. Some criteria and indicators, that can be used in the comparative analysis of electronic signature mechanisms properties are presented. The comparative analysis of the existing perspective electronic signatures mechanisms according to the standards DSTU ISO/IEC 14888-3:2014 and DSTU ISO/IEC 9796-3 is carried out. The results of the conducted electronic signature mechanisms evaluation are shown. Conclusions and recommendations on the use of defined electronic signature algorithms evaluation methods are made and provided.*

Keywords*: electronic signature mechanisms analysis, weight indices, electronic signature, electronic signature estimation criterion, electronic signature comparison analysis methods, electronic signature realization and application.*

1 Introduction

The significant number of standardized electronic signatures (ES) mechanisms [1-3,7] are applied in order to provide in different information technology electronic trust services at the international, regional and national levels. In the European Union (EU) it is made a number of normalization projects relatively ES [6,14]. And it would seem, that they solve problems at least to 2030 year. However, according to the recent researches, in terms of requirements and development of post quantum ES standards, appeared new, both theoretical and practical, problems of substantiation construction methods, analysis and comparative analysis of ES. Thus developers and users of electronic trust services applications have the ability to select ES from the significant number of existing international and national standards, primarily DSTU ISO/IEC 14888-1,2,3 [1,2], DSTU ISO/IEC 9796-3 [3], DSTU 4145-2002 [7] and others. Providers and users have the ability to select ES for application in the indicated conditions, moreover depending on the requirements and adopted models of threats and violator [6]. Therefore, in our opinion, now so important and, that require the solving, are theoretical and practical issues of methods substantiation and choice, and creation on their base the analysis techniques and comparative analysis of existing and perspective ES.

The special importance of solve the above mentioned problems is connected with the deployment of the development and implementation ES works, and other cryptographic primitives, that meet the post quantum period requirements [6]. This is stems from the fact, that to the post quantum cryptographic primitives demands are made not only relatively cryptographic stability, but also it is a significant number of feasibility and technical-operational requirements.

First time, according to our analysis, such analysis techniques and comparative analysis ES were proposed in [4,8,15-17] and detailed in [6]. The essence of the suggestions reduced to separation ES evaluating criteria on unconditional and conditional and then their use to calculate the values of integral conditional and unconditional ES evaluating criteria. In this case offered unconditional criteria and integral unconditional criterion on their base are effective and allow to estimate or compare ES. However, methods of calculating integral conditional criterion values based on pairwise comparisons and hierarchies methods, proposed in [4,6,8,15-17], to a large extent depend on the

experts competence and objectivity in their assessments. At the same time, there are other methods, including deserves attention method of weighting coefficients [9,11-13,18-20,22-24] and practical guidelines, that support it.

The objective of this article is the methods theoretical substantiation and practical implementation and development on their base ES evaluation technique and comparative analysis on conditional and unconditional criteria, their practical use to compare existing ES [1-3,6,7], and also the guidelines development for assessment and comparative analysis post quantum period ES.

2 Problem formulation

Analysis of a number of sources [4,6,8,15-17] showed, that an important stage of selection perspective cryptographic primitive is the decision on determine the most perspective ES method or methods, and also other cryptographic primitives, and the final stage is their comparative analysis according to determined partial and integral conditioned and unconditioned criteria. In fact, this problem practically not solved relatively cryptographic primitives, the evidence of this is carrying international projects AES, Neisse and SHA-3 [6]. In our opinion, at acceptance decision regarding recommendation of certain cryptographic primitives as standard, mainly taken into consideration their assessments and special services opinions, and experts subjective assessments. Although experts opinions and influence, in our opinion, were not significant. Therefore the important theoretical and practical problem is the substantiation and choice, according to the requirements, the sets of indicators and assessment criteria, substantiation and choice estimate method or methods and properties comparative analysis, and also the development and practical application of scientifically grounded assessment techniques and comparative analysis cryptographic primitives of certain class. In our case concentrate on existing and perspective standardized ES mechanisms, that are improved or will be developed for use in post quantum period.

The specified problem will consider mainly on algorithms, whose stability is based on complexity of discrete logarithm at finite field and the group of points of elliptic curves (EC): DSTU ISO/IEC 14888-3:2014 [1,2] and DSTU ISO/IEC 9796-3 [3]. In DSTU ISO/IEC 14888-3 is recommended to use 12 different ES mechanism, based on the use mathematical apparatus of finite fields, elliptic curves and EC points pairing.

Thus, the objective of research, which is the subject of the article is review, analysis and comparative analysis of ES with appendix according to DSTU ISO/IEC 14888-3: 2014 and DSTU ISO/IEC 9796-3 on the totality unconditional and conditional criteria [6], and also separately analysis and development of recommendations on the use methods and this type technique for ES analysis and comparison, using as example DSTU ISO/IEC 14888-3: 2014 [1,2] and DSTU ISO/IEC 9796-3 [3] algorithms, as well as possible for ES assessment, that will be developed for use in post quantum period.

3 The achievements state of the methods and assessment techniques and ES comparative analysis development and application

From described above follows the necessity and actuality of solving the problem, a great extent, automation and significantly reduce decision-making subjectivity relatively the benefits of the cryptographic primitives certain set, such as ES. The solution of tasks certain components of this problem is contained in [4,6]. Thus in [6] for ES evaluation and comparative analysis are proposed pairwise comparison methods and hierarchy method [4-6,8,10,15-17,21].

Later in the criterion will understand the sign on which basis is carried out the assessment, anything determination or classification [6], that is, in fact, will understand the measure of evaluation. Previous researches and [6] allow to substantiate the conclusion, that the evaluation and standardized ES algorithms comparison should implement using two sets of criteria: unconditional and conditional [6]. Given the [6], ES type cryptographic transformations evaluating can be carried out in 2 stages.

In the first stage it is checked the conformity standardized algorithms to requirements of unconditional criteria – partial and integral, and in the second, using conditional criteria – partial conditional criteria and integral conditional criterion. Just by using partial conditional criteria and integral conditional criterion, and it is possible to compare different ES type cryptographic transformation.

3.1 Expert assessment methods

In expert estimates understand search method and the result of applying the method, obtained based on the use personal expert opinion or collective opinion of the expert group [12,13,22-24], and also a set of logical and mathematical procedures, aimed at obtaining information from experts, its analysis and generalization for the preparation and making rational decisions [12,13,22].

Expert assessments methods – methods of organization work with specialists-experts and processing of experts opinions [12,13,22-24]. Essence of the method expert assessments – in basis of the making decision, forecast, conclusion is laid the specialist or team of specialists opinion, based on their knowledge and practical professional experience.

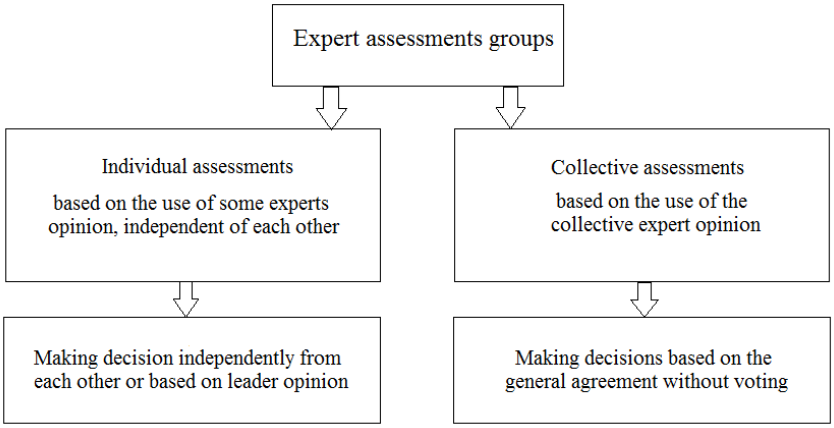

Fig. 1 – Scheme of expert assessments groups

Expert assessment stages [12,13,22-24]:

1. Research objective statement
2. The choice of research form, determining the project budget
3. Preparation of information materials, questionnaire blanks, procedure moderator
4. Selection of experts
5. Expert examination
6. Analysis of results (expert assessments processing)
7. Prepare a report with the results of expert assessment

There are known the following expert assessments methods (ways to develop both collective and individual expert assessments) [12,13,22-24]: associations method; pair (binary) comparison method; vectors advantages method; focal objects method; individual expert survey; midpoint method; simple ranking method; setting weight coefficients method; successive comparisons method; attribution points method. Methods for receiving individual opinion [12,13,22-24]: method "Delphi", interview method, report method.

Methods of expert group teamwork [12,13,22-24]: brainstorming (brainstorm), method "635", business game, commission assessment (method of "meeting", "round table"), method of "court".

3.2 ES mechanisms evaluation by unconditional criteria

To unconditional criteria will refer the criteria, which implementation for the ES type cryptographic transformations is mandatory, that is unconditional.

Analysis of the application state, development and assessment experience of the ES type cryptographic transformations properties, primarily in a group of EC points, the achieved results in the

practical solution of cryptanalysis tasks and various attacks implementing, allow as basic to choose the following unconditional evaluation criteria [6]:

$W_{\delta 1}$ – mathematical base reliability, which used in the cryptographic transformations for ES;

$W_{\delta 2}$ – ES type cryptographic transformations against known attacks practical protection;

$W_{\delta 3}$ – ES real protection against all known and the potential cryptanalytic attacks;

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

$W_{\delta 5}$ – ES type cryptographic transformation in a group of EC points theoretical protection;

$W_{\delta 6}$ – the absence of ES type cryptographic transformation weak private key;

$W_{\delta 7}$ – the complexity of the direct I_{np} and reverse $I_{зв}$ cryptographic transformations regarding ES is not higher than polynomial character.

Since the presented partial criteria are unconditional, then the selection criterion is a logical variable yes/no (1/0), so unconditional criterion can be written as [6]:

$$\left(W_{\delta 1}, W_{\delta 2}, W_{\delta 3}, W_{\delta 4}, W_{\delta 5}, W_{\delta 6}, W_{\delta 7}\right) \in (1,0). \quad (1)$$

Given the described above partial unconditional criteria $W_{\delta 1}$–$W_{\delta 7}$ and condition (1) cryptographic transformation accordance function can be presented as:

$$f_{фв}(\ ) = \mathrm{W}_{\delta 1} \wedge \mathrm{W}_{\delta 2} \wedge \mathrm{W}_{\delta 3} \wedge \mathrm{W}_{\delta 4} \wedge \mathrm{W}_{\delta 5} \wedge \mathrm{W}_{\delta 6} \wedge \mathrm{W}_{\delta 7}. \quad (2)$$

Hence, the quality of ES cryptographic transformation can be estimated using unconditional integral criterion – ES cryptographic transformation accordance function to requirements $f_{фв}(\ ) \in (0;1)$ and on $f_{фв}(\ ) = 1$ ES cryptographic transformation, that estimated, complies with the requirements.

Introduced thereby integral criterion allows to establish, whether the considered ES type cryptographic transformation complies considered discussed requirements. If the ES complies with the requirements, it can be reasonably recommended for use.

Provided a positive assessment of ES by integral unconditional criterion, further comparison and evaluation can be made based on the conditional criteria and integral conditional criterion [6].

3.3 ES mechanisms evaluation by conditional criteria

Research has shown that qualitative and quantitative comparison of ES type cryptographic transformations can be carried out using generalized conditional preference criterion [6] or integral conditional criterion.

As the main partial conditional criteria can (proposed) use the following:

W_{y1} – the possibility and conditions of free distribution and use of international or national ES cryptographic transformations standard in Ukraine taking into account Ukraine normative acts to export, import and restrictions on its use, including the provision of electronic trust services;

W_{y2} – the level of trust in international and national cryptographic transformation in a group of EC points standard, that defined by the results of researches and the degree of application extension and recognition in different countries, and internationally recognized systems, including for the provision of electronic trust services;

W_{y3} – the perspective of international or national standard application in Ukraine taking into account recognition and application perspective information and telecommunication systems, cloud computing and other information technology etc.;

W_{y4} – timing and spatial complexity of hardware, software, and hardware and software implementations ES means, and management and key certification, including for the provision of electronic trust services etc.;

W_{y5} – the possibility and conditions for the use of standards with different values of general system settings and keys, methods of making and maintenance public key certificates, including for the providing electronic trust services, etc.;

W_{y6} – ES flexibility degree from the standpoint of use in various applications, by different requirements and restrictions, in different conditions, the unification and standardization degree, including for the providing electronic trust services, etc.;

W_{y7} – the level of protection in the implementation of different types of threats, in different conditions of cryptanalytic attacks and rejection common parameters properties from the defined etc.;

W_{y8} – the possibility and conditions of use in the construction of anonymous signatures for national and international use, and the level of ensuring the anonymity.

Table 1 – Relations scale (degree of actions importance)

The importance degree	Definition	Explanation
1	**Equal importance**	Two actions do the same contribution to achieve the objective
3	Some advantage of one action importance over another (weak importance)	There are understandings in favor of advantage of one of the actions, but these understandings not enough convincing
5	**Substantial or strong importance**	There are reliable data or logical statements in order to show the advantage of one of the actions
7	**Obvious or very strong importance**	Convincing evidence in favor of one activity to another
9	**Absolute importance**	Evidence in favor of the advantage of one action to another supremely persuasive
2, 4, 6, 8	Intermediate values between two adjacent statements	The situation when it is necessary to compromise decision
Inverse values given above non-zero values	If to the actions i at comparison with the action j is ascribed one of the above mentioned non-zero integers, then to actions j at comparison with the action i is ascribed the reverse value	If coherence was postulated in obtaining N numerical values to form the matrix

If their application it is important to choose the method of clotting the partial conditional criteria to integral conditional criterion. The conducted analysis and practical researches have shown [4-6, 8-11, 15-21] that as a method of clotting the partial conditional criteria can choose the analytic hierarchy process based on pairwise comparisons and the weight indices determining method.

When using the analytic hierarchy process based on pairwise comparisons, obtained statements expressed in integers taking into account nine-point scale (table. 1) [4,6].

3.4 The ES mechanisms according to DSTU ISO/IEC 14888-3:2014 by unconditional criteria evaluation

Table 2 shows the results of comparative analysis regarding unconditional criteria for ES mechanisms according to DSTU ISO/IEC 14888-3:2014. Further comparison and evaluation based on conditional criteria and integral conditional criterion will be carried out for all standard ES mechanisms, other than ES mechanisms DSA, KCDSA, Pointcheval/Vaudenay and SDSA, that mechanisms, based on the finite fields mathematical apparatus.

Table 2 – Results of comparative analysis regarding unconditional criteria

ES criterion / ES algorithm	$W_{\delta 1}$	$W_{\delta 2}$	$W_{\delta 3}$	$W_{\delta 4}$	$W_{\delta 5}$	$W_{\delta 6}$	$W_{\delta 7}$	W_{δ}
DSA	0	1	0	1	0	1	1	0
KCDSA	0	1	0	1	0	1	1	0
Pointcheval/Vaudenay	0	1	0	1	0	1	1	0
SDSA	0	1	0	1	0	1	1	0
EC-DSA	1	1	1	1	1	1	1	1
EC-KCDSA	1	1	1	1	1	1	1	1
EC-GDSA	1	1	1	1	1	1	1	1
EC-RDSA	1	1	1	1	1	1	1	1
EC-SDSA	1	1	1	1	1	1	1	1
EC-FSDSA	1	1	1	1	1	1	1	1
IBS-1	1	1	1	1	1	1	1	1
IBS-2	1	1	1	1	1	1	1	1

3.5 The ES mechanisms according to DSTU ISO/IEC 9796-3:2014 by unconditional criteria evaluation

Table 3 shows the results of comparative analysis regarding unconditional criteria for ES mechanisms according to DSTU ISO/IEC 9796-3:2014.

Table 3 – Results of comparative analysis regarding unconditional criteria

ES criterion / ES algorithm	$W_{\delta 1}$	$W_{\delta 2}$	$W_{\delta 3}$	$W_{\delta 4}$	$W_{\delta 5}$	$W_{\delta 6}$	$W_{\delta 7}$	W_{δ}
NR	1	1	1	1	1	1	1	1
ECNR	1	1	1	1	1	1	1	1
ECMR	1	1	1	1	1	1	1	1
ECAO	1	1	1	1	1	1	1	1
ECPV	1	1	1	1	1	1	1	1
ECKNR	1	1	1	1	1	1	1	1

Further comparison and evaluation based on conditional criteria and integral conditional criterion will be carried out for all standard ES mechanisms.

4 The analytic hierarchy process based on pairwise comparisons and features of its use for the ES algorithms evaluation

For use the analytic hierarchy process must choose a conditional criteria system. With such set of indicators, using the conditional criteria can calculate the integral conditional criteria value, and, consequently, make the comparison by integral conditional criterion.

The elements pairwise comparison method [4,6] can be described as follows. The set of paired comparisons matrices is constructed. Paired comparisons are carried out in terms of the dominance of one element over another. Obtained statements are expressed in integers, considering the nine scale in table 1 [4,6].

4.1 The analytic hierarchy process application analysis and conditions in cryptography

Analytic hierarchy process (AHP) – the systematic approach to the complex problems of making decision mathematical tool. AHP does not prescribe to the decision making person (DMP) any "right" decision, and allows him to interactively find this option (alternative), which the best agrees with its understanding of the problem essence and requirements to its solution [5,10,15,21].

This method belongs to the criteria class and is widely utilized at present, including in evaluative activity. Method is based on alternatives evaluating hierarchical procedure. It is represented as follows [5,21]:

Level 0: objective – to estimate the weight of approach to the evaluation.

Level 1: criteria – the reliability of the results; the conformity to the evaluation objectives.

Level 2: criteria – the reliability, due to the authenticity of the information; the reliability, due to the latitude of the information.

The analytic hierarchy process contains the priorities synthesis procedure, that are calculated on the basis of objective experts' statements.

The analytic hierarchy process application [5,21]:

1. The construction of the hierarchy quality problem model, includes objective, alternative options of the objective achieve and criteria for alternatives quality evaluation.
2. Setting all hierarchy elements priorities using the pair comparisons method.
3. The synthesis of global alternatives priorities by elements on hierarchy priorities linear convolution.
4. Check the statements on consistency.
5. Decision making based on the results.

If using AHP using so-called objectives tree (fig. 2).

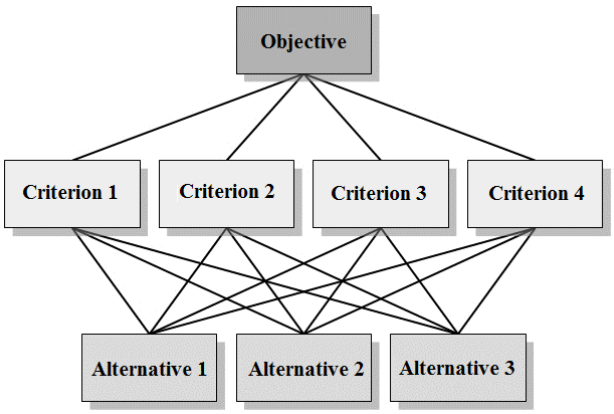

Figure 2 – Simple AHP hierarchy *(Objectives tree)*

4.2 The pairwise comparison method application analysis and conditions in cryptography

In pairwise comparison the expert compares investigated objects of their importance pairwise, establishing the most important object in each pair. All possible pairs of objects expert represents in a record of each combination (object 1 – object 2, object 2 – object 3, etc.) or in the matrix form [4,6].

The paired comparisons method is very simple and it allows to explore a large number of objects (compared, for example, by a rank method) and with greater accuracy [4].

Let $E_1,E_2,...,E_n$ – the plenty of n elements (alternatives) and $v_1,v_2,...,v_n$ – respectively their weight or intensity. Let compare pairwise the weight or intensity of each element with weight or intensity of any other element of the set relative to common to them property or objective (relative to father"–element). In this case, the pairwise comparisons matrix [E] is as follows:

The pairwise comparisons matrix has a reverse symmetry property, that is, $a_{ij}=1/a_{ji}$, where $a_{ij}=v_i/v_j$. In conducting pairwise comparisons should answer the following questions: which of the two compared elements is more important or has greater impact, which is more probable and which has a greater advantage.

When comparing the criteria, usually ask, which criterion is more important; when comparing alternatives in relation to the criterion – which of the alternatives has more advantages or more probable [4,6].

$[E] =$

	E_1	E_2	…	E_n
E_1	v_1/v_2	v_1/v_2	…	v_1/v_n
E_2	v_2/v_1	v_2/v_2	…	v_2/v_n
…	…	…	…	…
E_n	v_n/v_1	v_n/v_2	…	v_n/v_n

When constructing a pairwise comparisons matrix for all criteria, it is necessary to determine the consistency ratio [4,6] for each of criterion as follows. The assessment of eigenvector component is calculated by the formula (3):

$$q_i = (W_{yi} \times W_{yi+1} \times \ldots \times W_{yn})^{\frac{1}{n}}. \quad (3)$$

The normalized assessment of priority vector is calculated by the formula (4):

$$r_i = q_i \div z, \quad (4)$$

where z – consistency matrix ratio, which is calculated using the formula (5):

$$z = \sum_{i=1}^{n} q_i. \quad (5)$$

The consistency matrix ratio value is in the range $[0, \sum_{i=1}^{n} q_{i\max}]$, where $q_{i\max}$ – the maximum possible eigenvector component evaluation value for the selected case.

4.3 The ES mechanisms according to DSTU ISO/IEC 14888-3:2014 comparative analysis

Let us consider the practical application of the analytic hierarchy process based on pairwise comparisons on the example of ES mechanisms according to standard DSTU ISO/IEC 14888-3:2014. Comparing the ES algorithms relatively conditional criteria, construct for this objectives tree (fig. 3).

Now do the evaluation of each criterion. For this construct the pairwise comparisons matrix rela-

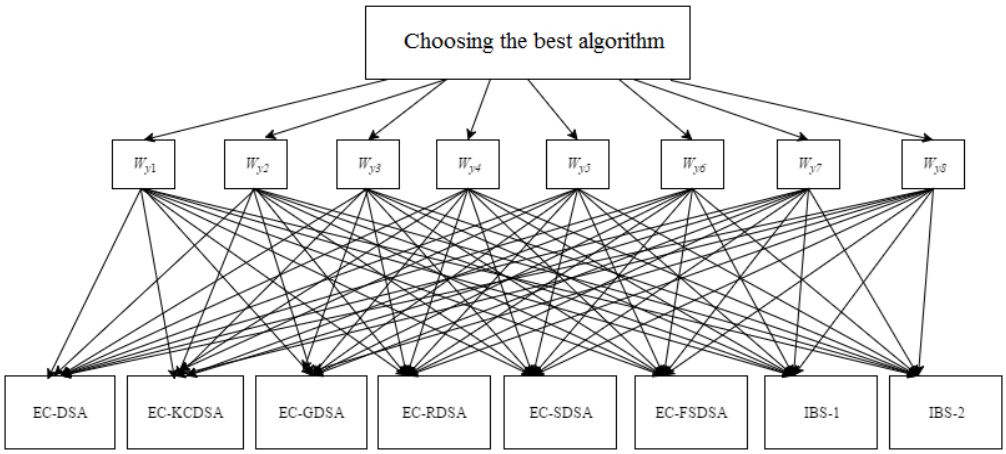

Figure 3 – Objectives tree (for DSTU ISO/IEC 14888-3:2014)

tive to the compared ES algorithms for each criterion (tabl. 4). As an example, we present a pairwise comparisons matrix relative to the compared ES algorithms for criterion W_{y1}. For this we construct table 5, using the formulas (3) – (5).

Table 4 – The criteria contribution to achieve a common objective, pairwise comparisons matrix

	W_{y1}	W_{y2}	W_{y3}	W_{y4}	W_{y5}	W_{y6}	W_{y7}	W_{y8}	q_j	r_j
W_{y1}	1	1/6	4	1/4	1/2	1/3	1/7	3	0,575	0,048
W_{y2}	6	1	4	5	4	3	1/7	5	2,38	0,198
W_{y3}	1/4	1/4	1	3	2	1/2	1/7	1	0,636	0,053
W_{y4}	4	1/5	1/3	1	1/4	1/4	1/7	1/6	0,376	0,031
W_{y5}	2	1/4	1/2	4	1	1/3	1/7	1/4	0,575	0,048
W_{y6}	3	1/3	2	4	3	1	1/7	1	1,167	0,097
W_{y7}	7	7	7	7	7	7	1	7	5,489	0,456
W_{y8}	1/3	1/5	1	6	4	1	1/7	1	0,832	0,069

Other pairwise comparisons matrices are constructed similarly [4,6]. To calculate the resulting priorities vector multiply the level 1 priority vector and the level 1 acquired values matrix (fig. 4).

$$v := \begin{pmatrix} 0.048 \\ 0.198 \\ 0.053 \\ 0.031 \\ 0.048 \\ 0.097 \\ 0.456 \\ 0.069 \end{pmatrix} \qquad M := \begin{pmatrix} 0.201 & 0.087 & 0.082 & 0.076 & 0.166 & 0.21 & 0.051 & 0.205 \\ 0.201 & 0.169 & 0.165 & 0.061 & 0.166 & 0.229 & 0.102 & 0.19 \\ 0.201 & 0.124 & 0.165 & 0.103 & 0.166 & 0.192 & 0.086 & 0.19 \\ 0.029 & 0.025 & 0.021 & 0.05 & 0.049 & 0.027 & 0.02 & 0.028 \\ 0.067 & 0.054 & 0.06 & 0.08 & 0.099 & 0.043 & 0.036 & 0.047 \\ 0.067 & 0.054 & 0.06 & 0.08 & 0.099 & 0.043 & 0.036 & 0.047 \\ 0.118 & 0.244 & 0.233 & 0.275 & 0.128 & 0.129 & 0.334 & 0.147 \\ 0.118 & 0.244 & 0.233 & 0.275 & 0.128 & 0.129 & 0.344 & 0.147 \end{pmatrix}$$

$$V2 := M \cdot v \qquad V2^T = (0.099 \;\; 0.144 \;\; 0.125 \;\; 0.025 \;\; 0.048 \;\; 0.048 \;\; 0.256 \;\; 0.256)$$

Figure 4 – The resulting priorities vector calculation

The consistency ratio is 12,03. The consistency ratio of the pairwise comparisons matrix by criterion W_{y1} is 9,54.

Table 5 – The pairwise comparisons matrix by criterion W_{y1}

	EC-DSA	EC-KCDSA	EC-GDSA	EC-RDSA	EC-SDSA	EC-FSDSA	IBS-1	IBS-2	q_j	r_j
EC-DSA	1	1	1	5	3	3	2	2	1,914	0,201
EC-KCDSA	1	1	1	5	3	3	2	2	1,914	0,201
EC-GDSA	1	1	1	5	3	3	2	2	1,914	0,201
EC-RDSA	1/5	1/5	1/5	1	1/3	1/3	1/5	1/5	0,278	0,029
EC-SDSA	1/3	1/3	1/3	3	1	1	1/2	1/2	0,639	0,067
EC-FSDSA	1/3	1/3	1/3	3	1	1	1/2	1/2	0,639	0,067
IBS-1	1/2	1/2	1/2	5	2	2	1	1	1,121	0,118
IBS-2	1/2	1/2	1/2	5	2	2	1	1	1,121	0,118

Let us consider the obtained numerical results. The investigated ES algorithms based on the transformation of group of EC points and pairing EC points can arrange the places, that they occupied on the results of comparison (1 – the best, 8 – the worst):

1. IBS-1 – 0,256;
2. IBS-2 – 0,256;
3. EC-KCDSA – 0,144;
4. EC-GDSA – 0,125;
5. EC-DSA – 0,099;
6. EC-SDSA – 0,048;
7. EC-FSDSA – 0,048;
8. EC-RDSA – 0,025.

Thus ES IBS-1,2 have the greatest advantages by an integral indicator. The ES algorithm EC-RDSA has the worst result, that is substantiated by the attacks implementation on the algorithm and the inability to use nationally. It should be noted, that the results cannot be taken for use, most likely, this is the ES comparison technique. For real use you'll need to choose conditional criteria and conduct researches.

4.4 The ES mechanisms according to DSTU ISO/IEC 9796-3:2014 comparative analysis

Let us consider the practical application of the analytic hierarchy process based on pairwise comparisons on the example of ES mechanisms according to standard DSTU ISO/IEC 9796-3:2014. Comparing the ES algorithms relatively conditional criteria, construct for this objectives tree (fig. 5).

Now do the evaluation of each criterion. For this construct the pairwise comparisons matrix relative to the compared ES algorithms for each criterion (table. 6).

The consistency ratio is 7,7037.

As an example, we present a pairwise comparisons matrix relative to the compared ES algorithms for criterion W_{y1}. For this we construct table 7, using the formulas (3) – (5). Other pairwise comparisons matrices are constructed similarly [4,6].

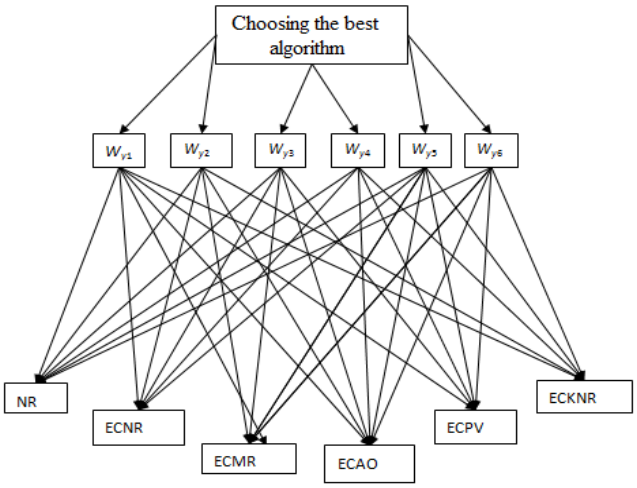

Figure 5 – Objectives tree

(for DSTU ISO/IEC 9796-3:2014)

Table 6 – The criteria contribution to achieve a common objective, pairwise comparisons matrix

	W_{y1}	W_{y2}	W_{y3}	W_{y4}	W_{y5}	W_{y6}	q_j	r_j
W_{y1}	1	1/6	4	1/4	1/2	1/3	0,5503	0,0714
W_{y2}	6	1	4	5	4	3	3,3604	0,4362
W_{y3}	1/4	1/4	1	3	2	1/2	0,7565	0,0982
W_{y4}	4	1/5	1/3	1	1/4	1/4	0,5054	0,0656
W_{y5}	2	1/4	1/2	4	1	1/3	0,8327	0,1081
W_{y6}	3	1/3	2	4	3	1	1,6984	0,2205

To calculate the resulting priorities vector multiply the level 1 priority vector and the level 1 acquired values matrix (fig. 6).

Let us consider the obtained numerical results. The investigated ES algorithms can arrange the places, that they occupied on the results of comparison (1 – the best, 6 – the worst):

1. ECPV – 0,252;
2. ECNR – 0,165;
3. ECAO – 0,155;
4. ECKNR– 0,139;
5. ECMR – 0,133;
6. NR – 0,108.

Table 7 – The pairwise comparisons matrix by criterion W_{y1}

	NR	ECNR	ECMR	ECAO	ECPV	ECKNR	q_j	r_j
NR	1	1/5	2	1/2	1/5	1/3	0,487	0,072
ECNR	5	1	1/4	3	2	3	1,680	0,25
ECMR	1/2	4	1	1/2	1/4	1/2	0,707	0,105
ECAO	2	1/3	2	1	1/4	1/3	0,693	0,103
ECPV	5	1/2	4	4	1	1/2	1,647	0,245
ECKNR	3	1/3	2	3	2	1	1,513	0,225

The consistency ratio is 6,72.

$$B1 := \begin{pmatrix} 0.071 \\ 0.436 \\ 0.098 \\ 0.065 \\ 0.108 \\ 0.220 \end{pmatrix} \qquad B2 := \begin{pmatrix} 0.072 & 0.05 & 0.105 & 0.103 & 0.245 & 0.025 \\ 0.101 & 0.16 & 0.080 & 0.140 & 0.334 & 0.127 \\ 0.042 & 0.27 & 0.08 & 0.161 & 0.373 & 0.146 \\ 0.046 & 0.104 & 0.343 & 0.157 & 0.068 & 0.280 \\ 0.167 & 0.167 & 0.167 & 0.167 & 0.167 & 0.167 \\ 0.152 & 0.183 & 0.193 & 0.192 & 0.136 & 0.142 \end{pmatrix}$$

$$B := B1^{T} \cdot B2 = (0.108 \quad 0.165 \quad 0.133 \quad 0.155 \quad 0.252 \quad 0.139)$$

Figure 6 – The resulting priorities vector calculation

The most perspective in DSTU ISO/IEC 9796-3:2014 are ES mechanisms ECPV (*elliptic curve Pintsov-Vanstone message recovery signature*) and ECNR (*elliptic curve Nyberg-Rueppel message recovery signature*). ECPV uses symmetric encryption (to include information in the signature) and does not provide limits on the amount of renewable information. NR algorithm has the worst result by an integral indicator, that is substantiated by mathematical apparatus, that is used in this algorithm.

5 Method and procedure of evaluation and comparative analysis ES algorithms based on weight indices

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. There are several such methods [9,11,18-20], some of them are considered detail below.

Let us consider the general problem formulation for ES evaluation technique based on the determining the weight indices method.

Let there are [9,11,18-20]:

1) *k* systems (ES mechanisms), which is necessary to evaluate;

2) *m* indicators, according to which systems are evaluated;

3) n experts, that carry out the evaluation.

We define some partial indicators, at which can be evaluated ES mechanisms:

x_1 – the possibility of free distribution and use of international or national ES cryptographic transformations standard in Ukraine;

x_2 – the level of trust in international and national cryptographic transformation in a group of EC points and based on mathematical apparatus of pairing EC points;

x_3 – the perspective of international or national standard application in Ukraine;

x_4 – the timing and spatial complexity of hardware, software, and hardware and software implementations ES means;

x_5 – the possibility of the standards use with different values of general system settings and keys;

x_6 – the ES algorithm flexibility degree from the standpoint of use in various applications, by different requirements and restrictions;

x_7 – the level of protection against the different types of threats in different conditions of cryptanalytic attacks;

x_8 – the possibility of use ES algorithm in the construction of anonymous signatures for national and international use, and the level of ensuring the anonymity.

Now determine the weight indices values of indicators themselves. We carry out the expert evaluation of the above partial indicators for this purpose. We'll use the following methods for the weight indices determining [9,11,18-20,22] for evaluation: 1 - using the Fishburn scale; 2 - based on the ranking method; 3 - based on the points attribution method; 4 - based on the numerical method.

After the weight indices values of indicators themselves determining, it is necessary to make the system expert evaluation by the chosen determining weight indices methods.

For this, for each system it is need to perform the indicators ranking in connection with that, which indicator is the most determined in chosen system, better than other describes it. That is, arrange the indicators in relation to the chosen system, from more significant to least significant.

5.1 The weight indices determining method, evaluations and comparative analysis of ES mechanisms according to DSTU ISO/IEC 14888-3:2014 using the Fishburn scale

Let as input is selected the following:

n – the number of experts, n=5

m – the number of indicators, m=8

We construct the table of the Fishburn scale method indicators value for ES algorithms of standard DSTU ISO/IEC 14888-3:2014 (EC-DSA, EC-GDSA, EC-KCDSA, EC-RDSA, EC-SDSA, EC-FSDSA, IBS-1 and IBS-2), accordance with the rules of the evaluation according to the specified method. The results are shown in table 8.

Table 8 – Weight indices values

Experts	**Indicators**							
	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
1	0,194	0,167	0,111	0,139	0,056	0,028	0,222	0,083
2	0,194	0,167	0,111	0,083	0,028	0,056	0,222	0,139
3	0,222	0,139	0,111	0,056	0,028	0,083	0,194	0,167
4	0,222	0,111	0,139	0,028	0,083	0,056	0,194	0,167
5	0,167	0,139	0,028	0,056	0,111	0,083	0,222	0,194
w_i	0,200	0,144	0,100	0,072	0,061	0,061	0,211	0,150

Similarly, we construct tables for all ES mechanisms according to DSTU ISO/IEC 14888-3:2014. After the evaluation, we obtain the following results, shown in fig. 7.

$$M\_Fishbem := \begin{pmatrix} 0.211 & 0.172 & 0.128 & 0.078 & 0.044 & 0.072 & 0.161 & 0.156 \\ 0.2 & 0.189 & 0.144 & 0.05 & 0.056 & 0.094 & 0.128 & 0.139 \\ 0.194 & 0.167 & 0.139 & 0.05 & 0.05 & 0.072 & 0.161 & 0.167 \\ 0.067 & 0.061 & 0.072 & 0.2 & 0.194 & 0.189 & 0.106 & 0.111 \\ 0.061 & 0.05 & 0.056 & 0.167 & 0.172 & 0.167 & 0.167 & 0.161 \\ 0.061 & 0.05 & 0.056 & 0.161 & 0.161 & 0.183 & 0.178 & 0.15 \\ 0.183 & 0.122 & 0.128 & 0.206 & 0.078 & 0.044 & 0.211 & 0.167 \\ 0.183 & 0.122 & 0.128 & 0.206 & 0.078 & 0.044 & 0.211 & 0.167 \end{pmatrix}$$

$V\_Fishbem := w\_pokaz1$

$V\_Fishbem = (0.2 \quad 0.144 \quad 0.1 \quad 0.072 \quad 0.061 \quad 0.061 \quad 0.211 \quad 0.15)$

$Rez\_Fishbem := M\_Fishbem \cdot V\_Fishbem^T$

$Rez\_Fishbem^T = (0.15 \quad 0.142 \quad 0.147 \quad 0.106 \quad 0.117 \quad 0.118 \quad 0.159 \quad 0.159)$

Figure 7 – The priorities resulting vector calculation

Further carry out analysis of the results according to fig. 7. For this we place *Rez_Fishbern* values as they decrease, i.e.

1. IBS-1 – 0,159;
2. IBS-2 – 0,159;
3. EC-DSA – 0,15;
4. EC-GDSA – 0,147;
5. EC-KCDSA – 0,142;
6. EC-FSDSA – 0,118;
7. EC-SDSA – 0,117;
8. EC-RDSA – 0,106.

It should be noted, that the results cannot be taken for use, most likely, this is the ES comparison technique. For real use you'll need to choose conditional criteria and conduct researches.

5.2 The weight indices determining method, evaluations and comparative analysis of ES mechanisms according to DSTU ISO/IEC 9796-3:2014 using the Fishburn scale

Let as input is selected the following:

n – the number of experts, $n=4$

m – the number of indicators, $m=6$

Table 9 – Ranking indicators by experts

Indicators / Experts	x_1	x_2	x_3	x_4	x_5	x_6
1	1	6	5	2	3	4
2	3	4	6	1	5	2
3	1	4	5	3	6	2
4	2	3	6	1	4	5

We construct the table of the Fishburn scale method indicators value for ES algorithms of standard DSTU ISO/IEC 9796-3, accordance with the rules of the evaluation according to the specified method. The results are shown in table 9–10. Similarly, we construct tables for all ES mechanisms according to DSTU ISO/IEC 9796-3:2014.

Table 10 – Weight indices values

Experts	Indicators					
	x_1	x_2	x_3	x_4	x_5	x_6
1	0,285	0,047	0,095	0,238	0,190	0,142
2	0,190	0,142	0,047	0,285	0,095	0,238
3	0,285	0,142	0,095	0,190	0,047	0,238
4	0,238	0,190	0,047	0,285	0,142	0,095
w_i	0,249	0,130	0,071	0,249	0,118	0,178

After the evaluation, we obtain the following results, shown in fig. 8.

Further carry out analysis of the results according to fig. 8. For this we place *Rez_1* values as they decrease, i.e.

1. ECPV – 0,245;
2. ECNR – 0,223;
3. ECAO – 0,186;
4. ECKNR – 0,179;
5. ECMR – 0,160;
6. NR – 0,144.

It should be noted, that the results cannot be taken for use, most likely, this is the ES comparison technique. For real use you'll need to choose conditional criteria and conduct researches.

$$M\_1 := \begin{bmatrix} 0.142 & 0.130 & 0.273 & 0.106 & 0.249 & 0.094 \\ 0.273 & 0.130 & 0.082 & 0.190 & 0.379 & 0.226 \\ 0.094 & 0.189 & 0.166 & 0.249 & 0.237 & 0.059 \\ 0.225 & 0.190 & 0.566 & 0.106 & 0.154 & 0.118 \\ 0.118 & 0.273 & 0.237 & 0.522 & 0.142 & 0.094 \\ 0.273 & 0.094 & 0.142 & 0.202 & 0.201 & 0.08 \end{bmatrix}$$

$$V\_F := \begin{bmatrix} 0.249 & 0.130 & 0.071 & 0.249 & 0.118 & 0.178 \end{bmatrix}$$

$$Rez\_1 := M\_1 \cdot V\_F^{\mathrm{T}}$$

$$Rez\_1^{\mathrm{T}} = \begin{bmatrix} 0.144 & 0.223 & 0.16 & 0.186 & 0.245 & 0.179 \end{bmatrix}$$

Figure 8 – The priorities resulting vector calculation

5.3 The weight indices determining method, evaluations and comparative analysis of ES mechanisms according to DSTU ISO/IEC 14888-3:2014 based on the ranking method

n – the number of experts, n=5

m – the number of indicators, m=8

We construct the table for indicators, accordance with the rules of the evaluation according to the specified method (table 11).

Table 11 – Weight indices values

Experts	Indicators							
	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
1	7	6	5	4	2	1	8	3
2	8	7	5	3	1	2	6	4
3	8	6	4	3	2	1	7	5
4	7	6	3	4	1	2	8	5
5	6	7	5	3	2	1	8	4
$r_j = \sum_{i=1}^{n} r_{ij}$	36	32	22	17	8	7	37	21
w_j	0,2	0,178	0,122	0,094	0,044	0,039	0,206	0,117

Similarly, we construct tables for all ES mechanisms according to DSTU ISO/IEC 14888-3:2014. After the evaluation, we obtain the following results, shown in fig. 9.

$$M\_Ranj := \begin{pmatrix} 0.189 & 0.183 & 0.156 & 0.1 & 0.067 & 0.061 & 0.072 & 0.172 \\ 0.189 & 0.161 & 0.122 & 0.056 & 0.072 & 0.094 & 0.15 & 0.156 \\ 0.194 & 0.15 & 0.172 & 0.05 & 0.061 & 0.106 & 0.144 & 0.122 \\ 0.05 & 0.05 & 0.067 & 0.133 & 0.194 & 0.2 & 0.133 & 0.172 \\ 0.05 & 0.061 & 0.056 & 0.167 & 0.167 & 0.167 & 0.167 & 0.167 \\ 0.056 & 0.061 & 0.05 & 0.156 & 0.15 & 0.161 & 0.183 & 0.183 \\ 0.178 & 0.122 & 0.089 & 0.106 & 0.078 & 0.044 & 0.211 & 0.172 \\ 0.178 & 0.122 & 0.089 & 0.106 & 0.078 & 0.044 & 0.211 & 0.172 \end{pmatrix}$$

$$V\_Ranj := w\_pokaz2$$

$$V\_Ranj = (0.2 \quad 0.178 \quad 0.122 \quad 0.094 \quad 0.044 \quad 0.039 \quad 0.206 \quad 0.117)$$

$$Rez\_Ranj := M\_Ranj \cdot V\_Ranj^{T}$$

$$Rez\_Ranj^{T} = (0.139 \quad 0.143 \quad 0.142 \quad 0.103 \quad 0.111 \quad 0.115 \quad 0.147 \quad 0.147)$$

Figure 9 – The priorities resulting vector calculation

Further we carry out analysis of the results according to fig. 9. For this we place *Rez_Ranj* values as they decrease, i.e.

1. IBS-1 – 0,147;
2. IBS-2 – 0,147;
3. EC-KCDSA – 0,143;
4. EC-GDSA – 0,142;
5. EC-DSA – 0,139;
6. EC-FSDSA – 0,115;
7. EC-SDSA – 0,111;
8. EC-RDSA – 0,103.

Thus ES IBS-1 and IBS-2 have the greatest advantages by the integral indicator. ES algorithm EC-RDSA (*as in the case of the analytic hierarchy process and method based on the Fishburn scale comparison*) has the worst result, that is substantiated by attack implementation on this algorithm and its inability to use nationally.

5.4 The weight indices determining method, evaluations and comparative analysis of ES mechanisms according to DSTU ISO/IEC 9796-3:2014 based on the ranking method

n – the number of experts, n=4

m – the number of indicators, m=6

We construct the table for indicators, accordance with the rules of the evaluation according to the specified method (table 12). Similarly, we construct tables for all ES mechanisms according to DSTU ISO/IEC 9796-3:2014.

Table 12 – Weight indices values

Experts	**Indicators**					
	x_1	x_2	x_3	x_4	x_5	x_6
1	5	1	4	6	3	2
2	4	2	6	5	3	1
3	5	3	6	4	2	1
4	5	2	4	6	1	3
$r_j = \sum_{i=1}^{n} r_{ij}$	19	8	20	21	9	7
w_j	0,226	0,095	0,238	0,250	0,226	0,083

After the evaluation, we obtain the following results, shown in fig. 10. Further we carry out analysis of the results according to fig. 10. For this we place *Rez_2* values as they decrease, i.e.

1. ECNR – 0,209;
2. ECPV – 0,207;
3. ECKNR – 0,200;
4. ECAO – 0,179;
5. ECMR – 0,168;
6. NR – 0,157.

Thus ES ECNR has the greatest advantages by the integral indicator. ES algorithm NR (*as in the case of the analytic hierarchy process and method based on the Fishburn scale comparison*) has the worst result, that is substantiated by mathematical apparatus used in this algorithm.

$$M\_2 := \begin{bmatrix} 0.130 & 0.270 & 0.178 & 0.059 & 0.107 & 0.250 \\ 0.107 & 0.059 & 0.238 & 0.202 & 0.273 & 0.119 \\ 0.071 & 0.190 & 0.071 & 0.166 & 0.238 & 0.261 \\ 0.154 & 0.261 & 0.059 & 0.261 & 0.130 & 0.130 \\ 0.250 & 0.130 & 0.095 & 0.238 & 0.226 & 0.059 \\ 0.107 & 0.059 & 0.154 & 0.238 & 0.261 & 0.178 \end{bmatrix}$$

$$V\_2 := [0.226 \quad 0.095 \quad 0.238 \quad 0.250 \quad 0.226 \quad 0.083]$$

$$Rez\_2 := M\_2 \cdot V\_2^{\mathrm{T}}$$

$$Rez\_2^{\mathrm{T}} = [0.157 \quad 0.209 \quad 0.168 \quad 0.179 \quad 0.207 \quad 0.2]$$

Figure 10 – The priorities resulting vector calculation

5.5 The weight indices determining method, evaluations and comparative analysis of ES mechanisms according to DSTU ISO/IEC 14888-3:2014 based on the points attribution method

n – the number of experts, n=5

m – the number of indicators, m=8

We construct the table for indicators, accordance with the rules of the evaluation according to the specified method (table 13). Similarly, we construct tables for all ES mechanisms according to DSTU ISO/IEC 14888-3:2014.

Table 13 – Weight indices values

Indicators / Experts	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	$\sum_{j=1}^{m} h_{ij}$	Indicators weights							
										r_{i1}	r_{i2}	r_{i3}	r_{i4}	r_{i5}	r_{i6}	r_{i7}	r_{i8}
1	7	5	2	4	6	1	10	8	43	0,163	0,116	0,046	0,093	0,139	0,023	0,232	0,186
2	6	5	3	4	9	2	8	7	44	0,136	0,114	0,068	0,091	0,204	0,045	0,182	0,159
3	8	6	1	5	4	3	9	7	43	0,186	0,140	0,023	0,116	0,093	0,070	0,209	0,163
4	7	5	3	8	4	2	9	6	44	0,159	0,114	0,068	0,182	0,091	0,045	0,204	0,136
5	9	6	2	5	4	3	10	7	45	0,196	0,130	0,043	0,109	0,087	0,065	0,217	0,152
									$\sum_{i=1}^{n} r_j$	0,84	0,614	0,248	0,591	0,614	0,248	1,044	0,796
									w_j	0,168	0,123	0,050	0,118	0,123	0,050	0,209	0,159

After the evaluation, we obtain the following results, shown in fig. 11. Further we carry out analysis of the results according to fig. 11. For this we place *Rez_Bal* values as they decrease, i.e.

1. IBS-1 – 0,137;
2. IBS-2 – 0,137;
3. EC-RDSA – 0,132;
4. EC-FSDSA – 0,128;
5. EC-DSA – 0,127;
6. EC-SDSA – 0,127;
7. EC-GDSA – 0,126;
8. EC-KCDSA – 0,124.

$$M\_2 := \begin{bmatrix} 0.130 & 0.270 & 0.178 & 0.059 & 0.107 & 0.250 \\ 0.107 & 0.059 & 0.238 & 0.202 & 0.273 & 0.119 \\ 0.071 & 0.190 & 0.071 & 0.166 & 0.238 & 0.261 \\ 0.154 & 0.261 & 0.059 & 0.261 & 0.130 & 0.130 \\ 0.250 & 0.130 & 0.095 & 0.238 & 0.226 & 0.059 \\ 0.107 & 0.059 & 0.154 & 0.238 & 0.261 & 0.178 \end{bmatrix}$$

$$V\_2 := [0.226 \quad 0.095 \quad 0.238 \quad 0.250 \quad 0.226 \quad 0.083]$$

$$Rez\_2 := M\_2 \cdot V\_2^{\mathrm{T}}$$

$$Rez\_2^{\mathrm{T}} = [0.157 \quad 0.209 \quad 0.168 \quad 0.179 \quad 0.207 \quad 0.2]$$

Figure 11 – The priorities resulting vector calculation

5.6 The weight indices determining method, evaluations and comparative analysis of ES mechanisms according to DSTU ISO/IEC 9796-3:2014 based on the points attribution method

n – the number of experts, n=4
m – the number of indicators, m=6

We construct the table for indicators, accordance with the rules of the evaluation according to the specified method (table 14).

Table 14 – Weight indices values

Indicators / Experts	x_1	x_2	x_3	x_4	x_5	x_6	$\sum_{j=1}^{m} h_{ij}$	Indicators weights					
								r_{i1}	r_{i2}	r_{i3}	r_{i4}	r_{i5}	r_{i6}
1	8	7	10	2	5	4	36	0,222	0,194	0,277	0,055	0,138	0,111
2	7	8	9	1	4	3	32	0,218	0,250	0,281	0,031	0,125	0,093
3	9	5	7	1	3	2	27	0,333	0,185	0,259	0,037	0,111	0,074
4	8	6	10	1	4	3	32	0,250	0,187	0,312	0,031	0,125	0,093
							$\sum_{i=1}^{n} r_j$	1,023	0,816	1,129	0,154	0,499	0,371
							w_j	0,256	0,204	0,282	0,038	0,125	0,092

Similarly, we construct tables for all ES mechanisms according to DSTU ISO/IEC 9796-3:2014.

After the evaluation, we obtain the following results, shown in fig. 12.

Further we carry out analysis of the results according to fig. 12. For this we place *Rez_3* values as they decrease, i.e.

1. ECPV – 0,202;
2. ECNR – 0,170;
3. ECKNR – 0,162;
4. ECAO – 0,148;
5. ECMR – 0,138;
6. NR – 0,130.

Like in the previous method, ES NR has the worst result, that is substantiated by mathematical apparatus used in this algorithm.

ES mechanism ECPV has the best result.

$$M\_3 := \begin{bmatrix} 0.162 & 0.037 & 0.089 & 0.290 & 0.185 & 0.233 \\ 0.108 & 0.175 & 0.245 & 0.178 & 0.120 & 0.170 \\ 0.155 & 0.065 & 0.086 & 0.229 & 0.295 & 0.164 \\ 0.061 & 0.282 & 0.115 & 0.202 & 0.123 & 0.212 \\ 0.197 & 0.248 & 0.284 & 0.107 & 0.100 & 0.049 \\ 0.226 & 0.06 & 0.179 & 0.231 & 0.167 & 0.128 \end{bmatrix}$$

$$V\_3 := [0.256 \;\; 0.204 \;\; 0.282 \;\; 0.038 \;\; 0.125 \;\; 0.092]$$

$$Rez\_3 := M\_3 \cdot V\_3^{\mathrm{T}}$$

$$Rez\_3^{\mathrm{T}} = [0.13 \;\; 0.17 \;\; 0.138 \;\; 0.148 \;\; 0.202 \;\; 0.162]$$

Figure 12 – The priorities resulting vector calculation

5.7 The weight indices determining method, evaluations and comparative analysis of ES mechanisms according to DSTU ISO/IEC 14888-3:2014 based on the numerical method

n – the number of experts, n=5
m – the number of indicators, m=8

We construct the table for indicators, accordance with the rules of the evaluation according to the specified method (table 15). Coefficients values are selected from the method based on the Fishburn scale.

Similarly, we construct tables for all ES mechanisms according to DSTU ISO/IEC 14888-3:2014.

Table 15 – Weight indices values

Indicators / Evaluation	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
$x_{i\min}$	0,167	0,111	0,028	0,028	0,028	0,028	0,194	0,083
$x_{i\max}$	0,222	0,167	0,139	0,139	0,111	0,083	0,222	0,194
δ_i	0,250	0,333	0,800	0,800	0,750	0,667	0,125	0,571
w_i	0,058	0,078	0,186	0,186	0,175	0,155	0,029	0,133

After the evaluation, we obtain the following results, shown in fig. 13.

$$M\_Chisl := \begin{pmatrix} 0.065 & 0.075 & 0.131 & 0.196 & 0.131 & 0.229 & 0.075 & 0.098 \\ 0.059 & 0.059 & 0.101 & 0.156 & 0.156 & 0.205 & 0.117 & 0.147 \\ 0.09 & 0.103 & 0.15 & 0.16 & 0.16 & 0.18 & 0.069 & 0.09 \\ 0.166 & 0.147 & 0.166 & 0.055 & 0.055 & 0.055 & 0.178 & 0.178 \\ 0.15 & 0.15 & 0.15 & 0.113 & 0.113 & 0.113 & 0.113 & 0.097 \\ 0.155 & 0.155 & 0.155 & 0.117 & 0.117 & 0.117 & 0.087 & 0.1 \\ 0.095 & 0.05 & 0.158 & 0.18 & 0.21 & 0.168 & 0.032 & 0.108 \\ 0.095 & 0.05 & 0.158 & 0.18 & 0.21 & 0.168 & 0.032 & 0.108 \end{pmatrix}$$

$V\_Chisl := w\_pokaz4$

$V\_Chisl = (0.058 \;\; 0.078 \;\; 0.186 \;\; 0.186 \;\; 0.175 \;\; 0.155 \;\; 0.029 \;\; 0.133)$

$Rez\_Chisl := M\_Chisl \cdot V\_Chisl^{T}$

$Rez\_Chisl^{T} = (0.144 \;\; 0.138 \;\; 0.141 \;\; 0.109 \;\; 0.123 \;\; 0.126 \;\; 0.15 \;\; 0.15)$

Figure 13 – The priorities resulting vector calculation

Further we carry out analysis of the results according to fig. 13. For this we place *Rez_Chisl* values as they decrease, i.e.

1. IBS-1 – 0,15;
2. IBS-2 – 0,15;
3. EC-DSA – 0,144;
4. EC-GDSA – 0,141;
5. EC-KCDSA – 0,138;
6. EC-FSDSA – 0,126;
7. EC-SDSA – 0,123;
8. EC-RDSA – 0,109.

Also in this case it should be noted, that the results cannot be taken for use, most likely, this is the ES comparison technique. For real use you'll need to choose conditional criteria and conduct researches.

5.8 The weight indices determining method, evaluations and comparative analysis of ES mechanisms according to DSTU ISO/IEC 9796-3:2014 based on the numerical method

n – the number of experts, n=4

m – the number of indicators, m=6

We construct the table for indicators, accordance with the rules of the evaluation according to the specified method (table 16). Coefficients values are selected from the method based on the Fishburn scale.

Similarly, we construct tables for all ES mechanisms according to DSTU ISO/IEC 9796-3:2014.

Table 16 – Weight indices values

Indicators / Evaluation	x_1	x_2	x_3	x_4	x_5	x_6
$x_{i\min}$	0,190	0,047	0,047	0,190	0,047	0,095
$x_{i\max}$	0,285	0,190	0,095	0,285	0,190	0,238
δ_i	0,333	0,752	0,505	0,333	0,752	0,600
w_i	0,101	0,229	0,154	0,101	0,229	0,183

After the evaluation, we obtain the following results, shown in fig. 14.

$$M\_4 := \begin{bmatrix} 0.246 & 0.053 & 0.109 & 0.262 & 0.108 & 0.219 \\ 0.054 & 0.108 & 0.224 & 0.180 & 0.216 & 0.216 \\ 0.250 & 0.166 & 0.054 & 0.250 & 0.054 & 0.222 \\ 0.073 & 0.083 & 0.357 & 0.179 & 0.223 & 0.083 \\ 0.052 & 0.240 & 0.214 & 0.213 & 0.214 & 0.064 \\ 0.227 & 0.170 & 0.204 & 0.113 & 0.113 & 0.171 \end{bmatrix}$$

$$V\_4 := [0.101 \;\; 0.229 \;\; 0.154 \;\; 0.101 \;\; 0.229 \;\; 0.183]$$

$$Rez\_4 := M\_4 \cdot V\_4^{\mathrm{T}}$$

$$Rez\_4^{\mathrm{T}} = [0.145 \;\; 0.172 \;\; 0.15 \;\; 0.166 \;\; 0.175 \;\; 0.162]$$

Figure 14 – The priorities resulting vector calculation

Further we carry out analysis of the results according to fig. 14. For this we place *Rez_4* values as they decrease, i.e.

1. ECPV – 0,175;
2. ECNR – 0,172;
3. ECAO – 0,166;
4. ECKNR – 0,162;
5. ECMR – 0,150;
6. NR – 0,145.

Also in this case it should be noted, that the results cannot be taken for use, most likely, this is the ES comparison technique. For real use you'll need to choose conditional criteria and conduct researches.

6 The analysis of ES researches results according to DSTU ISO/IEC 14888-3:2014

For chosen ES mechanisms evaluation techniques were obtained results, that are shown in previous chapters. ES mechanisms comparison was made based on expert evaluations. After that, calculations were made by aforementioned techniques.

One can assume, that the results of the evaluation ES mechanisms according to DSTU ISO/IEC 14888-3:2014, by different methods have been obtained almost identical – almost the same ES mechanisms arrangement from the best to the worst. Numeric scatter of weight indices values for one algorithm is almost negligible, only numeric values for ES mechanisms IBS-1,2 in the analytic hierarchy process based on pairwise comparisons differ from weight indices values for these ES mechanisms according to other evaluation methods, that is substantiated by more strong influence of the subjective experts opinion.

Fig. 15 graphically shows the results of the ES mechanisms evaluation by different evaluation methods.

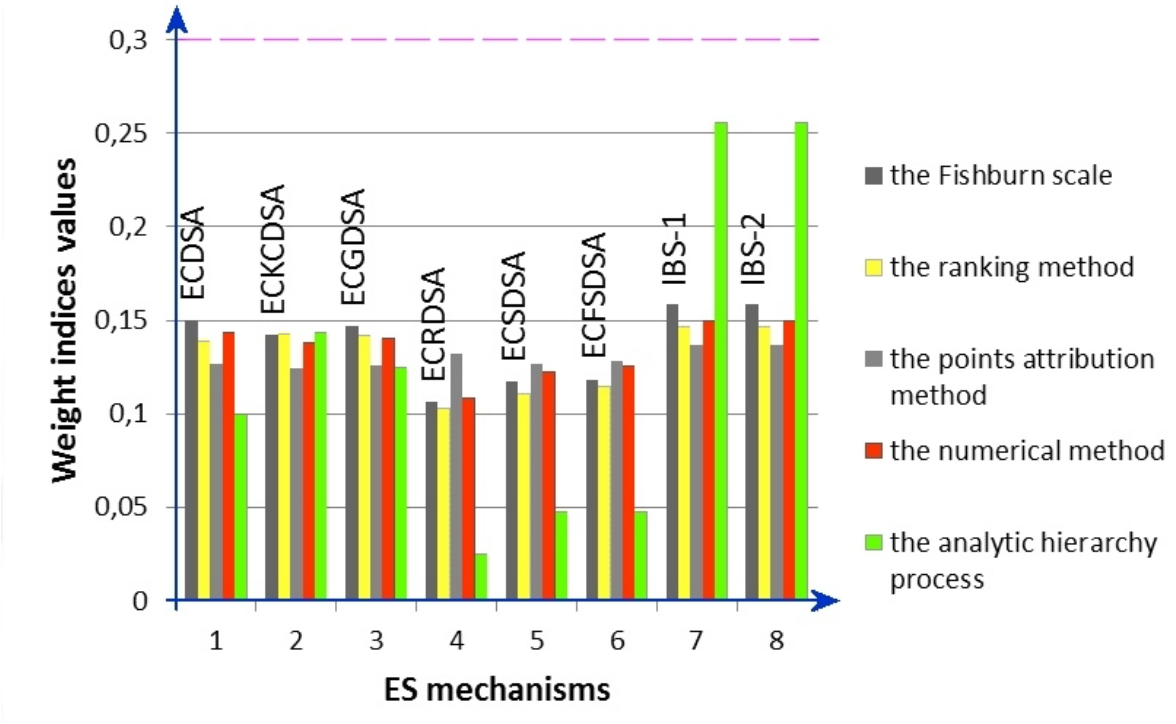

Figure 15 – Analysis of the comparisons results

7 The analysis of ES researches results according to DSTU ISO/IEC 9796-3:2014

For chosen ES mechanisms evaluation methods were obtained results, that are shown in previous chapters. ES mechanisms comparison was made based on expert evaluations. After that, calculations were made by aforementioned techniques.

ES mechanisms according to DSTU ISO/IEC 9796-3:2014 assessments have a similar ranking order by different evaluation methods – from highest to lowest.

Fig. 16 graphically shows the results of the ES mechanisms evaluation by different evaluation methods. The numbers from 1 to 6 are indicated the ES mechanisms: 1 – NR; 2 – ECNR; 3 – ECMR; 4 – ECAO; 5 – ECPV; 6 – ECKNR.

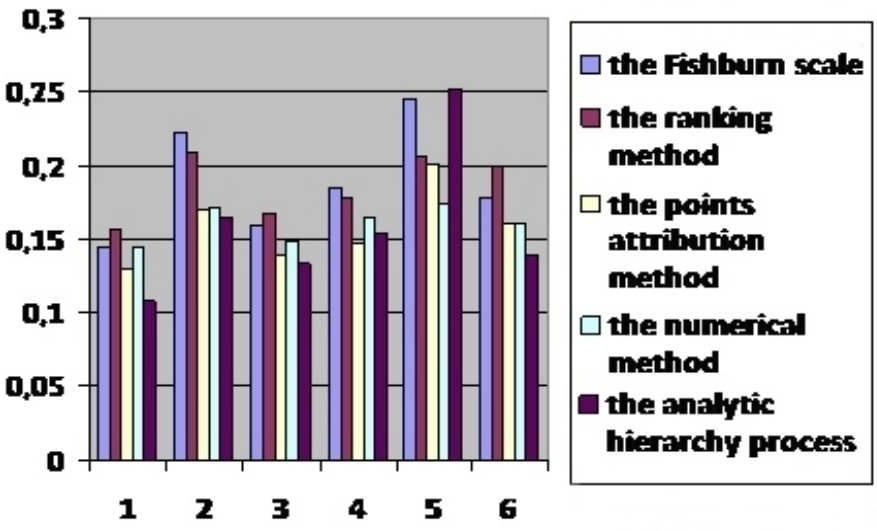

Figure 16 – The results of the ES mechanisms evaluation by different methods

8 Conclusions

1. In connection with the specific requirements for cryptographic transformations, including for ES, the main criteria should be divided into two classes: conditional and unconditional.

Unconditional criteria are those criteria, whose execution for any cryptographic transformations is mandatory, that is unconditional.

Conditional are called criteria, whose execution for any cryptographic transformations is occurred only on certain condition.

2. As a result of conducted researches, it was determined, that as the main criterion for integral evaluation can be and is recommended to use the integral unconditional criterion, that is derived by partial unconditional criteria.

If at least one partial criterion does not meet conditions, such cryptographic transformation is rejected as being, that does not meet the requirements.

3. The proposed comparative analysis technique of standardized ES based on the use of the partial unconditional and conditional criteria set, upon which calculated integral conditional and integral unconditional criteria value.

4. The research results allow to conclude, that in terms of evaluation objective the best use the weight indices determining method, because the experts subjectivity has the a significant impact to the result in the analytic hierarchy process based on pairwise comparisons.

5. The comparative analysis results of standardized ES algorithms DSTU ISO/IEC 14888-3:2014 allowed to make the following conclusions and recommendations: the maximum integral conditional criterion value for DSTU ISO/IEC 14888-3:2014 has been achieved for algorithms IBS-1 and IBS-2 by all evaluation methods.

The ES mechanisms according to DSTU ISO/IEC 14888-3:2014 evaluation results have been obtained almost identical by different methods. Numeric scatter of weight indices values for one algorithm is almost negligible, only numeric values for ES mechanisms IBS-1,2 in the analytic hierarchy process based on pairwise comparisons differ from weight indices values for these ES mechanisms according to other evaluation methods, that is substantiated by more strong influence of the subjective experts opinion in this method.

According to all evaluation methods in the first place are ES mechanisms IBS-1 and IBS-2, and in the last place – ES mechanisms EC-RDSA *(only for the determining the weight indices method based on the points attribution method on the last place based ES mechanism EC-KCDSA).*

6. Comparative analysis of signature mechanisms according to DSTU ISO/IEC 9796-3:2014 has shown that the most perspective mechanisms are signature mechanisms ECPV *(elliptic curve Pintsov-Vanstone message recovery signature)* and ECNR *(elliptic curve Nyberg-Rueppel message recovery signature).*

ES algorithm NR has the worst result, that is substantiated by mathematical apparatus used in this algorithm.

7. To obtain more precise evaluation results and for exact match of ES arrangement mechanisms by all evaluation methods, it is necessary to perform the evaluation procedure several times and carefully approach to the choice of experts that will conduct the evaluation.

References

[1] Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms : ISO/IEC 14888-3 (Edition 2): 2014. – 130 p.

[2] Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms : ISO/IEC 14888-3 (Edition 2 (2006-11-15)): 2006. – 68 p.

[3] Information technology – Security techniques – Digital signatures schemes giving message recovery. – Part 3: Discrete logarithm based mechanisms: ISO/IEC 9796-3:2014.

[4] Andreichikov A.V. Analiz, sintez, planirovanie reshenii v ekonomike / A.V. Andreichikov, O.N. Andreichikova // – M.: Finansy i statistika, 2002. – 359 s.

[5] Analiticheskaya ierarkhicheskaya protsedura Saati [E-resource]. – Access mode: http://www.gorskiy.ru/Articles/Dmss / AHP.html.

[6] Gorbenko Ju.I. Metody pobuduvannja ta analizu kryptografichnyh system. Monografija. / Ju.I. Gorbenko // Kharkiv. Fort. 2015, 959 s.

[7] Informacijni tehnologii' – Kryptografichnyj zahyst informacii' – Cyfrovyj pidpys, shho g'runtujet'sja na eliptychnyh kryvyh – Formuvannja ta perevirka: DSTU 4145-2002. – K.: Derzhstandart Ukrai'ny, 2003. – 35 s. – (Nacional'ni standarty Ukrai'ny).
[8] Korchenko A.G. Postroenie sistem zashchity informatsii na nechetkikh mnozhestvakh / A.G. Korchenko // – M.: MK-Press, 2006. – 320 s.
[9] Makarova I.L. Analiz metodov opredeleniya vesovykh koeffitsientov v integral'nom pokazatele obshchestvennogo zdorov'ya / I.L. Makarova // Mezhdunarodnyi nauchnyi zhurnal «Simvol nauki», Ufa, 2015. – № 7 – S. 87–94.
[10] Metod analiza ierarkhii [E-resource]. – Access mode: https://ru.wikipedia.org/wiki/ Metod analiza ierarkhii.
[11] Metody opredeleniya vesovykh koeffitsientov [E-resource]. – Access mode: http://8v83.tom.ru/.
[12] Metody ekspertnykh otsenok [E-resource]. – Access mode: https://habrahabr.ru/post/189626/.
[13] Metod ekspertnykh otsenok [E-resource]. – Access mode: http://center-yf.ru/data/Marketologu/Metod-ekspertnyh-ocenok.php.
[14] Novyc'kyj A. M. Elektronnyj dokumentoobig jak element zabezpechennja pravovogo reguljuvannja stanovlennja instytutiv informacijnogo suspil'stva / A.M. Novyc'kyj // Naukovyj visnyk Nacional'nogo universytetu derzhavnoi' podatkovoi' sluzhby Ukrai'ny (ekonomika, pravo). – 2013. – № 4. – S. 11–20. – Rezhym dostupu: http://nbuv.gov.ua/UJRN/Nvnudpsu_2013_4_3.
[15] Nogin V.D. Uproshchennyi variant metoda analiza ierarkhii na osnove nelineinoi svertki kriteriev / V.D. Nogin // Access mode: http://www.apmath.spbu.ru/ru/staff/nogin/nogin_p11.pdf.
[16] Okunev Yu.B. Printsipy sistemnogo podkhoda k proektirovaniyu v tekhnike svyazi / Yu.B. Okunev, V.G. Plotnikov // – M.: Svyaz', 1975. – 184 s.
[17] Orlovskii S.A. Problemy prinyatiya reshenii pri nechetkoi iskhodnoi informatsii / S.A. Orlovskii // – M.: Nauka, 1981. – 208 s.
[18] Postnikov V.M Metody vybora vesovykh koeffitsientov lokal'nykh kriteriev / V.M. Postnikov, S.B. Spiridonov // NAUKA i OBRAZOVANIE – Nauchnoe izdanie MGTU im. N.E. Baumana, 2015. – № 6. Access mode: http://technomag.bmstu.ru/index.html.
[19] Potapov D.K. O metodikakh opredeleniya vesovykh koeffitsientov v zadache otsenki nadezhnosti kommercheskikh bankov / D.K. Potapov, V.V. Evstaf'eva // Access mode: http://www.ibl.ru/konf/041208/60.pdf.
[20] Romanova I.K. Ob odnom podkhode k opredeleniyu vesovykh koeffitsientov metoda prostranstva sostoyanii / I.K. Romanova // NAUKA i OBRAZOVANIE – Nauchnoe izdanie MGTU im. N.E. Baumana, 2015. – № 4. Access mode: http://technomag.bmstu.ru/doc/763768.html.
[21] Saati T. Prinyatie reshenii: metod analiza ierarkhii / T. Saati // per. s angl. – M.: Radio i svyaz', 1993.
[22] Soglasovanie rezul'tatov otsenki ob"ektov uluchshenii [E-resource]. – Access mode: http://edu.dvgups.ru/METDOC/EMEN/FK/OTS_NEDV/METOD/UP/frame/3_4.htm.
[23] Ekspertnoe otsenivanie [E-resource]. – Access mode: https://ru.wikipedia.org/wiki/Ekspertnoe otsenivanie.
[24] Ekspertnye otsenki pri razrabotke reshenii [E-resource]. – Access mode: http://books.ifmo.ru/file/pdf/817.pdf.

Рецензент: Ірина Лисицька, д.т.н., проф., Харківський національний університет імені В.Н. Каразіна, м. Харків, Україна.
E-mail: lisitska@karazin.ua

Надійшло: Серпень 2016.

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
Марина Єсіна, аспірантка, Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: rinayes20@gmail.com
Наталія Ковальова, студентка (магістр), Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: natalikovalevaa@gmail.com

Методи та результати порівняльного аналізу електронних підписів з додатком та з відновленням повідомлення.

Анотація. У статті розглянуто методи порівняльного аналізу властивостей механізмів електронного підпису. Досліджено та проаналізовано існуючі методи порівняльного аналізу електронних підписів на основі методів експертних оцінок – метод аналізу ієрархій та варіації методу визначення вагових коефіцієнтів. Наведено певні критерії та показники, що можуть бути використані при порівняльному аналізі властивостей механізмів електронних підписів. Проведено порівняльний аналіз існуючих перспективних механізмів електронних підписів згідно стандартів ДСТУ ISO/IEC 14888-3:2014 та ДСТУ ISO/IEC 9796-3. Наведено результати проведеного оцінювання механізмів електронного підпису. Зроблено висновки та надано рекомендації із застосування методів оцінки визначених алгоритмів електронних підписів.

Ключові слова: аналіз механізмів ЕП, вагові коефіцієнти, електронний підпис, критерій оцінки ЕП, методи порівняльного аналізу ЕП, реалізація та застосування ЕП.

Рецензент: Ирина Лисицкая, д.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина. E-mail: lisitska@karazin.ua

Поступила: Август 2016.

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

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

Наталья Ковалёва, студентка (магистр), Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
E-mail: natalikovalevaa@gmail.com

Методы и результаты сравнительного анализа электронных подписей с дополнением и с восстановлением сообщений.

Аннотация. В статье рассмотрены методы сравнительного анализа свойств механизмов электронной подписи. Исследованы и проанализированы существующие методы сравнительного анализа электронных подписей на основе методов экспертных оценок – метод анализа иерархий и вариации метода определения весовых коэффициентов. Приведены некоторые критерии и показатели, которые могут быть использованы при сравнительном анализе свойств механизмов электронных подписей. Проведено сравнительный анализ существующих перспективных механизмов электронных подписей согласно стандартам ДСТУ ISO/IEC 14888-3:2014 и ДСТУ ISO/IEC 9796-3. Приведено результаты проведенного оценивания механизмов электронной подписи. Сделаны выводы и предоставлены рекомендации по применению методов оценки определенных алгоритмов электронных подписей.

Ключевые слова: анализ механизмов ЭП, весовые коэффициенты, электронная подпись, критерий оценки ЭП, методы сравнительного анализа ЭП, реализация и использование ЭП.

UDC 681.3.04

METHOD OF TABULAR REALIZATION OF ARITHMETIC OPERATIONS IN THE SYSTEM OF RESIDUAL CLASSES

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

[1] V.N. Karazin Kharkiv National University, Svobody sq.,4, Kharkov, 61022, Ukraine
krasnobayev@karazin.ua

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

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

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

Received on August 2016

***Abstract**: In this article the method of increase of productivity and reliability of functioning of the data processing system is suggested based on the use of position-independent computing system in the residual classes (SRC). The developed method takes into account properties of symmetry of tables of realization of basic arithmetic operations and is based on the use ¼ part of the numerical data of the aggregate tables, realizing module operations multiplication, summation and deduction in SRC. Method of bit-by-bit tabular realization is recommended in the digital information processing systems for the productivity improvement of decision of computing tasks.*

***Keywords:** specialized digital devices and systems, base of non-position number system, modular number system, cryptographic transformations.*

Introduction

Stormy development of the computing engineering presently allows to provide the control of operating parameters of the real-time systems in the set limits, that in the turn allows to warn emergency situations. Treatment of large volumes of information for the comparatively short interval of time with the set level of reliability of functioning is the distinctive feature of such systems. The existent data processing system (DPS) functioning in the binary base notation system (BNS) not always are able to decide the set problems in accordance with the produced requirements. One of basic lacks of such DPS is the sequential processing of information, because information submitted in BNS that is stipulating the presence of bit-to-bit communications. This circumstance does not allow parallelizing the decided algorithms at the level of elementary microoperation. The objective of the paper is to develop method of digit-by-digit tabular realization of arithmetic operations in the system of residual classes.

1 Analysis of the last researches

Application of untraditional architectures which are built by with the use of the notation systems (NS) of possessing the maximal level of internal parallelism is grounded in literature [1]. One of such NS is the system of residual classes (SRC). Short form of the residues is one of the SRC properties that allows to use the tabular method of realization of arithmetic operations, which, as is generally known, provides the ultra-high computing speed, i.e. the result of arithmetic operation can be got in the moment of receipt of entrance operands (for one cycle), what is unattainable for BNS.

Simultaneously with this circumstance wide introduction of technologies of the Programmable Logic Device allows successfully realizing the methods of tabular information processing in SRC at creation of fast-acting and high-fail-safe structures of DPS [2-4].

2 Basic materials of researches

The search of ways of increase of productivity and reliability of information processing resulted in the necessity of development of tabular method of realization of module operations.

Known tabular method of realization of operation of module multiplication in SRC, will be realized by means of the use of code of tabular multiplication (CTM) [5–7]. In this case the table $a_i b_i (\mathrm{mod}\, m_i)$ of module multiplication for arbitrary base m_i SRC is symmetric in relation to left (main) and right diagonals, and also vertical and horizontal lines. Symmetry in relation to a left diagonal is determined to commutability operation $a_i b_i$ of multiplication, and symmetry in relation to a right diagonal is determined to, that

$$(m_i - a_i)(m_i - b_i) \equiv a_i b_i (\mathrm{mod}\, m_i).$$

Symmetry in relative to a vertical and horizontal line is determined from the condition of multiple of value of the module to the sum of symmetric numbers of table of multiplication

$$a_i b_i + a_i (m_i - b_i) \equiv 0 (\mathrm{mod}\, m_i),$$
$$a_i b_i + b_i (m_i - a_i) \equiv 0 (\mathrm{mod}\, m_i).$$

Coming foregoing from is obvious, that for tabular realization of operation of module multiplication $a_i b_i (\mathrm{mod}\, m_i)$ it is enough to have numerical information only about its eighth part. Hereof is possibility to simplify the table of module multiplication, due to the exception from the operating device (OD) of DPS of part of surplus equipment (elements And in the blocks of matrix circuit). For the most effective realization of operation $a_i b_i (\mathrm{mod}\, m_i)$ methods allowing in four times to decrease the table of module multiplication are used. The decision the set problem is possible as a result of development and application of the special codes.

The method of determination of result of operation of module multiplication $a_i' b_i' (\mathrm{mod}\, m_i)$ in SRC by means of the use of CTM is following: if two operands are set in CTM $a_i = (\gamma_a, a_i')$ and $b_i = (\gamma_b, b_i')$, in order to get product of these numbers with respect to base m_i, it is enough to find product of $a_i' b_i' (\mathrm{mod}\ m_i)$ and invert its generalized index γ_i in case if γ_a it is differs from γ_b, i.e.

$$a_i b_i (\mathrm{mod}\ m_i) = (\gamma_i, a_i' b_i' (\mathrm{mod}\ m_i)),$$

where:

$$\gamma = \begin{cases} \bar{\gamma}_i, & \text{if } \gamma_a \neq \gamma_b, \\ \gamma_i, & \text{if } \gamma_a = \gamma_b; \end{cases}$$

and

$$a_i' = \begin{cases} a_i, & \text{if } \gamma_a = 0, \\ m_i - a_i, & \text{if } \gamma_a = 1. \end{cases}$$

Foregoing conclusions behave only to realization of operation of module multiplication [1].

During realization of arithmetic operations of summation and deduction basic difficulty consists that it is enough difficultly to synthesize the tabular algorithms of implementation of these module operations, because the tables of realization of operations of summation and deduction are different on the digital structure, hereupon, its do not possess those properties of symmetry, which the tables of module multiplication are possess. However got it is accomplished other results can be, exploring marketability one module operation by tables realizing operation reverse to her, and the opposite.

At research of digital properties of tables of module operations of summation and deduction [8] a next analytical correlation is proved

$$\begin{aligned} &\left[(\gamma_a, a_i') + (\gamma_b, b_i')\right] + \\ &+ \left\{\left[m_i - (\gamma_a, a_i')\right] - (\gamma_b, b_i')\right\} = 0 (\mathrm{mod}\, m_i), \end{aligned} \tag{1}$$

where $a_i = (\gamma_a, a_i')$, $b_i = (\gamma_b, b_i')$ – input operands represented in the special code of tabular presentation of operands offered in this article (SCTPO). We will write down expression (1) in a this form

$$(\gamma_a, a_i') + (\gamma_b, b_i') = m_i - \left\{\left[m_i - (\gamma_a, a_i')\right] - (\gamma_b, b_i')\right\}. \quad (2)$$

It ensues from expression (2), that for the receipt of result of operation of module summation in SCTPO it is enough to know the result of operation of module deduction, i.e. there is possibility effectively (from point of diminishment of amount of equipment of ROM) to use CTM simultaneously for three module operations: multiplication, summation and deduction. On the basis of expression (2) we will consider a method by means of which it will be possible to carry out implementations of any of three arithmetic operations in SRC: multiplication, summation and deduction. Operation of module summation is carried out by means of the algorithm described by expression (2). We will make the algorithm of implementation of operation of module summation by a table, for implementation of operation of module deduction $(a_i' - b_i') \bmod m_i$. In compliance with expression (2) we will consider the method of realization of operation of module summation.

1. The minuend $a_i = (\gamma_a, a_i')$ is inverted on the module of m_i, i.e. we will get the following expression: $\bar{a}_i = ((\gamma_a + 1) \bmod 2, a_i')$. We abandon a subtrahend (γ_b, b_i') without the changes.

2. By means of ROM realizing operation of module deduction, on input operands a_i' and b_i' the result of operation is determined as $(a_i' - b_i') \bmod m_i$. As well as for the algorithm of module multiplication the index of γ_i result of operation of module deduction is formed in compliance with the values of indexes of the corresponding operands, i.e. in concordance with the values $(\gamma_a + 1) \bmod 2$ and γ_b, where:

$$\gamma_i = \begin{cases} \bar{\gamma}, \text{ if } (\gamma_a + 1) \bmod 2 \neq \gamma_b, \\ \gamma, \text{ if } (\gamma_a + 1) \bmod 2 = \gamma_b. \end{cases}$$

Consequently, the result of operation of module deduction will have the following form:

$$(\gamma_i, (a_i' - b_i') \bmod m_i).$$

3. We invert the got result of module deduction on the module of m_i, i.e.

$$((\gamma_i + 1) \bmod 2, (a_i' - b_i') \bmod m_i).$$

For construction of tables of basic arithmetic operations there is most showy application of method of the special encoding, which is described higher, and is allowed simultaneously to decrease the size of tables of summation, deduction and multiplication in four times.

During realization of operations by tabular methods additional diminishment of equipment due to that a not single table is built which will realize a result in a binary code is possible in a number of cases, but k to more shallow tables realizing solutions on each of to digits of result, where k – is register capacity, necessary for storage of number on the examined base $k = \left[\log_2(m_i - 1)\right] + 1$.

Thus very often unification of tables occurs, i.e. reduction of amount of different types of tables necessary for realization of arithmetic unit. The chart of realization of the generalized $\otimes$ arithmetic operation ($\otimes$ – it is multiplication, summation and deduction) on the arbitrary module of m_i is represented in the table 1, and symmetry in relation to a vertical line, horizontal line and diagonals is similarly indicated. Subject to symmetry of tables of realization of basic arithmetic operations (multiplication, summation and deduction), and also on the basis of the methods of reduction of tables considered above, is information taken in the table 2 ¼ part of table 1, and in particular, its second quadrant. In a table 3 numeric data of the second quadrant of the table 1 are represented in a binary code. On the basis of the table 3 we will take in a table 4 values respective to the first (low-order position) digit of result. Thus for realization of DPS we will use only those table elements (blocks) 4, which correspond to the single values of low-order position digit of result.

Table 1 – Table of realization of the generalized arithmetic operation to the module of m

a / b	a_0	…	$a_{\frac{m-1}{2}}$	$a_{\frac{m+1}{2}}$	…	a_{m-1}
b_0	$(a_0 \otimes b_0) \bmod m = c_{00}$	…	$(a_{\frac{m-1}{2}} \otimes b_0) \bmod m = c_{(\frac{m-1}{2})0}$	$(a_{\frac{m+1}{2}} \otimes b_0) \bmod m = c_{(\frac{m+1}{2})0}$	…	$(a_{m-1} \otimes b_0) \bmod m = c_{(m-1)0}$
…	…	…	…	…	…	…
$b_{\frac{m-1}{2}}$	$(a_0 \otimes b_{\frac{m-1}{2}}) \bmod m = c_{0(\frac{m-1}{2})}$	…	$(a_{\frac{m-1}{2}} \otimes b_{\frac{m-1}{2}}) \bmod m = c_{(\frac{m-1}{2})(\frac{m-1}{2})}$	$(a_{\frac{m+1}{2}} \otimes b_{\frac{m-1}{2}}) \bmod m = c_{(\frac{m+1}{2})(\frac{m-1}{2})}$	…	$(a_{m-1} \otimes b_{\frac{m-1}{2}}) \bmod m = c_{(m-1)(\frac{m-1}{2})}$
$b_{\frac{m+1}{2}}$	$(a_0 \otimes b_{\frac{m+1}{2}}) \bmod m = c_{0(\frac{m+1}{2})}$	…	$(a_{\frac{m-1}{2}} \otimes b_{\frac{m+1}{2}}) \bmod m = c_{(\frac{m-1}{2})(\frac{m+1}{2})}$	$(a_{\frac{m+1}{2}} \otimes b_{\frac{m+1}{2}}) \bmod m = c_{(\frac{m+1}{2})(\frac{m+1}{2})}$	…	$(a_{m-1} \otimes b_{\frac{m+1}{2}}) \bmod m = c_{(m-1)(\frac{m+1}{2})}$
…	…	…	…	…	…	…
b_{m-1}	$(a_0 \otimes b_{m-1}) \bmod m = c_{0(m-1)}$	…	$(a_{\frac{m-1}{2}} \otimes b_{m-1}) \bmod m = c_{(\frac{m-1}{2})(m-1)}$	$(a_{\frac{m+1}{2}} \otimes b_{m-1}) \bmod m = c_{(\frac{m+1}{2})(m-1)}$	…	$(a_{m-1} \otimes b_{m-1}) \bmod m = c_{(m-1)(m-1)}$

Table 2 – Second quadrant of the table 1

a / b		a_0	a_1	a_2	…	$a_{\frac{m-1}{2}}$
			a_{m-1}	a_{m-2}	…	$a_{\frac{m+1}{2}}$
b_0		$(a_0 \otimes b_0) \bmod m = c_{00}$	$(a_1 \otimes b_0) \bmod m = c_{10}$	$(a_2 \otimes b_0) \bmod m = c_{20}$		$(a_{\frac{m-1}{2}} \otimes b_0) \bmod m = c_{(\frac{m-1}{2})0}$
b_1	b_{m-1}	$(a_0 \otimes b_1) \bmod m = c_{01}$	$(a_1 \otimes b_1) \bmod m = c_{11}$	$(a_2 \otimes b_1) \bmod m = c_{21}$	…	$(a_{\frac{m-1}{2}} \otimes b_1) \bmod m = c_{(\frac{m-1}{2})1}$
b_2	b_{m-2}	$(a_0 \otimes b_2) \bmod m = c_{02}$	$(a_1 \otimes b_2) \bmod m = c_{12}$	$(a_2 \otimes b_2) \bmod m = c_{22}$	…	$(a_{\frac{m-1}{2}} \otimes b_2) \bmod m = c_{(\frac{m-1}{2})2}$
…	…	…	…	…	…	…
$b_{\frac{m-1}{2}}$	$b_{\frac{m+1}{2}}$	$(a_0 \otimes b_{\frac{m-1}{2}}) \bmod m = c_{0(\frac{m-1}{2})}$	$(a_1 \otimes b_{\frac{m-1}{2}}) \bmod m = c_{1(\frac{m-1}{2})}$	$(a_2 \otimes b_{\frac{m-1}{2}}) \bmod m = c_{2(\frac{m-1}{2})}$	…	$(a_{\frac{m-1}{2}} \otimes b_{\frac{m-1}{2}}) \bmod m = c_{(\frac{m-1}{2})(\frac{m-1}{2})}$

Table 3 – Information of the second quadrant of table 1 represented in a binary code

a / b		a_0	a_1	a_2	…	$a_{\frac{m-1}{2}}$
			a_{m-1}	a_{m-2}	…	$a_{\frac{m+1}{2}}$
b_0		$c_{00_k}, c_{00_{(k-1)}}, \dots$ $\dots, c_{00_1}, c_{00_0}$	$c_{10_k}, c_{10_{(k-1)}}, \dots$ $\dots, c_{10_1}, c_{10_0}$	$c_{20_k}, c_{20_{(k-1)}}, \dots$ $\dots, c_{20_1}, c_{20_0}$	…	$c_{(\frac{m-1}{2})0_k}, c_{(\frac{m-1}{2})0_{(k-1)}}, \dots$ $\dots, c_{(\frac{m-1}{2})0_1}, c_{(\frac{m-1}{2})0_0}$
b_1	b_{m-1}	$c_{01_k}, c_{01_{(k-1)}}, \dots$ $\dots, c_{01_1}, c_{01_0}$	$c_{11_k}, c_{11_{(k-1)}}, \dots$ $\dots, c_{11_1}, c_{11_0}$	$c_{21_k}, c_{21_{(k-1)}}, \dots$ $\dots, c_{21_1}, c_{21_0}$	…	$c_{(\frac{m-1}{2})1_k}, c_{(\frac{m-1}{2})1_{(k-1)}}, \dots$ $\dots, c_{(\frac{m-1}{2})1_1}, c_{(\frac{m-1}{2})1_0}$
b_2	b_{m-2}	$c_{02_k}, c_{02_{(k-1)}}, \dots$ $\dots, c_{02_1}, c_{02_0}$	$c_{12_k}, c_{12_{(k-1)}}, \dots$ $\dots, c_{12_1}, c_{12_0}$	$c_{22_k}, c_{22_{(k-1)}}, \dots$ $\dots, c_{22_1}, c_{22_0}$	…	$c_{(\frac{m-1}{2})2_k}, c_{(\frac{m-1}{2})2(k-1)}, \dots$ $\dots, c_{(\frac{m-1}{2})2_1}, c_{(\frac{m-1}{2})2_0}$
…	…	…	…	…	…	…
$b_{\frac{m-1}{2}}$	$b_{\frac{m+1}{2}}$	$c_{0(\frac{m-1}{2})_k}, c_{0(\frac{m-1}{2})_{(k-1)}}, \dots$ $\dots, c_{0(\frac{m-1}{2})_1}, c_{0(\frac{m-1}{2})_0}$	$c_{1(\frac{m-1}{2})_k}, c_{1(\frac{m-1}{2})_{(k-1)}}, \dots$ $\dots, c_{1(\frac{m-1}{2})_1}, c_{1(\frac{m-1}{2})_0}$	$c_{2(\frac{m-1}{2})_k}, c_{2(\frac{m-1}{2})_{(k-1)}}, \dots$ $\dots, c_{2(\frac{m-1}{2})_1}, c_{2(\frac{m-1}{2})_0}$	…	$c_{(\frac{m-1}{2})(\frac{m-1}{2})_k}, c_{(\frac{m-1}{2})(\frac{m-1}{2})_{(k-1)}}, \dots$ $\dots, c_{(\frac{m-1}{2})(\frac{m-1}{2})_1}, c_{(\frac{m-1}{2})(\frac{m-1}{2})_0}$

By a similar appearance, based on a table 3, we will take in the tables of 5-7 values the proper to the second, *k-1* and *k* (*high-order position*) the digits of result of the generalized arithmetic operation.

Table 4 – Values of the first digit of result of the table 3

b \ a		a_0	a_1	a_2	…	$a_{\frac{m-1}{2}}$
			a_{m-1}	a_{m-2}	…	$a_{\frac{m+1}{2}}$
b_0		c_{00_0}	c_{10_0}	c_{20_0}	…	$c_{(\frac{m-1}{2})0_0}$
b_1	b_{m-1}	c_{01_0}	c_{11_0}	c_{21_0}	…	$c_{(\frac{m-1}{2})1_0}$
b_2	b_{m-2}	c_{02_0}	c_{12_0}	c_{22_0}	…	$c_{(\frac{m-1}{2})2_0}$
…	…	…	…	…	…	…
$b_{\frac{m-1}{2}}$	$b_{\frac{m+1}{2}}$	$c_{0(\frac{m-1}{2})_0}$	$c_{1(\frac{m-1}{2})_0}$	$c_{2(\frac{m-1}{2})_0}$	…	$c_{(\frac{m-1}{2})(\frac{m-1}{2})_0}$

Table 5 – Values of the second digit of result of the table 3

b \ a		a_0	a_1	a_2	…	$a_{\frac{m-1}{2}}$
			a_{m-1}	a_{m-2}	…	$a_{\frac{m+1}{2}}$
b_0		c_{00_1}	c_{10_1}	c_{20_1}	…	$c_{(\frac{m-1}{2})0_1}$
b_1	b_{m-1}	c_{01_1}	c_{11_1}	c_{21_1}	…	$c_{(\frac{m-1}{2})1_1}$
b_2	b_{m-2}	c_{02_1}	c_{12_1}	c_{22_1}	…	$c_{(\frac{m-1}{2})2_1}$
…	…	…	…	…	…	…
$b_{\frac{m-1}{2}}$	$b_{\frac{m+1}{2}}$	$c_{0(\frac{m-1}{2})_1}$	$c_{1(\frac{m-1}{2})_1}$	$c_{2(\frac{m-1}{2})_1}$	…	$c_{(\frac{m-1}{2})(\frac{m-1}{2})_1}$

Table 6 – Values of the $k-1$ digit of result of the table 3

b \ a		a_0	a_1	a_2	…	$a_{\frac{m-1}{2}}$
			a_{m-1}	a_{m-2}	…	$a_{\frac{m+1}{2}}$
b_0		$c_{00_{(k-1)}}$	$c_{10_{(k-1)}}$	$c_{20_{(k-1)}}$	…	$c_{(\frac{m-1}{2})0_{(k-1)}}$
b_1	b_{m-1}	$c_{01_{(k-1)}}$	$c_{11_{(k-1)}}$	$c_{21_{(k-1)}}$	…	$c_{(\frac{m-1}{2})1_{(k-1)}}$
b_2	b_{m-2}	$c_{02_{(k-1)}}$	$c_{12_{(k-1)}}$	$c_{22_{(k-1)}}$	…	$c_{(\frac{m-1}{2})2_{(k-1)}}$
…	…	…	…	…	…	…
$b_{\frac{m-1}{2}}$	$b_{\frac{m+1}{2}}$	$c_{0(\frac{m-1}{2})_{(k-1)}}$	$c_{1(\frac{m-1}{2})_{(k-1)}}$	$c_{2(\frac{m-1}{2})_{(k-1)}}$	…	$c_{(\frac{m-1}{2})(\frac{m-1}{2})_{(k-1)}}$

In spite of the fact that the size of every table is diminished and was multiplied the amount of tables, on the whole gaining in an amount the equipment takes place, as to the limit surplus of tables

is brief and, as we see, the blocks of table, which correspond to the significant digits of result, will be realized only. Because the result of operation appears by an absolute code, there is no necessity in logical elements forming of the SCTPO index.

Table 7 – Values of the k digit of result of the table 3

b \ a		a_0	a_1	a_2	…	$a_{\frac{m-1}{2}}$
			a_{m-1}	a_{m-2}	…	$a_{\frac{m+1}{2}}$
b_0		c_{00_k}	c_{10_k}	c_{20_k}	…	$c_{(\frac{m-1}{2})0_k}$
b_1	b_{m-1}	c_{01_k}	c_{11_k}	c_{21_k}	…	$c_{(\frac{m-1}{2})1_k}$
b_2	b_{m-2}	c_{02_k}	c_{12_k}	c_{22_k}	…	$c_{(\frac{m-1}{2})2_k}$
…	…	…	…	…	…	…
$b_{\frac{m-1}{2}}$	$b_{\frac{m+1}{2}}$	$c_{0(\frac{m-1}{2})_k}$	$c_{1(\frac{m-1}{2})_k}$	$c_{2(\frac{m-1}{2})_k}$	…	$c_{(\frac{m-1}{2})(\frac{m-1}{2})_k}$

The results of calculation of amount of logical elements during complete and bit-by-bit tabular realization of tables of the DPS operation device (OD) are resulted in the table 8. It is visible from the table 8, that tabular realization of arithmetic operations in BNS is not effective, and with the increase of digit grid of OD is impracticable.

Table 8 – Results of calculation of amount of equipment of the DPS OD

Capacity (l)	BNS	Modules of SRC	Complete tabular realization	Bit-by-bit tabular realization	Gain [%]
l=1	$2^8 \cdot 2^8 = 2^{16}$	m=3, m=4, m=5, m=7	263	132	49,81
l=2	$2^{16} \cdot 2^{16} = 2^{32}$	m=2, m=5, m=7, m=9, m=11, m=13	1259	546	56,63
l=3	$2^{24} \cdot 2^{24} = 2^{48}$	m=3, m=4, m=5, m=11, m=13, m=17, m=19	2833	1433	49,42
l=4	$2^{32} \cdot 2^{32} = 2^{64}$	m=2, m=3, m=5, m=7, m=11, m=13, m=17, m=19, m=23, m=29	6943	3788	45,44
l=8	$2^{64} \cdot 2^{64} = 2^{128}$	m=2, m=3, m=5, m=7, m=11, m=13, m=17, m=19, m=23, m=29, m=31, m=37, m=41, m=43, m=47, m=53	39079	24914	36,25

At the same time application of the SRC allows effectively (from point of increase of productivity and diminishment of amount of equipment of matrix circuit) to apply the tabular methods of realization of arithmetic operations.

Conclusion

Thus, the method of increase of productivity and reliability of the real-time DPS which functions in the SRC is offered in the article. Productivity of calculations of the DPS in the SRC rises due to the use of tabular principle of realization of arithmetic operations by introduction and use of SCTPO. Reliability of functioning of the DPS in the SRC rises due to diminution of intensity of refusals of tabular circuits of realization of arithmetic operations by diminution on 40-60% (depending on a computer word length) of amount of equipment of the DPS OP.

References

[1] Akushskii I. Ya., Yuditskii D. I. Mashinnaya arifmetika v ostatochnykh klassakh. – M.: Sov. radio, 1968. – 440 s.
[2] Kuznecov O. O., Olijnykov R. V., Gorbenko Ju. I., Pushkar'ov A. I., Dyrda O. V., Gorbenko I. D. Obg'runtuvannja vymog, pobuduvannja ta analiz perspektyvnyh symetrychnyh kryptoperetvoren' na osnovi blochnyh shyfriv // Visnyk Nacional'nogo universytetu "L'vivs'ka politehnika". – 2014. – № 806: Komp'juterni systemy ta merezhi. – S. 124 – 141.
[3] Koshman S. A., Deren'ko S. N., Krasnobaev V. A. Tablichnyi metod obrabotki tsifrovoi informatsii v klasse vychetov // Radioelektronni i komp'juterni systemy. – 2006. - № 5 (17). – S. 171–175.
[4] Kuznetsov A. A., Shvager A. S., Fesenko D. A. Sokrytie dannykh v klasternykh failovykh sistemakh // Radiotekhnika: Vseukr. mezhved. nauch.-tekhn. sb. – Khar'kov: KhNURE.–2015. – Vyp. 181. – S. 86-100.
[5] Kuznetsov A. A., Smirnov A. A., Sai V. N. Diskretnye signaly s mnogourovnevoi funktsiei korrelyatsii // Radiotekhnika: Vseukr. mezhved. nauch.-tekhn. sb. – Khar'kov: KhTURE.–2011. – Vyp. 166. – S. 142-152.
[6] Krasnobayev V. A., Koshman S. A., Mavrina M. A. A method for increasing the reliability of verification of data represented in a residue number system // Cybernetics and Systems Analysis. – November 2014. – Volume 50, Issue 6, pp 969-976.
[7] Koshman S. O., Barsov V. I., Krasnobajev V. A. Dyversnist' tablychnyh metodiv realizacii' aryfmetychnyh operacij u systemi zalyshkovyh klasiv // Problemy energozabezpechennja ta energozberezhennja v APK Ukrai'ny: Visnyk HNTUSG imeni Petra Vasylenka, vyp. 73, tom 2. - Harkiv, 2008. - S. 70-72.
[8] Krasnobayev V. A., Yanko A. S., Koshman S. A. A Method for arithmetic comparison of data represented in a residue number system // Cybernetics and Systems Analysis. – January 2016. – Volume 52, Issue 1, pp. 145-150.

Рецензент: Олександр Кузнецов, д.т.н., проф., Харківський національний університет імені В. Н. Каразіна, Харків, Україна.
E-mail: kuznetsov@karazin.ua

Надійшло: Серпень 2016

Автори:
Віктор Краснобаєв, д.т.н., проф., Харківський національний університет імені В. Н. Каразіна, Харків, Україна.
E-mail: krasnobaev_va@rambler.ru
Аліна Янко, аспірантка, Полтавський національний технічний університет імені Юрія Кондратюка, Полтава, Україна.
E-mail: al9_yanko@ukr.net
Сергій Кошман, к.т.н., доцент, Харківський національний технічний університет сільського господарства імені Петра Василенка, Харків, Україна.
E-mail: s_koshman@ukr.net

Метод табличної реалізації арифметичних операцій в системі залишкових класів.

Анотація. У статті запропонований метод підвищення продуктивності та надійності функціонування системи обробки інформації заснований на використовуванні непозиційної системи числення у залишкових класах (СЗК). Розроблений метод враховує властивості симетрії таблиць реалізації основних арифметичних операцій і заснований на використовуванні ¼ частини числових даних сукупності таблиць, що реалізовують модульні операції множення, складання та віднімання у СЗК. Метод порозрядній табличній реалізації рекомендований у системах цифрової обробки інформації для підвищення продуктивності рішення обчислювальних задач.

Ключові слова: продуктивність, надійність, система числення у залишкових класах, система обробки інформації, спеціальний код табличного представлення операндів.

Рецензент: Александр Кузнецов, д.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина. E-mail: kuznetsov@karazin.ua

Поступила: Август 2016

Авторы:
Виктор Краснобаев, д.т.н., проф., Харьковский национальный университет имени В. Н. Каразина, Харьков, Украина.
E-mail: krasnobaev_va@rambler.ru
Алина Янко, аспирантка, Полтавский национальный технический университет имени Юрия Кондратюка, Полтава, Украина.
E-mail: al9_yanko@ukr.net
Сергей Кошман, к.т.н., доцент, Харьковский национальный технический университет сельского хозяйства имени Петра Василенка, Харьков, Украина.
E-mail: s_koshman@ukr.net

Метод табличной реализации арифметических операций в системе остаточных классов.

Аннотация. В статье предложен метод повышения производительности и надёжности функционирования системы обработки информации основанный на использовании непозиционной системы счисления в остаточных классах (СОК). Разработанный метод учитывает свойства симметрии таблиц реализации основных арифметических операций и основан на использовании ¼ части числовых данных совокупности таблиц, реализующих модульные операции умножение, сложение и вычитание в СОК. Метод поразрядной табличной реализации рекомендован в системах цифровой обработки информации для повышения производительности решения вычислительных задач.

Ключевые слова: производительность, надёжность, система счисления в остаточных классах, система обработки информации, специальный код табличного представления операндов.

УДК 004.056.55

НЕСИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ НА ОСНОВЕ АЛГЕБРАИЧЕСКОГО КОДИРОВАНИЯ: СОВРЕМЕННОЕ СОСТОЯНИЕ, СУЩЕСТВУЮЩИЕ ПРОТИВОРЕЧИЯ И ПЕРСПЕКТИВЫ ПРАКТИЧЕСКОГО ИСПОЛЬЗОВАНИЯ НА ПОСТ-КВАНТОВЫЙ ПЕРИОД

Александр Кузнецов[1], Андрей Пушкарев[2], Сергей Кавун[3], Вячеслав Калашников[4]

[1] Харьковский национальный университет имени В.Н. Каразина, площадь Свободы, 4, г. Харьков, 61022, Украина
kuznetsov@karazin.ua

[2] Департамент Государственной службы специальной связи и защиты информации Украины, г. Киев, Украина

[3] Харьковский учебно-научный институт ГВУЗ "Университет банковского дела", пр. Победы 55, г. Харьков, 61174, Украина
kavserg@gmail.com

[4] Технологический университет Монтеррея, Монтеррей, Мексика
пр. Еухеніо Гарса Сада 2501, 64849 Монтеррей, Нуево-Леон, Мексика
kalash@itesm.mx

Рецензент: Роман Олійников, д.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, площадь Свободы, 4, г. Харьков, 61022, Украина
roliynykov@gmail.com

Поступила в августе 2016

Аннотация. *Рассматриваются несимметричные криптосистемы на основе алгебраического кодирования, исследуются современное состояние, существующие противоречия и перспективы практического использования на пост-квантовый период. Предлагается новая схема криптопреобразования, существенно повышающая относительную скорость передачи информации. Показано преимущество предлагаемой конструкции по сравнению с уже известными схемами Мак-Элиса и Нидеррайтера.*

Ключевые слова: *несимметричные криптосистемы, пост-квантовая криптография, криптография на основе кодов.*

1 Введение

Для предоставления базовых услуг безопасности в современных информационно-телекоммуникационных системах применяются различные криптографические механизмы, в частности, несимметричные (двухключевые) криптосистемы, в которых задача поиска секретного ключа по известному открытому ключу связана с решением известной и очень сложной математической задачи (факторизации, дискретного логарифмирования и пр.) [1-3]. Однако с появлением квантовых вычислений, основанных на принципах квантовой механики, в частности, на принципе суперпозиции и явлении квантовой запутанности, скорость решения определенных математических задач значительно возрастает [4]. Существует ряд квантовых алгоритмов, например, алгоритмы Дойча и Йожи, Саймона, Гровера, Шора и другие, выполнение которых занимает гораздо меньше времени, чем выполнение любого вероятностного классического алгоритма [5-11]. Алгоритм Шора позволяет найти за конечное (и приемлемое) время все простые множители больших чисел или решить задачу дискретного логарифмирования, и, как следствие, найти секретный ключ соответствующего асимметричного криптоалгоритма (RSA, ECC, или других) [10]. Следовательно, разработка и теоретическое обоснование новых криптографических алгоритмов, в которых сложность поиска секретного параметра по известному открытому ключу остается высокой даже с учетом возможного применением квантовых вычислений (т.е. для пост-квантового периода), является чрезвычайно важной научной задачей [12-14].

Среди возможных кандидатов для пост-квантовой криптографии *(Post-Quantum Cryptography)* особое место занимают алгоритмы, построение которых основано на использовании алгебраических кодов, замаскированных под код общего положения (случайный код, полный код) [15-18]. В русскоязычной литературе подобные алгоритмы получили название теоретико-кодовых схем [19,20], или крипто-кодовых преобразований [21,22]. Наряду с высокой скоростью криптографического преобразования и возможностью совмещать контроль ошибок с защитой от несанкционированного ознакомления [23] крипто-кодовые преобразования остаются стойкими даже в случае использования квантовых вычислений. Кроме того, на сегодняшний день уже известны различные криптографические примитивы (алгоритмы несимметричного [15,16,18,20] и симметричного [17] шифрования, генераторы псевдослучайных последовательностей и поточного шифрования [24 - 26], протоколы доказательства с нулевым разглашением *(Zero-knowledge proof)* [27,28], схемы электронной цифровой подписи [29,30], идентификации [31,32] и пр.), основанные на использовании алгебраических кодов, что делает это направление универсальным инструментом, позволяющим на едином математическом и программном обеспечении реализовать широкий спектр эффективных механизмов криптографической защиты информации. И хотя известны также и вычислительно эффективные атаки на отдельные варианты теоретико-кодовых схем [19, 33 - 36], базовая конструкция [15], предложенная около 40 лет назад, остается стойкой ко всем известным методам криптоанализа, что с исторической ретроспективы подтверждает надежность и перспективность крипто-кодовых преобразований, особенно в контексте построения эффективных пост-квантовых алгоритмов криптографической защиты [37].

В данной статье рассматриваются общетеоретические положения алгебраического кодирования и несимметричные криптосистемы на их основе. Исследуются современное состояние, существующие противоречия и перспективы практического использования несимметричных кодовых криптосистем на пост-квантовый период. Предлагается новая схема криптопреобразования, существенно повышающая относительную скорость передачи информации. Показано преимущество предлагаемой конструкции по сравнению с уже известными схемами Мак-Элиса и Нидеррайтера [15,16].

2 Общие положения алгебраической теории блоковых кодов, используемые для описания теоретико-кодовых схем

Введем основные термины и определения алгебраической теории кодирования [38-40], используемые в дальнейшем при рассмотрении несимметричных кодовых криптосистем (теоретико-кодовых схем), в том числе алгоритмов формирования и проверки ЭЦП.

Зафиксируем конечное поле $GF(q)$ и рассмотрим векторное пространство V_n, как множество n-последовательностей с элементами из $GF(q)$ с покомпонентным сложением и умножением на скаляр.

Линейный (n,k,d) *код* V_k над $GF(q)$ есть подпространство в V_n, т.е. непустое множество n-последовательностей (*кодовых слов*) с элементами из $GF(q)$, где k – *размерность* линейного подпространства, d - минимальный вес Хемминга (число ненулевых элементов) $w_h(c)$ произвольного ненулевого кодового слова c кода V_k:

$$d = \min_{\forall c \in V_k, c \neq 0} w_h(c).$$

В виду линейности подпространства V_k набор весов различных ненулевых кодовых слов совпадает с набором расстояний по Хеммингу между различными кодовыми словами, т.е. d называют также *минимальным кодовым расстоянием* по Хеммингу кода V_k. Величину $R = \frac{k}{n}$ называют *относительной скоростью кода*, а $\delta = \frac{d}{n}$ называют *относительным минимальным кодовым расстоянием*.

Основная проблема теории избыточного кодирования впервые сформулирована в работе К. Шеннона [41]: найти коды с большой относительной скоростью R и с большим минимальным кодовым расстоянием d. Она вытекает из следующей теоремы.

Теорема 1 [41]. Пусть $C(P_0)$ – пропускная способность дискретного симметричного канала с вероятностью ошибки P_0. Тогда для любого $\varepsilon > 0$, если $R < C(P_0)$ и n достаточно велико, существует (n, k, d) код с относительной скоростью $k / n \geq R$, вероятность ошибки которого $P_{ош} < \varepsilon$.

Теорема 1 доказана вероятностными методами и не дает механизма для построения кодов с высокими R и δ. Для линейных блоковых кодов справедлива следующая оценка (граница Варшамова-Гилберта).

Теорема 2 [40]. Если выполняется равенство

$$q^{n-k} \geq \sum_{i=0}^{d-2} C_{n-1}^{i} (q-1)^{i}, \tag{1}$$

тогда существует линейный (n, k, d) код над $GF(q)$.

На практике чаще используют асимптотические границы, которые дают представление о предельных кодовых характеристиках при бесконечно большой длине кода. Прологарифмируем выражение (1), получим

$$n - k \geq \log_q \left(\sum_{i=0}^{d-2} C_{n-1}^{i} (q-1)^{i} \right).$$

Устремим $n \to \infty$, получим асимптотическую границу Варшамова-Гилберта:

$$R \leq 1 - H_q(\delta), \tag{2}$$

где $H_q(x)$ - q - ичная функция энтропии на отрезке $\left[0, \frac{q-1}{q}\right]$, причем

$$H_q(x) = x \log_q (q-1) - x \log_q (x) - (1-x) \log_q (1-x), \; 0 < x \leq \frac{q-1}{q}.$$

Таким образом, проблема помехоустойчивого кодирования состоит в поиске регулярных алгоритмов построения таких линейных блоковых (n, k, d) кодов, параметры которых удовлетворяют кодовой границе (1) и/или асимптотические кодовые границы которых удовлетворяют (2).

Линейный код V_k (как линейное подпространство в V_n) задается набором базисных (линейно независимых) векторов

$$(g_{0,0}, g_{0,1}, ..., g_{0,n-1}),$$
$$(g_{1,0}, g_{1,1}, ..., g_{1,n-1}),$$
$$\dots$$
$$(g_{k-1,0}, g_{k-1,1}, ..., g_{k-1,n-1}),$$

которые обычно представляются в матричном виде через порождающую матрицу

$$G = \begin{pmatrix} g_{0,0} & g_{0,1} & \dots & g_{0,n-1} \\ g_{1,0} & g_{1,1} & \dots & g_{1,n-1} \\ \dots & \dots & \dots & \dots \\ g_{k-1,0} & g_{k-1,1} & \dots & g_{k-1,n-1} \end{pmatrix}$$

ранга $rank(G) = k$ и размерности $k \times n$.

Произвольное кодовое слово $c = (c_0, c_1, ..., c_{n-1})$ кода V_k есть линейная комбинация строк из матрицы G. Кодирование заключается в сопоставлении каждого *информационного слова* $i = (i_0, i_1, ..., i_{k-1})$ с символами из $GF(q)$ некоторому кодовому слову $(c_0, c_1, ..., c_{n-1})$. Наиболее простой способ кодирования задается выражением

$$c = iG. \tag{3}$$

Посредством линейных операций над строками матрицу G удобно привести к каноническому виду

$$G^* = \begin{pmatrix} 1 & 0 & ... & 0 & g^*_{0,k} & g^*_{0,k+1} & ... & g^*_{0,n-1} \\ 0 & 1 & ... & 0 & g^*_{1,k} & g^*_{1,k+1} & ... & g^*_{1,n-1} \\ ... & ... & ... & ... & ... & ... & ... & ... \\ 0 & 0 & ... & 1 & g^*_{k-1,k} & g^*_{k-1,k+1} & ... & g^*_{k-1,n-1} \end{pmatrix} = I \| P, \tag{4}$$

где I - единичная подматрица размером $k \times k$, P - подматрица размером $k \times (n-k)$ в правой части матрицы G^*, $\|$ - символ конкатенации (объединения).

Тогда при использовании выражения $c = iG$ имеем *систематическое* правило кодирования $c = i \| iP$, т.е. информационный вектор $i = (i_0, i_1, ..., i_{k-1})$ будет в явном виде содержаться в кодовом слове $c = (c_0, c_1, ..., c_{n-1})$.

Линейное подпространство, отождествляющее код V_k, имеет ортогональное дополнение (обозначим его U_{n-k}). Базис подпространства U_{n-k} задается векторами

$$(h_{0,0}, h_{0,1}, ..., h_{0,n-1}),$$
$$(h_{1,0}, h_{1,1}, ..., h_{1,n-1}),$$
$$...$$
$$(h_{n-k-1,0}, h_{n-k-1,1}, ..., h_{n-k-1,n-1})$$

и обычно представляется в матричном виде через проверочную матрицу

$$H = \begin{pmatrix} h_{0,0} & h_{0,1} & ... & h_{0,n-1} \\ h_{1,0} & h_{1,1} & ... & h_{1,n-1} \\ ... & ... & ... & ... \\ h_{n-k-1,0} & h_{n-k-1,1} & ... & h_{n-k-1,n-1} \end{pmatrix}$$

ранга $rank(H) = n-k$ и размерности $(n-k) \times n$.

Условие ортогональности векторов из V_k и U_{n-k} в матричном виде записывается как

$$GH^T = 0, \tag{5}$$

где под нулем понимается нулевая матрица, размерности $k \times (n-k)$.

Линейное подпространство U_{n-k} называют *дуальным* (двойственным) к V_k кодом над $GF(q)$. *Определение кода* V_k *через ортогональное дополнение* U_{n-k} (через дуальный код) можно сформулировать следующим образом: произвольная n-последовательностей $c = (c_0, c_1, ..., c_{n-1})$ с элементами из $GF(q)$ является кодовым словом кода V_k тогда и только тогда, когда она ортогональна каждой строке проверочной матрицы H, т.е. при $cH^T = 0$.

Посредством линейных операций над строками приведем матрицу H к каноническому виду

$$H^* = \begin{pmatrix} h^*_{0,0} & h^*_{0,1} & ... & h^*_{0,k-1} & 1 & 0 & ... & 0 \\ h^*_{1,0} & h^*_{1,1} & ... & h^*_{1,k-1} & 0 & 1 & ... & g^*_{1,n-1} \\ ... & ... & ... & ... & ... & ... & ... & ... \\ h^*_{n-k-1,0} & h^*_{n-k-1,1} & ... & h^*_{n-k-1,k-1} & 0 & 0 & ... & 1 \end{pmatrix} = P^* \| I, \tag{6}$$

где P^*- подматрица размером $(n-k) \times k$ в левой части матрицы H^*, I - единичная подматрица размером $(n-k) \times (n-k)$, $\|$ - символ конкатенации (*объединения*).

Тогда из условия $G*H*^T = 0$ имеем $P* = -P^T$ (с операциями над $GF(q)$).

Единичные вектора-столбцы в матрицах $G*$ и $H*$ могут быть выбраны произвольно с соответствующим формированием единичных подматриц и систематическим размещением информационных символов в кодовом слове.

Основной целью избыточного кодирования информации является контроль *(обнаружение и исправление)* ошибок, произошедших при передаче сообщения по каналу с шумами [38-40]. Для контроля ошибок кодирующее устройство вносит избыточность *(проверочную часть длины $r = n - k$)* в передаваемые данные. На приемной стороне, анализируя свойства проверочной части и ее соответствие передаваемым данным, декодер уменьшает влияние ошибок, возникших при передаче.

Обозначим вектор ошибок, воздействующий на передаваемое кодовое слово c, как n-последовательность $e = (e_0, e_1, ..., e_{n-1})$ с элементами из $GF(q)$. Искаженное кодовое слово обозначим вектором $c* = c + e = (c_0 + e_0, c_1 + e_1, ..., c_{n-1} + e_{n-1})$.

Синдромом в теории кодирования называют вектор $s = (s_0, s_1, ..., s_{n-k-1})$ с элементами из $GF(q)$, который характеризует воздействие вектора ошибок на произвольное кодовое слово:

$$s = c*H^T = cH^T + eH^T = eH^T, \quad (7)$$

т.е. значение вектора s зависит только от вектора ошибок $e = (e_0, e_1, ..., e_{n-1})$ и не зависит от выбранного кодового слова $c = (c_0, c_1, ..., c_{n-1})$.

Таким образом, процесс декодирования состоит в анализе синдрома: при $s = 0$ принимается решение об отсутствии ошибок; при $s \neq 0$ принимается решение об искажении кодового слова ненулевым вектором ошибок. Дальнейшие действия зависят от принятой стратегии: в системах обнаружения ошибок с переспросом осуществляется запрос на повторную передачу кодового слова; в системах с прямым исправлением ошибок осуществляется поиск вектора $e = (e_0, e_1, ..., e_{n-1})$ по вычисленному значению $s \neq 0$.

Следует отметить, что при больших n и k задача поиска вектора e по ненулевому синдрому s для случайно выбранного в пространстве V_n линейного кода V_k является чрезвычайно сложной математической задачей. В общем случае эта задача относится к классу NP-сложных [37]. Однако для алгебраических кодов, со специфической структурой матриц G и H, декодирование (задача поиска вектора ошибок e и/или восстановление безошибочного кодового слова c) является полиномиально разрешимой задачей.

Алгебраическое кодирование основано на использовании специальных алгебраических уравнений, позволяющих однозначно представить информационные и кодовые слова, вектора ошибок и синдромов и свести задачу декодирования к решению систем линейных уравнений. Действительно, каждый вектор из V_n можно представить многочленом от формальной переменной x степени не выше $n-1$. При этом элементы вектора отождествляются с коэффициентами многочлена, а множество многочленов имеет структуру векторного пространства, идентичную структуре пространства V_n, а так же структуру кольца многочленов по модулю двучлена $x^n - 1$. Рассмотрим следующие многочлены:

- информационный многочлен $i(x) = i_0 x^0 + i_1 x^1 + ... + i_{k-1} x^{k-1}$ (соответствует вектору i);
- кодовый многочлен $c(x) = c_0 x^0 + c_1 x^1 + ... + c_{n-1} x^{n-1}$ (соответствует вектору c);
- многочлен ошибок $e(x) = e_0 x^0 + e_1 x^1 + ... + e_{n-1} x^{n-1}$ (соответствует вектору e);
- кодовый многочлен с ошибками $c*(x) = c*_0 x^0 + c*_1 x^1 + ... + c*_{n-1} x^{n-1}$ (соответствует вектору $c*$);
- синдромный многочлен $s(x) = s_0 x^0 + s_1 x^1 + ... + s_{n-k-1} x^{n-k-1}$ (соответствует вектору s).

Зададим, например, с помощью корней $X_0, X_1, ..., X_{n-k-1} \in GF(q^m)$, приведенный ненулевой многочлен $g(x) = (x - X_0)(x - X_1)...(x - X_{n-k-1})$ степени $r = n - k$ и правило кодирования

$$c(x) = i(x)g(x), \tag{8}$$

которое является полиномиальным аналогом выражения (3).

Многочлен $g(x)$ по аналогии с матрицей G называют *порождающим*, а соответствующая ему матрица G может быть получена циклически сдвинутой построчной записью коэффициентов многочлена $g(x)$ [38-40]. Линейные блоковые коды заданные таким образом называют *циклическими*, т.к. из принадлежности пространству V_k некоторой последовательности c (и соответствующего многочлена $c(x)$) следует также и принадлежность любой циклически сдвинутой последовательности (что в терминах многочленов трактуется как многочлен $x^i c(x)$, $i \in 0,1,...,n-k-1$ с операциями в кольце по модулю двучлена $x^n - 1$).

Многочлен $g(x)$ в общем случае определен над $GF(q^m)$ и тогда кодовые многочлены $c(x)$ также будут определены над расширенным полем $GF(q^m)$. Однако в случае, если все корни $X_0, X_1, ..., X_{n-k-1} \in GF(q^m)$ являются также всеми корнями некоторого набора минимальных многочленов элементов $GF(q^m)$, тогда порождающий многочлен $g(x)$ всегда будет иметь коэффициенты из подполя $GF(q)$, причем:

$$g(x) = H.O.K.\left(\prod_i f_i(x)\right),$$

где i пробегает по всем классам сопряженных элементов поля $GF(q^m)$, $f_i(x)$ - минимальный многочлен элемента $\alpha^i \in GF(q^m)$, α - примитивный элемент, $H.O.K.$ - наименьшее общее кратное.

Значение многочлена в его корне равно нулю, т.е. для всех $X_j \in \{X_0, X_1, ..., X_{n-k-1}\}$ выполняется равенство

$$c(X_j) = c_0 X_j^0 + c_1 X_j^1 + ... + c_{n-1} X_j^{n-1},$$

что в матричном виде соответствует записи:

$$(c_0, c_1, c_2, ..., c_{N-1}) \cdot \begin{vmatrix} 1 & X_0 & X_0^2 & ... & X_0^{n-1} \\ 1 & X_1 & X_1^2 & ... & X_1^{n-1} \\ 1 & X_2 & X_2^2 & ... & X_2^{n-1} \\ ... & ... & ... & ... & ... \\ 1 & X_{r-1} & X_{r-1}^2 & ... & X_{r-1}^{n-1} \end{vmatrix}^T = 0.$$

Полученное выражение соответствует условию взаимной ортогональности произвольного кодового слова $c = (c_0, c_1, c_2, ..., c_{n-1})$ и матрицы в правой части произведения. Следовательно, положим

$$cH^T = 0,\ H = \begin{pmatrix} X_0^0 & X_0^1 & ... & X_0^{n-1} \\ X_1^0 & X_1^1 & ... & X_1^{n-1} \\ ... & ... & ... & ... \\ X_{n-k-1}^0 & X_{n-k-1}^1 & ... & X_{n-k-1}^{n-1} \end{pmatrix}, \tag{9}$$

где H – проверочная матрица кода, заданная корнями порождающего многочлена.

Для построения матрицы H с элементами из подполя $GF(q)$ следует заменить каждый элемент $X_j^i \in GF(q^m)$ в (9) вектором-столбцом из m элементов поля $GF(q)$.

Если выбрать в качестве корней многочлена $g(x)$ $2t$ подряд следующих элементов $X_0 = \alpha^j, X_1 = \alpha^{j+1}, ..., X_{n-k-1} = \alpha^{j+2t-1} \in GF(q^m)$, тогда, по теореме Боуза-Чоудхури-Хоквингема [38-40], полученный код (БЧХ) будет иметь минимальное кодовое расстояние равное $d = 2t+1$. Для кода БЧХ над $GF(q^m)$ проверочная матрица примет вид

$$H = \begin{pmatrix} \alpha^0 & \alpha^j & \dots & \alpha^{j(n-1)} \\ \alpha^0 & \alpha^{j+1} & \dots & \alpha^{(j+1)(n-1)} \\ \dots & \dots & \dots & \dots \\ \alpha^0 & \alpha^{j+2t-1} & \dots & \alpha^{(j+2t-1)(n-1)} \end{pmatrix}. \quad (10)$$

Заданные таким образом коды называют *кодами Рида-Соломона*, их (n,k,d) параметры над $GF(q^m)$ связаны соотношением $d = n-k+1$ (верхняя граница Синлгтона), т.е. они обладают *максимально-достижимым кодовым расстоянием* (МДР) [38-40]. Ограничением на подполе $GF(q)$ с заменой всех $\alpha^i \in GF(q^m)$ в (10) соответствующими векторами-столбцами из m элементов поля $GF(q)$ получают коды над $GF(q)$, (n,k,d) параметры которых удовлетворяют ограничению (нижняя граница БЧХ) $d \ge n-km+1$.

Предположим, что кодовое слово c исказилось при его передаче, а число ошибок на блоке из N символов не превышает исправляющей способности $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ алгебраического (n,k,d) кода. Другими словами, многочлен $e(x)$ содержит не более t ненулевых коэффициентов. Из (7) и (9) следует равенство

$$(s_0, s_1, ..., s_{n-k-1}) = (e_0, e_1, e_2, ..., e_{N-1}) \cdot \begin{vmatrix} 1 & X_0 & X_0^2 & \dots & X_0^{N-1} \\ 1 & X_1 & X_1^2 & \dots & X_1^{N-1} \\ 1 & X_2 & X_2^2 & \dots & X_2^{N-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & X_{n-k-1} & X_{n-k-1}^2 & \dots & X_{n-k-1}^{N-1} \end{vmatrix}^T,$$

что эквивалентно следующей системе уравнений:

$$\begin{aligned} s_0 &= e_0 + e_1 X_0 + e_2 X_0^2 + \dots + e_{n-1} X_0^{n-1} = \sum_{i=0}^{n-1} e_i X_0^i, \\ s_1 &= e_0 + e_1 X_1 + e_2 X_1^2 + \dots + e_{n-1} X_1^{n-1} = \sum_{i=0}^{n-1} e_i X_1^i, \\ &\dots \\ s_{n-k-1} &= e_0 + e_1 X_{n-k-1} + e_2 X_{n-k-1}^2 + \dots + e_{n-1} X_{n-k-1}^{n-1} = \sum_{i=0}^{n-1} e_i X_{n-k-1}^i. \end{aligned} \quad (11)$$

Задача декодирования вектора c^* состоит в нахождении всех e_i, $i = 0,..., n-1$ по известным элементам вектора $s = (s_0, s_1, ..., s_{n-k-1})$. Система уравнений (11) содержит $n-k$ нелинейных уравнения от n неизвестных, прямых методов ее решения такой системы не известно. В алгебраической теории кодирования [38-40] для нахождения элементов вектора $e = (e_0, e_1, ..., e_{n-1})$ используют искусственный прием, состоящий в рассмотрении многочлена локаторов ошибок $\Lambda(x)$, корнями которого являются ненулевые элементы вектора e, т.е.

$$\Lambda(x) = \prod_j (x + X_j), \quad (12)$$

где j – индекс ненулевых элементов вектора e, X_j - т.н. локатор ошибки, произошедшей в j-ом символе кодового слова.

Раскроем скобки в выражении (12), получим

$$\Lambda(x) = x^u + \lambda_{u-1} x^{u-1} + \dots + \lambda_1 x + \lambda_0, \quad (13)$$

где степень u многочлена $\Lambda(x)$ задает число произошедших ошибок на блоке из n символов, $u \le t$, т.е. число ненулевых элементов вектора e.

Набор коэффициентов $(\lambda_0, \lambda_1, ..., \lambda_{u-1})$ многочлена (13) однозначно задает его корни, которые однозначно указывают (локализуют) расположение произошедших ошибок.

Умножим многочлен (13) на $e_i X^i$ и вычислим его значение в X_j, получим:

$$e_i X_j^{u+i} + e_i \lambda_{u-1} X_j^{u+i-1} + ... + e_i \lambda_1 X_j^{i+1} + e_i \lambda_0 X_j^i = 0,$$

где $X_j \in GF(q^m)$, т.е. $X_j = \alpha^{Jj}$ (где α - примитивный элемент поля $GF(q^m)$) для некоторого J_j.

Следовательно, $X_j^{a+b} = \alpha^{a+b+Jj} = X^b_{j+a}$, т.е. справедливо выражение

$$e_i X^i_{j+u} + e_i \lambda_{u-1} X^i_{j+u-1} + ... + e_i \lambda_1 X^i_{j+1} + e_i \lambda_0 X^i_j = 0$$

Последнее равенство выполняется для любых j и i. Просуммируем по всем $i = 0...n-1$:

$$\sum_{i=0}^{N-1} \left(e_i X^i_{j+u} + e_i \lambda_{u-1} X^i_{j+u-1} + ... + e_i \lambda_1 X^i_{j+1} + e_i \lambda_0 X^i_j \right) = 0.$$

Изменим порядок суммирования, вынесем коэффициенты многочлена $\Lambda(x)$ за знак суммирования, получим:

$$\sum_{i=0}^{N-1} e_i X^i_{j+u} + \lambda_{u-1} \cdot \sum_{i=0}^{N-1} e_i X^i_{j+u-1} + ... + \lambda_1 \cdot \sum_{i=0}^{N-1} e_i X^i_{j+1} + \lambda_0 \cdot \sum_{i=0}^{N-1} e_i X^i_j = 0.$$

Значение каждого слагаемого в последнем выражении соответствует произведению коэффициентов многочлена $\Lambda(x)$ на соответствующие синдромы в выражении (11), так что запишем

$$s_{j+u} + \lambda_{u-1} \cdot s_{j+u-1} + ... + \lambda_1 \cdot s_{j+1} + \lambda_0 \cdot s_j = 0.$$

Перепишем выражение для каждого $j = 0...u$, получим систему линейных уравнений:

$$\begin{aligned} s_u + \lambda_{u-1} \cdot s_{u-1} + ... + \lambda_1 \cdot s_1 + \lambda_0 \cdot s_0 &= 0, \\ s_{u+1} + \lambda_{u-1} \cdot s_u + ... + \lambda_1 \cdot s_2 + \lambda_0 \cdot s_1 &= 0, \\ &... \\ s_{2 \cdot u} + \lambda_{u-1} \cdot s_{2 \cdot u-1} + ... + \lambda_1 \cdot s_{u+1} + \lambda_0 \cdot s_u &= 0. \end{aligned} \quad (14)$$

Система из u линейных уравнений (14) с u неизвестными разрешима, сложность ее решения растет полиномиально от числа неизвестных [38-40]. Так, например, для решения системы (14) методом Гаусса необходимо выполнить u^3 арифметических операций (сложений и умножений над элементами поля $GF(q^m)$).

Решение системы (14) дает значения коэффициентов многочлена локаторов ошибок (13). Корнями многочлена (13) являются локаторы – такие элементы поля $GF(q^m)$, которые однозначно указывают расположение ненулевых элементов вектора ошибок e. Следовательно, для локализации ошибок необходимо найти корни уравнения (13).

Наиболее простая процедура поиска корней $\Lambda(x)$ состоит в подстановке в многочлен всех n элементов $X_j \in GF(q^m)$ и выборе таких элементов, которые обращают в нуль $\Lambda(x)$. В литературе такой прием получил название процедура Ченя [38-40]. Используя схему Горнера перепишем многочлен $\Lambda(x)$ в виде

$$\Lambda(x) = x^u + \lambda_{u-1} x^{u-1} + \lambda_{u-2} x^{u-1} ... + \lambda_1 x + \lambda_0 = (...((x + \lambda_{u-1})x + \lambda_{u-2})x + ... + \lambda_1)x + \lambda_0.$$

Для вычисления значения многочлена $\Lambda(x)$ в такой форме потребуется не более $u-1$ арифметических операций (сложений и умножений над элементами поля $GF(q^m)$), т.е. сложность этого этапа декодирования не превысит $n(u-1)$ арифметических операций.

После локализации ошибок - нахождении локаторов ошибок X_j, необходимо вычислить значения ошибок в j-ом символе, т.е. вычислить элементы вектора e и восстановить кодовое слово: $c = c^* - e$. Для нахождения значений ошибок воспользуемся выражением (11). Подставим значения найденных локаторов X_j и неизвестные значения e_j в систему уравнений. Остальные e_i при $i \neq j$ равны нулю. Следовательно, система уравнений (11) запишется в виде:

$$s_0 = \sum_{i \in J} e_i X_0^i,$$

$$s_1 = \sum_{i \in J} e_i X_1^i,$$

$$\dots$$

$$s_{n-k-1} = \sum_{i \in J} e_i X_{n-k-1}^i,$$

где J – множество индексов ненулевых элементов вектора ошибок, т.е. набор номеров локаторов ошибок, причем $|J| = u \le t$. Полученная система из $n-k$ линейных уравнений содержит $|J| = u \le t$ неизвестных значений ошибок e_i, причем $t < n - k$. Следовательно, система разрешима, ее решение дает неизвестные ненулевые значения ошибок вектора e. Для решения системы уравнений от u неизвестных методом Гаусса, необходимо выполнить u^3 арифметических операций (сложений и умножений над элементами поля $GF(q^m)$). Для восстановления кодового слова длины n кодовых символов достаточно снять действие найденного вектора ошибок: $c = c^* - e$, т.е. выполнить u арифметических операций.

Таким образом, задача декодирования алгебраического блокового (n,k,d) кода (нахождения вектора ошибок $e = (e_0, e_1, ..., e_{n-1})$) сводится к решению двух систем линейных уравнений от $u \le t = \left\lfloor \frac{d-1}{2} \right\rfloor$ неизвестных и вычислению n значений многочлена $\Lambda(x)$ степени u. Для обращения матриц и решения систем линейных уравнений потребуется порядка u^3 арифметических операций, что при больших u может потребовать существенных вычислительных затрат. На практике для декодирования алгебраических кодов используют алгоритм Берлекэмпа-Мэсси, суть которого состоит в итеративном построении минимального регистра сдвига с обратной связью, генерирующего известную последовательность синдромов $s = (s_0, s_1, ..., s_{n-k-1})$. Сложность такого алгоритма составляет u^2 арифметических операций. Еще более эффективным, с точки зрения вычислительной сложности, является рекуррентный алгоритм Берлекэмпа-Месси [38-40]. Асимптотическая сложность декодирования кодов Рида-Соломона в этом случае не превосходит величины $O(n\log^2 n)$, причем очень близка к величине $O(n\log n)$.

Коды Рида-Соломона имеют небольшою длину – число корней $X_0, X_1, ..., X_{n-k-1} \in GF(q^m)$ не может быть больше числа элементов поля $GF(q^m)$ и, следовательно, $n \le q^m - 1$ (процедурами модификации кодов можно увеличить длину кода еще на 2 символа). Ограничением на подполе $GF(q)$ можно получить большую длину n кода при фиксированном q, однако кодовые (n,k,d) параметры лежат значительно ниже кодовых границ (1), (2) и с увеличением длины n это тенденция усиливается. Тем не менее существуют классы алгебраических кодов, которые лежат выше границ (1) и (2).

Определение 1 [38-40]. Пусть $X = (X_0, X_1, ..., X_{n-1})$ вектор над $GF(q^m)$, причем все X_i – различные элементы $GF(q^m)$. Пусть также $B = (B_0, B_1, ..., B_{n-1})$ – вектор над $GF(q^m)$ с необязательно различными B_i элементами $GF(q^m)$. Тогда (n, k, d) обобщенный код Рида-Соломона $ОРС_k(X, h)$ состоит из всех векторов вида

$$(B_0 \cdot F(X_0), B_1 \cdot F(X_1), ..., B_{n-1} \cdot F(X_{n-1})),$$

где $F(x)$ – любой многочлен с коэффициентами из $GF(q^m)$, степень которого не превосходит k.

Код ОРС является МДР кодом, его проверочная матрица $ОРС_k(X, h)$ равна:

$$H=\begin{pmatrix} Y_0 & Y_1 & \dots & Y_{n-1} \\ X_1\cdot Y_0 & X_2\cdot Y_1 & \dots & X_{n-1}\cdot Y_{n-1} \\ X_1^2\cdot Y_0 & X_2^2\cdot Y_1 & \dots & X_{n-1}^2\cdot Y_{n-1} \\ \dots & \dots & \dots & \dots \\ X_1^{n-k-1}\cdot Y_0 & X_2^{n-k-1}\cdot Y_1 & \dots & X_{n-1}^{n-k-1}\cdot Y_{n-1} \end{pmatrix}= \\ =\begin{pmatrix} 1 & 1 & \dots & 1 \\ X_1 & X_2 & \dots & X_{n-1} \\ X_1^2 & X_2^2 & \dots & X_{n-1}^2 \\ \dots & \dots & \dots & \dots \\ X_1^{n-k-1} & X_2^{n-k-1} & \dots & X_{n-1}^{n-k-1} \end{pmatrix}\cdot\begin{pmatrix} Y_0 & 0 & \dots & 0 \\ 0 & Y_1 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & Y_{n-1} \end{pmatrix}, \tag{15}$$

где вектор $Y = (Y_0, Y_1, \dots, Y_{n-1})$ такой, что $\forall Y_i \in GF(q^m)$, $Y_i \neq 0$ и дуальным к $ОРС_k(X, B)$ является $ОРС_{n-k}(X, Y)$.

Через определение ОРС вводится обширный класс т.н. альтернантных кодов [38-40].

Определение 2 [38-40]. Альтернантный (n, k, d) код $A(X, B)$ состоит из всех слов кода $ОРС_k(X, B)$ таких, что их компоненты лежат в поле $GF(q)$. Другими словами, $A(X, B)$ равен ограничению кода $ОРС_k(X, B)$ на подполе $GF(q)$, т.е. он состоит из всех векторов c над $GF(q)$, для которых выполняется равенство $cH^T = 0$, где H – проверочная матрица $ОРС_k(X, B)$, задаваемая выражением (15). Порождающая матрица $A(X, B)$ может быть получена заменой каждого элемента матрицы H в (15) соответствующим вектором-столбцом длины m над $GF(q)$.

Параметры кода $A(X, B)$ связаны соотношением: $n - mr \le k \le n - r$; $d \ge r + 1$, причем доказано [38-40], что среди большого числа всех возможных альтернантных кодов при фиксированном n и k найдутся такие коды, параметры которых лежат выше кодовых границ (1) и (2). Одним из частных случаев $A(X, B)$ являются коды Гоппы [42,43].

Определение 3 [40]. Альтернантный (n, k, d) код Гоппы $\Gamma(L, G)$ над $GF(q)$ состоит из всех векторов $c = (c_1, c_2, \dots, c_n)$ таких, что

$$R_c(x) \equiv 0 \bmod G(x), \tag{16}$$

где

$$R_c(x) = \sum_{i=1}^{n} \frac{c_i}{x - \alpha_i},$$

$G(x)$ – многочлен с коэффициентами из $GF(q^m)$ (многочлен Гоппы), $L = (\alpha_1, \alpha_2, \dots, \alpha_n)$ – подмножество элементов из $GF(q^m)$ таких, что $G(\alpha_i) \neq 0 \ \ \forall \alpha_i \in L$.

Используя выражение (16) проверочную матрицу кода Гоппы можно задать следующим образом. Многочлен $x - \alpha_i$ в кольце многочленов по модулю $G(x)$ имеет обратный многочлен:

$$(x - \alpha_i)^{-1} = -\frac{G(x) - G(\alpha_i)}{x - \alpha_i} G^{-1}(\alpha_i).$$

Следовательно, вектор $c = (c_1, c_2, \dots, c_n)$ принадлежит коду Гоппы $\Gamma(L, G)$ тогда и только тогда, когда

$$\sum_{i=1}^{n} c_i \frac{G(x) - G(\alpha_i)}{x - \alpha_i} G^{-1}(\alpha_i) = 0. \tag{17}$$

Если $G(x) = \sum_{i=0}^{r} g_i x^i$, где $g_i \in GF(q^m)$ и $g_r \neq 0$, то

$$\frac{G(x) - G(\alpha_i)}{x - \alpha_i} = g_r(x^{r-1} + x^{r-2}\alpha_i + \dots + \alpha_i^{r-1}) + g_{r-1}(x^{r-2}\alpha_i + \dots + \alpha_i^{r-1}) + \dots + g_2(x + \alpha_i) + g_1.$$

Приравнивая согласно (17) нулю все коэффициенты при x^{r-1}, x^{r-2}, …, 1, получим, что условие $cH^T = 0$ выполнится только если

$$H = \begin{pmatrix} g_r G^{-1}(\alpha_1) & g_r G^{-1}(\alpha_2) & \dots \\ (g_{r-1} + \alpha_1 g_r) G^{-1}(\alpha_1) & (g_{r-1} + \alpha_2 g_r) G^{-1}(\alpha_2) & \dots \\ \dots & \dots & \dots \\ (g_1 + \alpha_1 g_2 + \dots + \alpha_1^{r-1} g_r) G^{-1}(\alpha_1) & (g_1 + \alpha_2 g_2 + \dots + \alpha_2^{r-1} g_r) G^{-1}(\alpha_2) & \dots \end{pmatrix}$$

$$\begin{pmatrix} \dots & g_r G^{-1}(\alpha_n) \\ \dots & (g_{r-1} + \alpha_n g_r) G^{-1}(\alpha_n) \\ \dots & \dots \\ \dots & (g_1 + \alpha_n g_2 + \dots + \alpha_n^{r-1} g_r) G^{-1}(\alpha_n) \end{pmatrix} =$$

$$= \begin{pmatrix} g_r & 0 & \dots & 0 \\ g_{r-1} & g_r & \dots & 0 \\ \dots & \dots & \dots & \dots \\ g_1 & g_2 & \dots & g_r \end{pmatrix} \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \dots & \dots & \dots & \dots \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \dots & \alpha_n^{r-1} \end{pmatrix} \begin{pmatrix} G^{-1}(\alpha_1) & 0 & \dots & 0 \\ 0 & G^{-1}(\alpha_2) & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & G^{-1}(\alpha_n) \end{pmatrix}.$$

Матрица

$$\begin{pmatrix} g_r & 0 & \dots & 0 \\ g_{r-1} & g_r & \dots & 0 \\ \dots & \dots & \dots & \dots \\ g_1 & g_2 & \dots & g_r \end{pmatrix}$$

- обратима. Следовательно, проверочная матрица

$$H = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \dots & \dots & \dots & \dots \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \dots & \alpha_n^{r-1} \end{pmatrix} \begin{pmatrix} G^{-1}(\alpha_1) & 0 & \dots & 0 \\ 0 & G^{-1}(\alpha_2) & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & G^{-1}(\alpha_n) \end{pmatrix} =$$

$$= \begin{pmatrix} G^{-1}(\alpha_1) & G^{-1}(\alpha_2) & \dots & G^{-1}(\alpha_n) \\ \alpha_1 G^{-1}(\alpha_1) & \alpha_2 G^{-1}(\alpha_2) & \dots & \alpha_n G^{-1}(\alpha_n) \\ \dots & \dots & \dots & \dots \\ \alpha_1^{r-1} G^{-1}(\alpha_1) & \alpha_2^{r-1} G^{-1}(\alpha_2) & \dots & \alpha_n^{r-1} G^{-1}(\alpha_n) \end{pmatrix}$$

также задает *(n, k, d)* код Гоппы *Γ(L, G)* над *GF(q)*.

Последнее выражение при $Y = (Y_1, Y_2, \dots, Y_n)$, $Y_1 = G^{-1}(\alpha_1)$, $Y_2 = G^{-1}(\alpha_2)$, …, $Y_n = G^{-1}(\alpha_n)$ эквивалентно выражению (15). Проверочную матрицу *Γ(L, G)* над *GF(q)* с элементами из *GF(q)* можно получить путем представления каждого элемента из $GF(q^m)$ вектором-столбцом длины *m* символов из *GF(q)*. Справедлива следующая оценка.

Теорема 3 [40,42,43]. Параметры *(n, k, d)* кода Гоппы *Γ(L, G)* связаны соотношениями: $n = |L|$, $k \geq n - mr$, $r = deg\ G(x)$, $d \geq r + 1$.

Для сепарабельных (когда многочлен *G(x)* не имеет кратных корней ни в одном расширении поля) двоичных кодов Гоппы минимальное кодовое расстояние $d \geq 2r + 1$. Причем, если *G(x)* - неприводимый многочлен степени *r* над $GF(q^m)$ и $L = GF(q^m)$, тогда существует код Гоппы над $GF(q^m)$ лежащий на границе Варшамова-Гилберта [40,42,43].

Теорема 3 гарантирует существование альтернантных кодов, построенных через многочлен Гоппы, с кодовыми характеристиками, удовлетворяющими (1), (2). При соответствую-

щем выборе вектора-шаблона $Y = (Y_1, Y_2, \ldots, Y_n)$ удается построить блоковые коды лежащие выше границы Варшамово-Гилберта [40,42,43]. Это свойство рассмотренных кодовых конструкций указывает на перспективность применения альтернантных кодов, в том числе и кодов Гоппы, для решения различных инженерных задач как в области повышения помехоустойчивости передачи данных, так и для криптографической защиты информационных ресурсов. В частности, использование рассмотренных положений алгебраической теории блоковых кодов в криптографических целях позволяет реализовать несимметричные криптосистемы доказуемой стойкости *(provable security)*, которые, помимо высокой скорости двухключевого криптографического преобразования и возможности совмещать контроль ошибок с защитой от несанкционированного ознакомления [15-22], остаются стойкими даже в случае использования квантовых вычислений [28].

3 Несимметричные криптосистемы на основе алгебраических блоковых кодов (теоретико-кодовые схемы)

Рассмотрим схемы несимметричного криптографического преобразования, построение которых основано на использовании алгебраических кодов, замаскированных под код общего положения (случайный код, полный код) [15-22]. Рассмотрим современное состояние, существующие противоречия и перспективы их практического использования в том числе на постквантовый период.

Криптосистема Мак-Элиса. Первой и наиболее изученной схемой несимметричного шифрования, основанной на использовании алгебраических блоковых кодов, является предложенная в 1978 году криптосистема Мак-Элиса (McEliece) [15]. Она обладает неоспоримыми преимуществами: высокой скоростью криптографического преобразования, а также возможностью совмещать контроль ошибок с защитой от несанкционированного ознакомления [15-22]. Подобные (крипто-кодовые) преобразования остаются стойкими и при использовании квантовых вычислений [28]. Открытым ключом в схеме Мак-Элиса является матрица

$$G_X = XGPD, \tag{18}$$

где G – порождающая матрица алгебраического (n,k,d) кода над $GF(q)$ (в оригинальной статье [15] предлагалось использовать рассмотренный выше двоичный код Гоппы), X - невырожденная $k \times k$ матрица с элементами из $GF(q)$, P и D – перестановочная и диагональная $n \times n$ матрицы (для двоичных кодов используется только матрица P).

Матрицы X, P и D являются секретным ключом, который маскирует используемый алгебраический блоковый код под случайный код (код общего положения), т.е. открытый ключ G_X представляется злоумышленнику как случайно сформированная порождающая матрица некоторого линейного кода, для которого неизвестен алгоритм быстрого декодирования. Напротив, уполномоченный пользователь, знающий секретный ключ (матрицы X, P и D), может снять действие маскирующих матриц и воспользоваться быстрым алгоритмом декодирования алгебраического кода с порождающей матрицей G.

Криптограмма представляет собой вектор длины n, который вычисляется по правилу

$$c_X^* = IG_X + e, \tag{19}$$

где вектор

$$c_X = IG_X$$

является кодовым словом замаскированного кода, т.е. c_X принадлежит (n,k,d) коду с порождающей матрицей G_X, I – k-разрядный информационный вектор над $GF(q)$, вектор e – секретный вектор ошибок веса

$$w_h(e) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

Вектор e следует рассматривать как одноразовый сеансовый секретный ключ, его вес определяет сложность декодирования искаженного кодового слова (криптограммы) c_X^*. Злоумышленнику необходимо декодировать кодограмму c_X^* используя известную ему порождающую матрицу G_X. Однако декодирование случайного кода (при соответствующих параметрах n, k, q и $w_h(e)$) вычислительно недостижимо. Не зная матрицы X, P и D злоумышленник не может восстановить матрицу G и воспользоваться алгоритмом декодирования полиномиальной сложности. Из этих соображений величину $w_h(e)$ следует максимизировать, например, при $w_h(e) = t$ сложность декодирования будет максимальной, что обеспечит наивысший уровень стойкости кодовой криптосистемы для заданных параметров n, k, q.

Для уполномоченного пользователя (знающего секретный ключ) декодирование – полиномиально разрешимая задача. Действительно, легитимный пользователь, получив вектор c_X^*, строит вектор $\overline{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1}$. Матрица $\Lambda = PD$ сохраняет вес и расстояние по Хеммингу, т.е. для любых кодовых слов c и c' выполняются равенства:

$$w_h(c) = w_h(c\Lambda),\ w_h(c, c') = w_h(c\Lambda, c'\Lambda).$$

Это означает, что вектор $\overline{c}^*$ является искаженным не более чем в t разрядах кодовым словом алгебраического кода с порождающей матрицей G и его можно декодировать быстрым алгоритмом полиномиальной сложности [19].

Уполномоченный пользователь, используя алгоритмом полиномиальной сложности, декодирует вектор $\overline{c}^* = I' \cdot G + e'$, т.е. находит I'. Затем он вычисляет k-разрядный информационный вектор $I = I' X^{-1}$.

Таким образом, в криптосистеме Мак-Элиса основным средством маскировки линейного блокового *(n, k, d)* кода под линейный случайный код (код общего положения) являются матрицы *X, P, D*. Дополнительным секретным параметром, который можно использовать в случае кодов Гоппы, является многочлен Гоппы *G(x)*, или, в более широком смысле, вектор $Y = (Y_0, Y_1, \ldots, Y_{n-1})$ в случае альтернантных кодов (см. выражения (15)-(17)). Изменение шаблона не снижает конструктивных кодовых характеристик, т.е. с точки зрения криптографического преобразования не приведет к снижению безопасности. Однако знание вектора-шаблона $Y = (Y_0, Y_1, \ldots, Y_{n-1})$ (или многочлена *G(x)*) является необходимым для правильного декодирования информационного сообщения, т.е. для корректного расшифрования на приемной стороне.

Опубликовано большое число различных атак на крипто-кодовые схемы защиты информации [19,33-36], некоторые из которых оказались достаточно эффективными относительно отдельных вариантов кодовых криптосистем. Однако базовая конструкция [15], предложенная около 40 лет назад, остается стойкой ко всем известным, на сегодняшний день, методам криптоанализа, в том числе и в случае использования квантовых вычислительных систем.

Наиболее естественным направлением в развитии методов криптоанализа кодовой схемы Мак-Элиса является использование неалгебраических методов декодирования. Действительно, если существует вычислительно эффективный способ декодирования кодового слова (19) только по известной порождающей матрице (18), тогда информационное сообщение I может быть эффективно восстановлено и без знания секретного ключа (матриц X, P и D).

Среди универсальных методов декодирования линейных блоковых кодов, заданных произвольной порождающей матрицей, особое место занимают перестановочные алгоритмы [38-40]. Основная идея такого декодирования состоит в использовании различных наборов информационных множеств. Представим порождающую матрицу (19) в каноническом виде (4). Единичные вектора-столбцы в (4) могут быть выбраны произвольно с соответствующим формированием единичных подматриц и систематическим размещением k символов информационного множества. Оставшиеся $(n-k)$ символов однозначно вычисляются по элементам информационного множества. Позиции этих $(n-k)$ символов задают размещение

единичных вектор-столбцов соответствующей проверочной матрицы H^* (6). Если выбрать размещение $(n-k)$ единичных вектор-столбцов в (6) таким образом, чтобы они покрыли все t позиций ненулевых элементов вектора ошибок e, тогда кодовое слово, вычисленное по k символам информационного множества, не будет содержать ошибок, т.е. слово (19) можно декодировать даже без знания специальной алгебраической структуры порождающей (проверочной) матрицы используемого алгебраического кода.

Таким образом, при реализации переставного декодирования конкретная комбинация ошибок будет исправлена, только если удастся найти такое информационное множество, которое целиком содержит эту комбинацию. Такое множество, являющееся кровельной комбинацией ошибок, и набор проверочных множеств, которые покрывают все наборы ошибок данного типа, называют покрытием [38]. Задача декодера состоит в том, чтобы найти проверочное множество, которое покрывает неизвестную комбинацию ошибок.

Рассмотрим границы для количества кровельных множеств. Предположим, что с помощью *(n, k, d)* кода исправляются все комбинации из *t* или меньшего количества ошибок. Рассмотрим комбинацию только из *t* кратных ошибок, так как все ошибки меньшей кратности будут покрыты. Общее количество комбинаций ошибок во всех *n* позициях равно $C_n^t = \frac{n!}{t!(n-t)!}$. Поскольку объем кровельного множества равен *n – k*, максимальное количество комбинаций ошибок, которые могут быть покрытые данным множеством равно $C_{n-k}^t = \frac{(n-k)!}{t!(n-k-t)!}$. Наименьшее количество множеств, которые могут исправить все комбинации из *t* ошибок, ограничивается выражением [38]:

$$N \geq \frac{C_n^t}{C_{n-k}^t} = \frac{\frac{n!}{t!(n-t)!}}{\frac{(n-k)!}{t!(n-k-t)!}} = \frac{n!(n-k-t)!}{(n-t)!(n-k)!}. \qquad (20)$$

На рис. 1 приведены зависимости наименьшего числа кровельных множеств, которые потребуется для исправления всех комбинации из *t* ошибок произвольного линейного блокового кода. Оценки *N* приведены в логарифмическом масштабе в зависимости от относительной скорости кодирования $R = k/n$ и рассчитаны для параметров двоичных сепарабельных кодов Гоппы: $n = 2^m$, $k \geq n - mr$, $r = deg\ G(x)$, $d \geq 2r + 1$.

Зависимости, приведенные на рис. 1, можно интерпретировать как оценки стойкости крипто-кодовых преобразований, выраженные в наименьшем числе покрывающих множеств, которые потребуется перебрать для декодирования любой конфигурации вектора ошибок e. Эти зависимости не учитывают вычислительную сложность формирования слов-кандидатов, вычисляемых по выбранной конфигурации информационного множества *(реальная стойкость будет еще выше)*.

Как следует зависимостей, представленных на рис.1, наибольшую стойкость схема Мак-Элиса обеспечивает при использовании кодов с относительной скоростью $R \approx 2/3$, что согласуется с выводами большинства исследований [28].

В таблице 1 приведены параметры некоторых схем с кодами Гоппы и $R \approx 2/3$, оценки стойкости к атаке перестановочного декодирования, оценки вычислительной сложности кодирования (зашифрования) и декодирования (расшифрования), а также аналогичные оценки для несимметричного шифрования RSA и блочного симметричного шифрования AES (FIPS-197) / Kalyna (DSTU 7624:2014) [44, 45].

Для схемы Мак-Элиса значения в таблице 1 оценивались следующим образом:

- размер открытого ключа оценивался как число двоичных элементов матрицы $G_X - kn$ бит;
- размер закрытого ключа оценивался как число элементов матрицы X (k^2 бит) плюс число элементов, необходимых для хранения правила перестановки ($n\log_2 n$ бит).

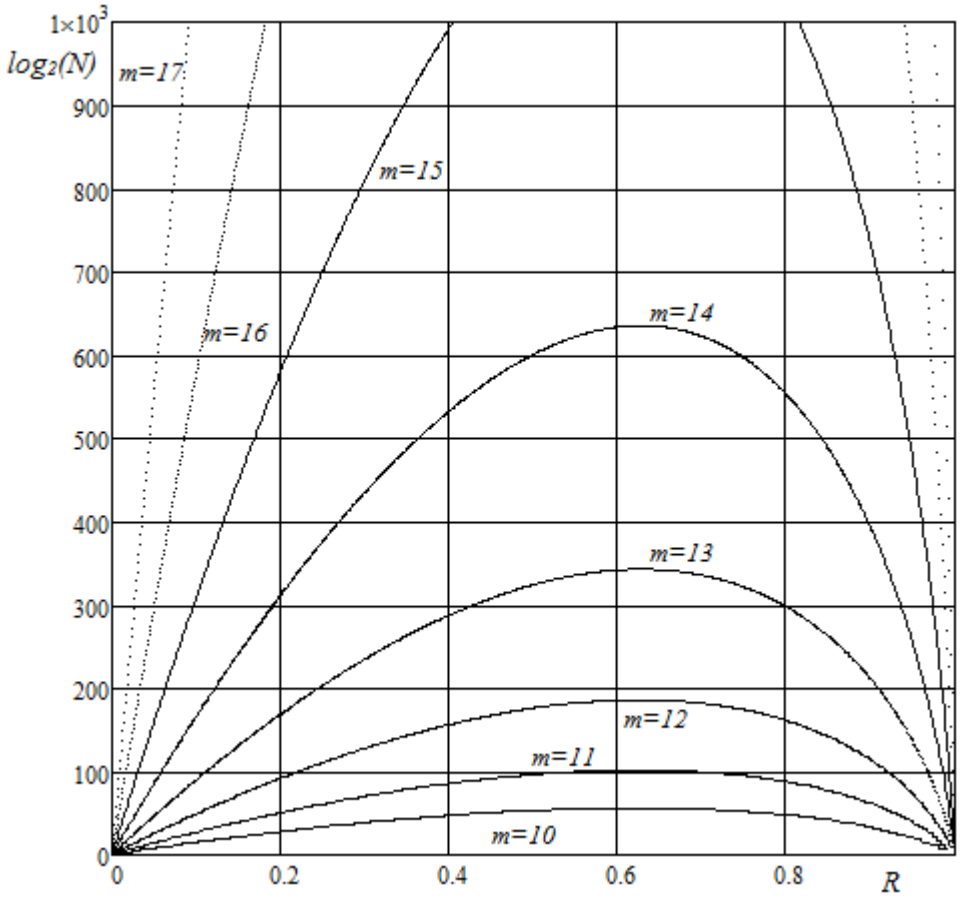

Рис. 1 – Оценка стойкости схемы Мак-Элиса на сепарабельных двоичных кодах Гоппы к атаке перестановочным декодированием

Таблица 1 – Оценка характеристик криптосистемы Мак-Элиса

Оцениваемые параметры	**Уровень стойкости** *(без учета квантового криптоанализа)*			
	Достаточный (2^{80} … 2^{128})	**Высокий** (2^{192} … 2^{256})		**Сверхвысокий** ($> 2^{512}$)
Криптосистема Мак-Элиса				
Параметры (*n, k, d*)	(2 048, 1 300, 137)	(4 096, 2 584, 253)		(16 384, 10 322, 867)
Размер секретного ключа, бит	1 712 528	6 726 208		106 773 060
Размер открытого ключа, бит	2 662 400	10 584 064		169 115 648
Сложность шифрования, операций XOR	1 300	2 584		10 322
Сложность расшифрования, операций над $GF(2^m)$	4 624	15 876		187 489
Оценка стойкости (эквивалентная длина ключа симметричного шифра), $\log_2 N$	102	186		636
Оценка стойкости к квантовому криптоанализу, бит	49	91		310
Криптосистема RSA				
Размер модуля и открытого (закрытого) ключа, бит	2 048	7 680	15360	
Сложность шифрования (расшифрования), битовых операций	$3{,}2 \cdot 10^9$	$1{,}7 \cdot 10^{11}$	$1{,}4 \cdot 10^{12}$	
Оценка стойкости (эквивалентная длина ключа симметричного шифра), бит	112	192	256	
Оценка стойкости к квантовому криптоанализу, бит	40	41	44	
Блочный симметричный шифр AES (FIPS-197) / Kalyna (DSTU 7624:2014)				
Размер секретного ключа (оценка стойкости), бит	128	196	256	512
Сложность шифрования (расшифрования), операций на слово	40	48	56	72
Оценка стойкости к квантовому криптоанализу, бит	64	98	128	256

Сложность шифрования оценивалась как максимальное число операций, которые необходимо выполнить для формирования кодового слова посредством матричного вычисления выражения (19). Для двоичного *(n, k, d)* кода это соответствует *k* операциям XOR над *n* битными словами. Если вычисления реализуются под управлением 32(64)-битной операционной системы, тогда каждое *n* битное кодовое слово представляется как набор из *n/32* (*n/64*) машинных слов и для вычисления каждого из них потребуется выполнить не более *k* операций XOR.

Сложность расшифрования оценивалась как максимальное число арифметических операций над конечным полем $GF(2^m)$, которые необходимо выполнить для декодирования кодового слова с ошибками. При этом сложность декодирования оценивалась как t^2. В практических приложениях операции сложения элементов поля $GF(2^m)$ реализуются операцией XOR, а операции умножения – табличным способом, т.е. через обращение к ячейке памяти с заданным входными аргументами адресом, так что оценка t^2 выглядит вполне правдоподобной.

Оценка стойкости кодовой криптосистемы Мак-Элиса к квантовому криптоанализу проведена в работах [46, 47]. В частности, в [47] приводится оценка числа итераций для декодирования квантовых алгоритмом Гровера *(Grover's algorithm).* Эта оценка имеет вид:

$$C^{\frac{n}{2\log n}},\ C = \frac{1}{(1-R)^{1-R}}, \tag{21}$$

где $R = k/n$ - относительная скорость используемого кода.

Значения, приведенные в таблице 1, рассчитаны по соотношению (21). На практике оценка (21) снижает стойкость криптосистемы *(примерно в два раза уменьшается эквивалентная длина ключа)*, что, впрочем, вполне ожидаемо для надежных постквантовых алгоритмов *(как и для большинства симметричных шифров)*.

Для криптосистемы RSA значения в таблице 1 оценивались следующим образом. Скорость криптопреобразования (шифрования и расшифрования) оценивалась как сложность модульного возведения в степень. В работе [48] показано (стр. 613), что в общем случае для *l*-битных чисел операция модульного возведения в степень требует порядка $\frac{3}{2}l^3$ двоичных операций. Пусть *p* и *q* – два *l*-битных простых числа, модуль преобразования RSA (общесистемный параметр) равен *n* = *pq* (2*l*-битное число), а открытым (секретным) ключом являются 2*l*-битные числа *e* и *d*. Тогда сложность модульного возведения в степень при шифровании (расшифровании) потребует $\frac{3}{2}(2l)^3 = 12l^3$ операций. Более эффективным является последовательное вычисление возведения в степень по модулям (*p – 1*) и (*q – 1*), соответственно. Такой алгоритм потребует в два раза большее число операций, однако в связи с уменьшением размерности модулей общее число операций сократится. Сложность преобразования составит $2\frac{3}{2}l^3 = 3l^3$ и значения, приведенные в таблице 1, соответствуют этой оценке. Размер модуля и соответствующая оценка стойкости (как эквивалентная длина ключа симметричного шифра) указана в работе [49].

Оценки объема квантовых ресурсов, необходимых для решения некоторых асимметричных криптографический задач с помощью алгоритма Шора, при различных параметрах этих задач, и сравнение их со сложностью решения переборного задачи при поиске ключа симметричного шифра приведены в [50]. В частности, для m-битного числа дается оценка $4m^3$ временной сложности квантового алгоритма факторизации Шора и значения, приведенные в таблице 1, соответствуют этой оценке.

Описание блочных симметричных шифров AES (FIPS-197) и Kalyna (DSTU 7624:2014) приведено в [44, 45]. Исследование сложности квантовых алгоритмов криптоанализа симметричных шифров представлено в [51]. В частности, квантовый алгоритм Гровера для решения переборных задач, в том числе, переборного поиска m-битного секретного ключа

симметричного шифра, требует выполнения $\frac{\pi}{4}\sqrt{2^m}$ итераций. На практике же это приводит к соответствующему снижению стойкости *(в два раза уменьшается эквивалентная длина ключа)*.

Следует обратить внимание на высокую скорость криптографического преобразования в схеме Мак-Элиса, которая приближается по скорости шифрования к блочным симметричным шифрам. Действительно, при использовании кода Гоппы с рекомендованными в авторской статье [15] параметрами

$$n = 1024, k = 524, t = 50, d = 2t + 1 = 101,$$

для зашифрования матричным способом (вычисление $IG_X + e$) потребуется выполнить не более 524 операций XOR на одно обрабатываемое слово.

Для примера, один из самых быстрых современных блочных симметричных шифров AES *(американский стандарт шифрования FIPS-197)* требует для зашифрования не менее 4 операций XOR на 32-х битное слово на каждом раунде [44], что при 10 раундах составит не менее 40 операций XOR.

Вторым важным преимуществом схемы Мак-Элиса является возможность совмещать криптографичское преобразование с контролем возникающих ошибок. Действительно, если при формировании криптограммы (18) использовать случайный вектор ошибок e, веса $w(e) < t$, тогда появляется возможность одновременно с криптографическим преобразованием данных контролировать ошибки в пределах исправляющей способности. Уменьшение веса вектора e снизит криптографическую стойкость схемы Мак-Элиса, однако повысит помехоустойчивость передачи данных, т.е. в такой «гибридной» схеме изменяя $w(e)$ можно адаптивно реагировать на потребность в соответствующих услугах безопасности.

Обозначим долю веса вектора ошибок вектора e, приходящегося на искусственное внесение при формировании криптограммы (см. выражение (18)) символом $\rho = w(e) / t$. Тогда стойкость криптосистемы, построенная на алгебраических кодах, будет определяться величиной $\rho \cdot t$, а обеспечиваемая помехоустойчивость передаваемых криптограмм определяться величиной $(1 - \rho) \cdot t$.

Третье и, очевидно, одно из важнейших положительных свойств криптосистемы Мак-Элиса является высокая устойчивость к квантовому криптоанализу. По сравнению с другими несимметричными криптосистемами, например, с RSA, сложность квантового криптоанализа кодовой криптосистемы с увеличением ее параметров возрастает очень быстро. Фактически, сложность криптоанализа квантовыми алгоритмами сопоставима с решением переборных задач поиска эквивалентных ключей симметричных шифров. Данные таблицы 1 наглядно подтверждают эту тенденцию.

Основными недостатками рассмотренной кодовой крптосистемы являются огромные объемы ключевых данных (десятки мегабит), а также снижение относительной скорости передачи информации (наибольшая стойкость криптосистемы достигается при относительной скорости кодирования $R = k/n \approx 2/3$). Ниже будет показано, что относительную скорость передачи данных можно существенно повысить (рассматриваемые в данной работе кодовые криптосистемы снимают этот конструктивный недостаток схемы Мак-Элиса).

Криптосистема Нидеррайтера. Альтернативным примером криптосистем на кодах есть схема Нидеррайтера, впервые предложенная в [16]. Открытым ключом в этой криптосистеме есть матрица

$$H_X = XHPD, \tag{22}$$

где H – проверочная матрица алгебраического (n,k,d) кода над $GF(q)$ (в оригинальной статье [16] предлагалось использовать обобщенные коды Рида-Соломона), X - невырожденная $(n-k)\times(n-k)$ матрица с элементами из $GF(q)$, P и D – перестановочная и диагональная $n \times n$ матрицы (для двоичных кодов используется только матрица P).

Матрицы X, P и D (как и для криптосистемы Мак-Элиса) являются секретным ключом, который маскирует используемый алгебраический блоковый код под случайный код (код

общего положения), т.е. открытый ключ (22) представляется злоумышленнику как случайно сформированная проверочная матрица некоторого линейного кода, для которого неизвестен алгоритм быстрого декодирования.

Напротив, уполномоченный пользователь, знающий секретный ключ (матрицы X, P и D), может снять действие маскирующих матриц и воспользоваться быстрым алгоритмом декодирования алгебраического кода с проверочной матрицей H.

Криптограмма S_X представляет собой вектор длины $(n-k)$ и вычисляется по правилу

$$S_X = e \cdot H_X^T, \tag{23}$$

где вектор e – вектор длины n и веса $w_h(e) \le t$, который несет конфиденциальную информацию (информационное сообщение, подлежащее зашифрованию). Наибольшая стойкость обеспечивается при $w_h(e) = t$.

Уполномоченный пользователь (имеющий секретный ключ) находит одно из q^k решений выражения $S_X = c_X^* \cdot H_X^T$. Найденное решение - суть кодовое слово с ошибками $c_X^* = I \cdot G_X + e$. Далее, как и в схеме Мак-Элиса, уполномоченный пользователь строит вектор $\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1}$ и декодирует полученное слово. Однако, вместо восстановления информационного слова I', он вычисляет кодовое слово $c' = I' \cdot G$, а затем и вектор ошибок $e' = \bar{c}^* - c'$. На последнем шаге производится вычисление вектора $e = e' \cdot P \cdot D$, который несет конфиденциальную информацию.

Таким образом, в криптосистеме Нидеррайтера основным средством маскировки линейного кода под случайный код являются (как и в криптосистеме Мак-Элиса) матрицы *X, P, D.* Если использовать коды Гоппы, тогда многочлен *G(x)* может выступать дополнительным секретным параметром.

В работе [19] показано, что стойкости криптосистем Мак-Элиса и Ниддерайтера эквивалентны и эффективную атаку на одну из схем можно легко трансформировать в атаку на другую схему. В этом смысле оценки стойкости криптосистемы Мак-Элиса, приведенные в таблице 1, справедливы и по отношению к криптосистеме Ниддерайтера. Другие характеристики этих криптосистем (скорость шифрования/расшифрования, объемы закрытого и открытого ключа) также сопоставимы.

Очевидным преимуществом теоретико-кодовой схемы Нидеррайтера по сравнению с криптосистемой Мак-Элиса является потенциально большая относительная скорость передачи данных. Действительно, относительная скорость в криптосистеме Мак-Элиса определяется относительной скоростью используемого (n,k,d) кода, т.е. равна $R = k/n$, причем наибольшая стойкость достигается при $R = k/n \approx 2/3$ (см. рис. 1). Информационное сообщение в системе Нидеррайтера сперва преобразуется в равновесную последовательность e длины n и веса $w_h(e) \le t$, а затем умножается на проверочную матрицу как в (23).

Положим $w_h(e) = t$ (в этом случае будет обеспечена максимальная стойкость криптосистемы для заданных (n,k,d) параметров кода). Тогда максимальное число бит информационных данных, которые можно зашифровать в системе Нидеррайтера при использовании двоичного (n,k,d) кода, будет определятся выражением:

$$l_{\inf} = \lfloor \log_2 C_n^t \rfloor = \left\lfloor \log_2 \left(\frac{n!}{t!(n-t)!} \right) \right\rfloor,$$

где $\lfloor x \rfloor$ - наибольшее целое число, меньшее x.

Криптограмма (23) представляет собой синдромный вектор длины $n-k$, т.е. относительная скорость передачи данных в криптосистеме Нидеррайтера (для двоичных кодов) будет определяться выражением:

$$R^* = \frac{\left\lfloor \log_2\left(\frac{n!}{t!(n-t)!}\right)\right\rfloor}{n-k}.$$

Последнее выражение легко обобщается на случай недвоичных кодов с основанием q:

$$R^* = \frac{\left\lfloor \log_q\left((q-1)^t \frac{n!}{t!(n-t)!}\right)\right\rfloor}{n-k}. \quad (24)$$

Если предположить, что информационная последовательность будет преобразовываться во все возможные вектора e длины n и веса $0 \le w_h(e) \le t$, тогда последнее выражение примет вид:

$$R^* = \frac{\left\lfloor \log_q\left(\sum_{i=0}^{t}(q-1)^i \frac{n!}{i!(n-i)!}\right)\right\rfloor}{n-k}. \quad (25)$$

Алгоритм кодирования информационной последовательности в равновесную последовательность e длины n и веса $w_h(e)$ для произвольного основания q приводится, например, в работе [52].

Выражение (25) достигает максимума для т.н. *совершенных кодов* (perfect codes), кодовые (n,k,d) параметры которых удовлетворяют верхней границе Хемминга для мощности (числа кодовых слов) $A_q(n,d)$ произвольного линейного q-ичного кода [38-40]:

$$A_q(n,d) \le \frac{q^n}{\sum_{i=0}^{t}(q-1)^i \frac{n!}{i!(n-i)!}}. \quad (26)$$

Мощность линейного (n,k,d) кода над $GF(q)$ равна q^k, следовательно из (26) следует ограничение на число информационных символов кода

$$k \le n - \log_q\left(\sum_{i=0}^{t}(q-1)^i \frac{n!}{i!(n-i)!}\right).$$

Если параметры (n,k,d) кода удовлетворяют верхней границе Хемминга, т.е. достигается равенство в (26) и код совершенен, тогда

$$\log_q\left(\sum_{i=0}^{t}(q-1)^i \frac{n!}{i!(n-i)!}\right) = n-k, \quad (27)$$

что после подстановки в (25) дает $R^* = 1$, т.е. относительная скорость передачи максимальна и криптограмма в схеме Нидеррайтера не будет содержать избыточных символов.

В качестве примера приведем совершенный двоичный ($q = 2$) код Хемминга исправляющий одну ошибку ($t = 1$). Он определен для любого положительного целого $m > 2$ и имеет кодовые параметры $(2^m - 1, 2^m - m - 1, 3)$ [38 – 40]. Очевидно, что для этих значений

$$\sum_{i=0}^{t}\frac{n!}{i!(n-i)!} = 2^m,\ n-k = m$$

и относительная скорость (25) равна 1.

Другим примером является совершенный двоичный код Голея *(perfect binary Golay code)* с параметрами $(23, 12, 7)$ [38-40]. Он позволяет исправить $t = 3$ ошибки и для этих значений имеем

$$\sum_{i=0}^{t}\frac{n!}{i!(n-i)!} = 2048,\ n-k = 12,$$

т.е. относительная скорость (25) также равна 1.

К сожалению, в [53-54] показано, что любой нетривиальный совершенный код имеет параметры кода Хэмминга или кода Голея, т.е. достижение максимальной относительной скорости в системе Нидеррайтера ограничивается только этими конструкциями.

Большинство других кодов, в том числе и коды Гоппы, обладают конструктивными (n,k,d) параметрами, лежащими существенно ниже верхней границы (26) *(реальные дистанционные характеристики кодов Гоппы выше)*. Например, для кода Гоппы с параметрами *n = 1024, k = 524, t = 50* (использован в авторском варианте [15] схемы Мак-Элиса) относительная скорость шифрования (24) в схеме Нидеррайтера равна $R^* \approx 0{,}57$, что несущественно больше по сравнению со скоростью $R \approx 0{,}51$ в схеме МакЭлиса. С увеличением длины кода конструктивные параметры кодов Гоппы ухудшаются, что приводит к снижению скорости R^*. Эту тенденцию наглядно демонстрируют результаты расчетов, представленные в таблице 2, в которой приводятся оценки относительной скорости передачи данных для криптосистем Мак-Элиса и Нидеррайтера при использовании кодов с параметрами из таблицы 1.

Таблица 2 – Относительная скорость передачи данных для различных крипто-кодовых схем с двоичными кодами Гоппы

Кодовые (n,k,d) параметры	(1 024, 524, 101)	(2 048, 1 300, 137)	(4 096, 2 584, 253)	(16 384, 10 322, 867)
Схема Мак-Элиса	≈ 0,51	≈ 0,63	≈ 0,63	≈ 0,63
Схема Нидеррайтера	≈ 0,57	≈ 0,57	≈ 0,53	≈ 0,48
Предлагаемая схема	≈ 0,79	≈ 0,84	≈ 0,83	≈ 0,81

Очевидно, что с увеличением длины кода Гоппы скорость (24), (25) для схемы Нидеррайтера снижается и не превосходит относительной скорости кодирования $R = k/n$. В авторской статье [16] в схеме Нидеррайтера предлагалось использовать обобщенные коды Рида-Соломона, их (n,k,d) параметры связаны соотношением $d = n - k + 1$, т.е. удовлетворяют верхней границе Синлгтона [38 – 40]. Тогда, например, для $q = 1024$ расширенный код Рида-Соломона будет иметь параметры (1 024, 524, 501) и оценка (24) дает относительную скорость для схемы Нидеррайтера $R^* \approx 0{,}66$, что на 30% выше по сравнению с $R \approx 0{,}51$ для схемы Мак-Элиса. Однако в работе [19] предложена эффективная атака на криптосистемы с обобщенными кодами Рида-Соломона, т.е. применение этого класса кодов несостоятельно. Таким образом, стойкие ко всем известным атакам криптосистемы Мак-Элиса и Нидеррайтера на двоичных кодах Гоппы сравнимы по относительной скорости передачи данных. Наибольшая стойкость обеспечивается для относительной скорости передачи данных 1/2 .. 2/3 и этот существенный недостаток частично снимается в предлагаемой ниже криптосистеме.

Предлагаемая криптосистема. По своей сути предлагаемая криптосистема является дальнейшим развитием схемы Мак-Элиса с дополнительным кодированием информационных данных по схеме Нидеррайтера. На рис. 2 схематично изображен процесс криптографического преобразования с использованием кодов:

– в схеме Мак-Элиса информация размещается в кодовом слове замаскированного кода. Зашифрование состоит в добавлении случайного вектора ошибок, который можно интерпретировать как сеансовый (одноразовый) ключ. Расшифрование состоит в декодировании кодового слова, т.е. снятия действия случайного вектора ошибок с кодового слова, содержащего информационную последовательность;

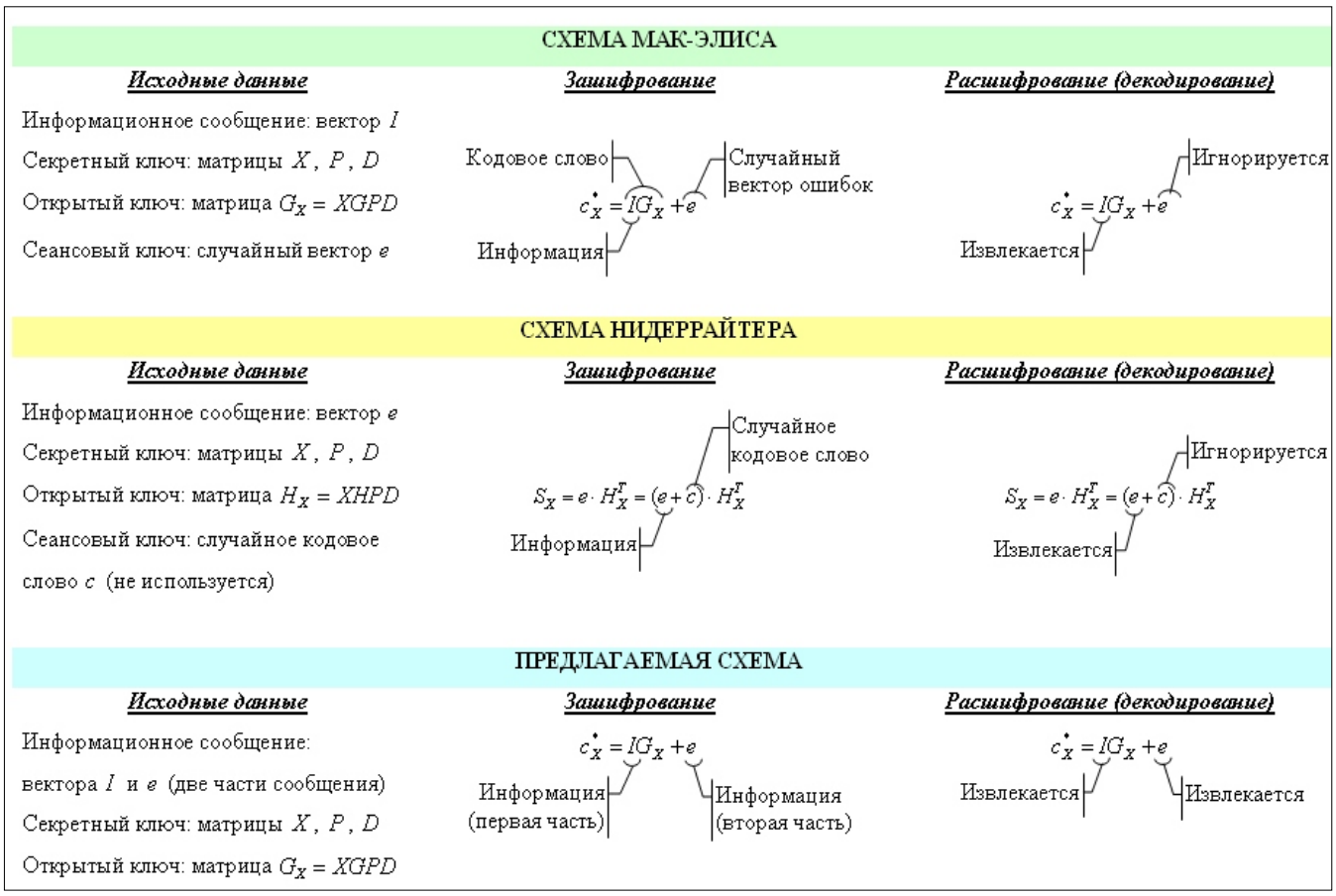

Рис. 2 – Криптографическое преобразование с использованием кодов

- в схеме Нидеррайтера информация размещается в векторе ошибок (посредством равновесного кодирования). По сформированному вектору ошибок вычисляется синдромная последовательность замаскированного кода, которая не зависит от кодового слова, т.е. к исходному вектору ошибок может быть добавлено произвольное кодовое слово (по умолчанию считается нулевым). Синдромный вектор позволяет однозначно декодировать это слово на приемной стороне, только теперь информация извлекается не из кодового слова, а из вектора ошибок;
- в предлагаемой схеме информационная последовательность разбивается на две части. Первая часть помещается в кодовое слово, вторая – в вектор ошибок (посредством равновесного кодирования). Для повышения стойкости эти две части могут быть дополнительно преобразованы (перемешаны, зашифрованы и т.д.). Дальше все преобразования выполняются как в схеме Мак-Элиса. Но на приемной стороне информация извлекается как из кодового слова (1-я часть), так и из вектора ошибок (2-я часть).

Таким образом, предлагаемая схема объединяет способы преобразования информационных данных схем Мак-Элиса и Нидеррайтера, что позволяет существенно повысить относительную скорость передачи данных. Зашифрование осуществляется по правилу (19), где I – первая информационная часть сообщения (как в схеме Мак-Элиса) и e – вторая часть информационного сообщения (как в схеме Нидеррайтера). Если предположить, что $w_h(e) = t$, тогда относительная скорость будет определяться выражением:

$$R^{**} = \frac{k + \left\lfloor \log_q \left((q-1)^t \frac{n!}{t!(n-t)!} \right) \right\rfloor}{n}, \qquad (28)$$

где в числителе первое слагаемое соответствует первой части информационных данных I, а второе слагаемое – второй части e.

Для случая $0 \le w(e) \le t$ выражение (28) перепишется в виде

$$R^{**} = \frac{k + \left\lfloor \log_q \left(\sum_{i=0}^{t} (q-1)^i \frac{n!}{i!(n-i)!} \right) \right\rfloor}{n}. \quad (29)$$

Для случая использования совершенных кодов выражение (29), как и (25), достигает максимума. Действительно, подставив (27) в (29) получим:

$$R^{**} = \frac{k+n-k}{n} = 1.$$

Кроме того, предлагаемая схема за счет информационного кодирования вектора e позволяет повысить относительную скорость и для несовершенных кодов. В качестве примера в таблице 2 приведены оценки относительной скорости передачи информации при использовании различных двоичных кодов Гоппы. Очевидно, что использование предлагаемой схемы шифрования увеличивает относительную скорость передачи данных на 30-40% по сравнению с лучшим показателем среди схем Мак-Элиса и Нидеррайтера.

4 Выводы

Несимметричные криптосистемы на основе алгебраических блоковых кодов были предложены около 40 лет назад и воспринимались тогда большинством исследователей как некое экзотическое и малоприменимое направление в криптографии. Очевидные недостатки (огромные объемы ключевых данных и снижение относительной скорости передачи) в течение длительного времени сдерживали их дальнейшее развитие и практическое использование. И только в последние годы, когда стало понятно, что многие существующие, стандартизированные и широко используемые на практике криптоалгоритмы могут оказаться беззащитными против атак квантового криптоанализа, кодовые криптосистемы получили заслуженное внимание исследователей. Декодирование случайного кода – чрезвычайно сложная вычислительная задача и переборный поиск при ее решении – вероятно лучшее из известных на сегодняшний день решение. Квантовые алгоритмы ускоряют этот процесс, что снижает временны*е* затраты криптоанализа, но это снижение не является критичным (примерно в два раза уменьшается эквивалентная длина ключа).

Фактически следует признать, что кодовые криптосистемы являются реальной альтернативой современных несимметричных криптосистем (RSA, ECC, или других) в части построения надежных постквантовых алгоритмов. Приведенные в таблице 1 расчеты наглядно подтверждают этот вывод. Кроме того, особенности построения кодовых схем позволяют одновременно с криптозащитой реализовать дополнительную услугу контроля возникающих ошибок, что, безусловно, представляет интерес для телекоммуникационных систем специального назначения.

Для практического применения кодовых криптосистем необходимо решить (или смирится с их существованием) несколько конструктивных проблем. Первая, и наиболее очевидная, - огромные объемы ключевых данных. В связи с возможностью использования квантовых вычислительных систем эти объемы придется значительно увеличить (примерно в четыре раза). Так например, для рассмотренных вариантов (таблица 1), объемы ключей достигают сотен мегабит и пока не представляется возможным их уменьшить без снижения стойкости криптосистемы. Ключи в кодовых схемах – это генераторные (порождающие и/или проверочные) матрицы линейного кода, которые должны выглядеть для злоумышленника как случайный набор линейнонезависимых векторов. Сжать или каким-то образом уменьшить этот набор не представляется возможным.

Вторая проблема – низкая относительная скорость передачи данных – в данной работе частично решена. Предложена новая схема шифрования, которая, фактически, объединяет известные способы кодирования информационных данных *(применяются в схемах Мак-Элиса и Нидеррайтера)*. В результате относительная скорость увеличивается, что повышает эффек-

тивность криптосистемы в целом. Если использовать эффективные *(в смысле дистанционных свойств)* коды, относительная скорость будет близка к 100%.

Даже для конструкций, которые лежат значительно ниже верхних кодовых границ наблюдается существенное (на 30-40%) повышение относительной скорости передачи данных (см. таблицу 2). По мнению авторов, это улучшение позволяет приступить к разработке конкретных протоколов криптографической защиты с использованием кодовых схем и начать их практическое внедрение.

Ссылки

[1] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography – CRC Press, 1997. – 794 p.
[2] Niels Ferguson and Bruce Schneier. Practical Cryptography. – John Wiley & Sons, 2003. – 432 pp.
[3] Arto Salomaa. Public-Key Cryptography, Second, Enlarged Edition. – Springer-Verlag, Berlin, Heidelberg, New York, 1996. – x+271 pp.
[4] Nigel Smart. Cryptography: An Introduction (3rd Edition). – 432 pp. https://www.cs.umd.edu/~waa/414-F11/IntroToCrypto.pdf
[5] David Deutsch and Richard Jozsa. Rapid solutions of problems by quantum computation. // Proceedings of The Royal Society of London A: Mathematical, Physical and Engineering Sciences, vol. 439, no. 1907. – 1992. – P. 553-558.
[6] Cleve R., Ekert A., Macchiavello C., Mosca M. Quantum algorithms revisited // Proceedings of The Royal Society of London A: Mathematical, Physical and Engineering Sciences, vol. 454, no. 1969. – 1998. – P. 339-354.
[7] Simon D. R. On the power of quantum computation // Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium. – P. 116-123.
[8] Grover L. A fast quantum mechanical algorithm for database search. // Proceedings of the 28th annual ACM symposium on the theory of computing (STOC, 96). ACM Press, New York. – 1996. – P. 212–219.
[9] Grover L. A framework for fast quantum mechanical algorithms. // Proceedings of the 13th annual ACM symposium on theory of computing (STOC' 98). ACM Press, New York. – 1998. – P. 53–62.
[10] Shor P. W. Algorithms for quantum computation: discrete logarithms and factoring // Foundations of Computer Science : Conference Publications. – 1994. – P. 124-134.
[11] Shor P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // Foundations of Computer Science: Conference Publications. – 1997. – P. 1484-1509.
[12] Neal Koblitz and Alfred J. Menezes. A Riddle Wrapped in an Enigma. https://eprint.iacr.org/2015/1018.pdf.
[13] Committee on National Security Systems, Use of public standards for the secure sharing of information among national security systems, Advisory Memorandum 02-15, July 2015. https://cryptome.org/2015/08/CNSS_Advisory_Memo_02-15.pdf.
[14] Bernstein, Daniel J., Buchmann, Johannes, and Dahmen, Erik. Post-Quantum Cryptography. – 2009, Springer-Verlag, Berlin-Heidleberg. – 245 p.
[15] McEliece R. J. A public-key cryptosystem based on algebraic coding theory. DSN Progress Report 42-44, Jet Propulsion Lab., Pasadena, CA, January-February, 1978. P. 114-116.
[16] Niederreiter H. Knapsack-type cryptosystems and algebraic coding theory // Problem Control and Inform Theory, 1986, v. 15. P. 19-34.
[17] T. R. N. Rao and K. H. Nam. Private-key algebraic-coded cryptosystem. Advances in Cryptology – CRYPTO 86, New York. – NY: Springer. – pp. 35–48.
[18] Yu. V. Stasev, A. A. Kuznetsov. Asymmetric Code-Theoretical Schemes Constructed with the Use of Algebraic Geometric Codes // Cybernetics and Systems Analysis, Volume 41, Issue 3, May 2005, Pages 354 – 363.
[19] Sidel'nikov V.M. Kriptografiya i teoriya kodirovaniya. Materialy konferentsii «Moskovskii universitet i razvitie kriptografii v Rossii», MGU. – 2002. – 22 s.
[20] Sidel'nikov V.M., Shestakov S.O. O sisteme shifrovaniya, postroennoi na osnove obobshchennykh kodov Rida-Solomona. // Diskretnaya matematika. – 1992. – T.4.№3. – S. 57-63.
[21] Kuznetsov A.A. Algebraicheskaya teoriya blokovykh kodov i ee prilozheniya v kriptografii // Persha mizhnarodni naukova konferencija 25–27 travnja 2005r. „Teorija ta metody obrobky sygnaliv". Tezy dopovidej. – K.: NAU. – 2005. – S. 6-8.
[22] Kuznetsov A.A. Issledovanie effektivnosti kriptosistem na algebraicheskikh blokovykh kodakh // Systemy obrobky informacii'. – Kharkiv: KhUPS. –2005 – Vyp. 4. – S. 202–206.
[23] Kuznetsov A.A. Issledovanie pomekhoustoichivosti i kriptostoikosti teoretiko-kodovykh skhem. // Modeljuvannja ta informacijni tehnologii'. – Kyi'v: NANU. – 2005. – №33. – S. 81-84.
[24] Fisher Jean-Dernard, Jacques Stern. An efficient Pseudo-Random Generator Provably as Secure as Syndrome Decoding / Jean-Dernard Fisher, Stern Jacques // EUROCRYPT'96 Proceeding, LNCS 1070. P. 245-255.
[25] Kuznetsov A.A., Korolev R.V., Ryabukha Yu.N. Usovershenstvovannyi metod bystrogo formirovaniya posledovatel'nostei psevdosluchainykh chisel // Zbirnyk naukovyh prac' HUPS. – Kharkiv: KhUPS. – 2008. – Vyp. 3 (18). – S. 101-104.
[26] Gaborit, P., Laudaroux, C., and Sendrier, N.: Synd: a very fast code-based cipher stream with a security reduction. In IEEE Conference, ISIT'07, pages 186–190.
[27] Kirill Morozov, Tsuyoshi Takagi. Zero-Knowledge Protocols for the McEliece Encryption // Information Security and Privacy Volume 7372 of the series Lecture Notes in Computer Science pp 180-193.
[28] Bernstein D. Post-quantum cryptography [Text] / D. Bernstein, J. Buchmann, E. Dahmen. – Berlin: Springer, 2009. – 246 p.
[29] Courtois, N., Finiasz M., Sendrier N.: How to achieve a McEliece-based digital signature scheme. In Advances in Cryptology - ASIACRYPT 2001, volume 2248, pages 157–174.
[30] Finiasz M.: Parallel-CFS: Strengthening the CFS McEliece-based signature scheme. In Biryukov A., Gong G., Stinson D., eds.: Selected Areas in Cryptography. Volume 6544 of LNCS., Springer (2010) pp. 159-170.
[31] Stern J.: A new identification scheme based on syndrome decoding. In Advances in Cryptology - CRYPTO'93, volume 773 of LNCS. Springer Verlag (1994).

[32] Veron P.: Improved identification schemes based on error-correcting codes. Appl. Algebra Eng. Commun. Comput., 8(1):57–69 (1996).
[33] Anne Canteaut and Nicolas Sendrier. Cryptanalysis of the original McEliece cryptosystem. In Kazuo Ohta and Dingyi Pei, editors, Advances in cryptology — ASIACRYPT'98, volume 1514 of Lecture Notes in Computer Science, pages 187– 199.
[34] Vladimir M. Sidelnikov and Sergey O. Shestakov. On insecurity of cryptosystems based on generalized Reed-Solomon codes. Discrete Mathematics and Applications, 1992. – P. 439–444.
[35] Minder L., Shokrollahi A. Cryptanalysis of the Sidelnikov Cryptosystem // Advances in Cryptology — EUROCRYPT 2007: 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Barcelona, Spain, May 20-24, 2007. Proceedings — Springer Berlin Heidelberg, 2007. – P. 347—360.
[36] Daniel J. Bernstein and Tanja Lange and Christiane Peters. Attacking and defending the McEliece cryptosystem. https://cr.yp.to/codes/mceliece-20080807.pdf.
[37] E. Berlekamp, R. McEliece, H. van Tilborg. On the Inherent Intractability of Certain Coding Problems. // IEEE Transactions on Information Theory, vol. IT-24, No. 3, May 1978. – P. 384-386.
[38] Clark G.C., Cain J.B. Error-Correction Coding for Digital Communications. – Springer, 1981, - 432 p.
[39] Blahut R. E. Theory and Practice of Error Control Codes. – Addison Wesley Publishing Company, Inc., Reading, Massachusetts, 1983, 1983, – 500 pp.
[40] F. J. MacWilliams and N. J. A. Sloane. The theory of error-correcting codes. – North-Holland, Amsterdam, New York, Oxford, 1977, – 762 pp.
[41] Claude E. Shannon. Communication in the Presence of Noise. Proceedings of the IRE, vol. 37, no. 1, pp. 10–21, Jan. 1949.
[42] V. D. Goppa. Novyi klass lineinykh korrektiruyushchikh kodov // Probl. peredachi inform., 1970, tom 6, vypusk 3, S. 24–30.
[43] V. D. Goppa. Na neprivodimykh kodakh dostigaetsya propusknaya sposobnost' DSK. // Probl. peredachi inform., 1974, tom 10, vypusk 1, S. 111–112.
[44] National Institute of Standards and Technology, "FIPS-197: Advanced Encryption Standard", November 2001: http://csrc.nist.gov/publications/ fips/fips197/fips-197.pdf.
[45] A New Encryption Standard of Ukraine: The Kalyna Block Cipher. https://eprint.iacr.org/2015/650.pdf.
[46] Raphael Overbeck, Nicolas Sendrier, Code-based cryptography. In: Daniel J. Bernstein, et al. (eds). First International Workshop on Post-quantum Cryptography, PQ Crypto 2006, Leuven, The Netherland, May 23-26, 2006. Selected papers, pp. 95-145.
[47] D. J. Bernstein. Grover vs. McEliece. In N. Sendrier, editor, Post-Quantum Cryptography, Third International Workshop, PQCrypto 2010, Darmstadt, Germany, May 25-28, 2010. Proceedings, volume 6061 of Lecture Notes in Computer Science, pages 73–80. Springer, 2010.
[48] A. Menezes, P. van Oorschot, S. Vanstone. Chapter 14. Efficient Implementation // Handbook of Applied Cryptography. – CRC-Press, 1996. – 816 p.
[49] Kerry Maletsky. RSA vs ECC Comparison for Embedded Systems. White Paper. Atmel Corporation – 2015, 5p. http://www.atmel.com/images/atmel-8951-cryptoauth-rsa-ecc-comparison-embedded-systems-whitepaper.pdf.
[50] John Proos and Christof Zalka. Shor's discrete logarithm quantum algorithm for elliptic curves. arxiv.quant-ph/0301141 v2, 2004.
[51] Ziatdinov M. Using frequency analysis and Grover's algorithm to implement known ciphertext attack on symmetric ciphers // Lobachevskii Journal of Mathematics 2013 vol.34 N4, pages 313-315.
[52] Metod nedvijkovogo rivnovagovogo koduvannja / V. B. Dudykevych, O. O. Kuznjecov, B. P. Tomashevs'kyj // Suchasnyj zahyst informacii'. - 2010. - № 3. - S. 57-68. - Rezhym dostupu: http://nbuv.gov.ua/UJRN/szi_2010_3_10.
[53] Tietavainen A., Perko A. There are no unknown perfect binary codes. - Annales Universitatis Turkuensis. - Ser. A, I 148, 3-10[6], 1971.
[54] Lint van J. H. Nonexistence theorems for perfect error-correcting codes. - Computers in Algebra and Number Theory. - Vol. IV [6], 1971.

Reviewer: Roman Oliynikov, Doctor of Sciences (Engineering), Full Professor, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: roliynykov@gmail.com

Received: August 2016.

Authors:
Alexandr Kuznetsov, Doctor of Sciences (Engineering), Full Prof., V.N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: kuznetsov@karazin.ua
Andriy Pushkar'ov, Director of department, State Service of Special Communication and Information Protection of Ukraine, Kyiv, Ukraine.
Sergii Kavun, Doctor of Sciences (Economics), Ph.D. (Engineering), Full Prof., Department of Information Technologies, Kharkiv Educational and Research Institute of the University of Banking, Kharkiv, Ukraine.
E-mail: kavserg@gmail.com
Vyacheslav Kalashnikov, Doctor of Sciences (Physics and Mathematics), Full Prof., Department of Systems and Industrial Engineering, Campus Monterrey, Monterrey, Mexico. E-mail: kalash@itesm.mx

Code-Based Public-Key Cryptosystems: the current state, the existing contradictions and prospects of practical use for the post-quantum period.

Abstract. Discusses the asymmetric cryptosystem based on algebraic coding, are investigated with temporary status, controversies and prospects of practical use for the post-quantum period. We propose a new scheme of crypto-transformation, significantly increases the relative rate of information transmission. Shown the advantage of the proposed design compared to the already known schemes Mac-Elisa and Niederreiter.

Keywords: Public-Key Cryptosystems, Post-Quantum Cryptography, Code-Based Cryptography.

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

Надійшло: Серпень 2016.

Автори:
Олександр Кузнецов, д.т.н., проф., академік Академії наук прикладної радіоелектроніки, Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: kuznetsov@karazin.ua
Андрій Пушкарьов, директор департаменту Державної служби спеціального зв'язку та захисту інформації України, Київ, Україна.
Сергій Кавун, доктор економічних наук, к.т.н., проф., Харківський навчально-науковий інститут ДВНЗ "Університет банківської справи", Харків, Україна.
E-mail: kavserg@gmail.com
В'ячеслав Калашников, д.ф.-м.н., проф., департамент систем і промислового виробництва Технологічного університету Монтеррея, Монтеррей, Мексика.
E-mail: kalash@itesm.mx

Несиметричні криптосистеми на основі алгебраїчного кодування: сучасний стан, наявні суперечності і перспективи практичного використання на пост-квантовий період.

Анотація. Розглядаються несиметричні криптосистеми на основі алгебраїчного кодування, досліджуються сучасний стан, наявні суперечності і перспективи практичного використання на пост-квантовий період. Пропонується нова схема криптоперетворення, яка істотно підвищує відносну швидкість передачі інформації. Показано перевагу запропонованої конструкції в порівнянні з вже відомими схемами Мак-Еліса та Нидеррайтера.

Ключові слова: несиметричні криптосистеми, пост-квантова криптографія, криптографія на основі кодів.

UDC 621.396

5G NETWORK ARCHITECTURE

O. Zamula, V. Morozov

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

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

Received on September 2016

Abstract. *The work deals with the main stages in the history of the development of different generations of cellular communication and options for the organization of their architecture. A brief overview of the main features and principles of construction of cellular networks of different generations. The analysis of the features and principles works of modern cellular networks of the fifth generation. Defined possibilities forward directions of modernization of existing cellular communication networks and opportunities to increase their potential.*

Keywords*: cellular network, 5G, MIMO, LTE, WiMAX.*

1 Introduction

Today wireless technology has a fixed position in our everyday life. In order to satisfy rising demand for high-speed wireless connection in near future, the wireless based networks of today will have to advance in various ways. Various current constituent technologies such as high-speed packet access (HSPA) and long-term evolution (LTE) will be used to develop future wireless based technologies. Nevertheless, auxiliary components may also constitute future new wireless based technologies, which may adjunct the evolved technologies. Ultra-dense deployments, direct device-to-device communication, different ways of accessing spectrum and considerably higher frequency ranges and instigation of massive antenna configurations these are all kinds of new technology components [1].

From analog voice calls to current technologies mobile wireless communication has come to high quality mobile broadband services with end-user data rates of several megabits per second over wide areas and tens to hundreds, of megabits per second locally. Evolution of various mobile devices such as smartphones and tablets and extensive improvements in terms of potentiality of mobile communication networks, have resultant exponential growth in network traffic. This paper tries to include a survey from 1G to 5G technologies and general 5G architecture.

We assume that in future there would be network with unbounded access to information and sharing of data which is accessible anytime and everywhere for everyone and everything. To make it true, new technology components need to be examined for the evolution of existing wireless based technologies. Present wireless based technologies, like Wi-Fi, LTE technology, HSPA and 3rd Generation Partnership Project will be incorporating new technology components that will be helping to meet the needs of the future. Nevertheless, there may be certain scenarios that cannot be adequately addressed along with the evolution of ongoing existing technologies. The instigation of completely new wireless based technologies will complement the current technologies which are needed for the long term realization of the future networks.

2 Evolution of wireless technologies

Wireless communications history starts with communicating the letter ‘S’ for 3 km in the form of three dot Morse code with the help of electromagnetic waves by Italian inventor G. Marconi. After this inception, wireless communications have become an important part of present day society. Since satellite communication, television and radio transmission has advanced to pervasive mobile

telephone, wireless communications has transformed the style in which society runs. The evolution of wireless technologies is shown in Fig. 1.

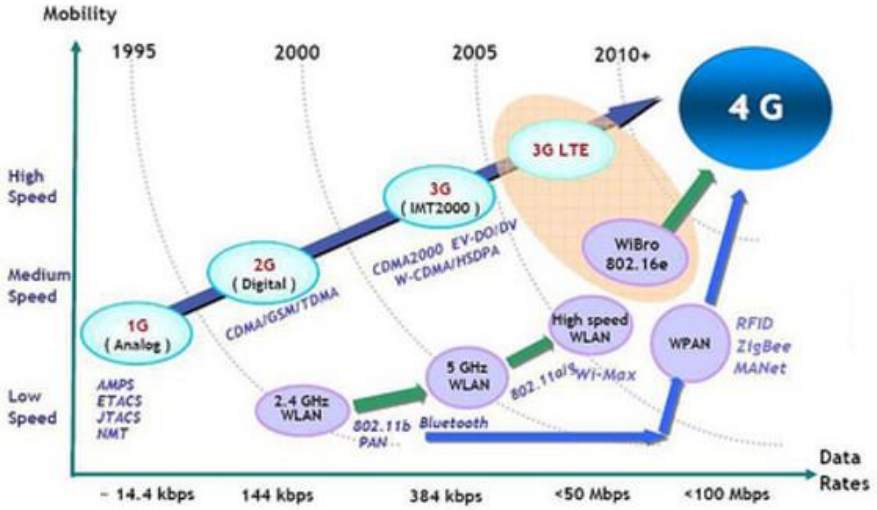

Figure 1 – Evolution of wireless technologies

It shows the evolving generations of wireless technologies in terms of data rate and mobility. With evolution of wireless technologies, the data rate, mobility, coverage and spectral efficiency increases. Technologies of 1G and 2G use circuit switching while 2.5G and 3G uses both circuit and packet switching and the next generations from 3.5G are using packet switching. Along with these factors, it also differentiate between licensed spectrum and unlicensed spectrum. All the evolving generations use the licensed spectrum while the Wi-Fi, Bluetooth and WiMAX are using the unlicensed spectrum. An overview about the evolving wireless technologies is below.

The 1st generation was announced in initial 1980's and has a data rate up to 2.4kbps. Major subscribers were Advanced Mobile Phone System, Nordic Mobile Telephone, and Total Access Communication System. It has a lot of disadvantages like below par capacity, reckless handoff, inferior voice associations, and with no security, since voice calls were stored and played in radio towers due to which vulnerability of these calls from unwanted eavesdropping by third party increases [4].

The 2nd generation was introduced in late 1990's. Digital technology is used in 2nd generation mobile telephones. Global Systems for Mobile communications (GSM) was the first 2nd generation system used for voice communication and having a data rate up to 64kbps. 2G mobile handset battery lasts longer because of the radio signals having low power. It also provides services like Short Message Service and e-mail. Vital eminent technologies were GSM, Code Division Multiple Access (CDMA), and IS-95 [4].

The 2.5G generation generally subscribes a 2nd generation cellular system merged with General Packet Radio Services (GPRS) and other amenities doesn't commonly endow in 2G or 1G networks. A 2.5G system generally uses 2G system frameworks, but it applies packet switching along with circuit switching and has a data rate up to 144kbps. The main 2.5G technologies were GPRS, Enhanced Data Rate for GSM Evolution (EDGE), and CDMA 2000 [4].

The 3G generation was established in late 2000 and imparts transmission rate up to 2Mbps. Third generation systems merge high speed mobile access to services based on Internet Protocol (IP). Aside from transmission rate, unconventional improvement was made for maintaining quality of service. Additional amenities like global roaming and improved voice quality made 3G as a remarkable generation. The major disadvantage for 3G handsets is that, they require more power than most 2G models. Along with this 3G network plans are more expensive than 2G [4]. Since 3G involves the introduction and utilization of Wideband CDMA, Universal Mobile Telecommunications Systems and CDMA 2000 technologies, the evolving technologies like High Speed Uplink/Downlink Packet Access and Evolution-Data Optimized has made an intermediate wireless generation between 3G and 4G named as 3.5G with improved data rate of 5-30 Mbps.

LTE technology and Fixed Worldwide Interoperability for Microwave Access (WiMAX) is the future of mobile data services. LTE and Fixed WiMAX has the potential to supplement the capacity of the network and provides a substantial number of users the facility to access a broad range of high speed services like on demand video, peer to peer file sharing and composite Web services. Along with this, a supplementary spectrum is accessible which accredit operators manage their network very compliantly and offers better coverage with improved performance for less cost [3-4].

4G is generally referred as the descendant of the 3G and 2G standards. 3rd Generation Partnership Project is presently standardizing LTE Advanced as forthcoming 4G standard along with WiMAX. A 4G system improves the prevailing communication networks by imparting a complete and reliable solution based on IP. Features like voice, data and multimedia will be imparted to subscribers on anytime and everywhere basis and at quite higher data rates as related to earlier generations. Applications that are being made to use a 4G network are Multimedia Messaging Service, Digital Video Broadcasting, and video chat, High Definition TV content and mobile TV [2-3].

With an exponential increasing users demand, 4G will be replaced with 5G with an advanced access technology named Non- and quasi-orthogonal or filter bank multi carrier multiple access and Beam Division Multiple Access (BDMA). BDMA technique concept is explained by considering the case of the base station communicating with the mobile stations. In this communication, an orthogonal beam is allocated to each mobile station and BDMA technique will divide that antenna beam according to locations of the mobile stations for giving multiple accesses to the mobile stations, which correspondingly increase the capacity of the system [5]. Incentives to move towards 5G is based on current drifts, it is commonly assumed that 5G cellular networks must eliminate six weaknesses of 4G i.e. higher capacity, higher data rate, lower End-to-End latency, massive device connectivity, reduced cost and consistent quality of experience provisioning. These challenges are concisely shown in Fig. 2 along with some potential facilitators to address them. An overview of the challenges, facilitators, and corresponding design fundamentals for 5G is shown in Fig. 2 [8].

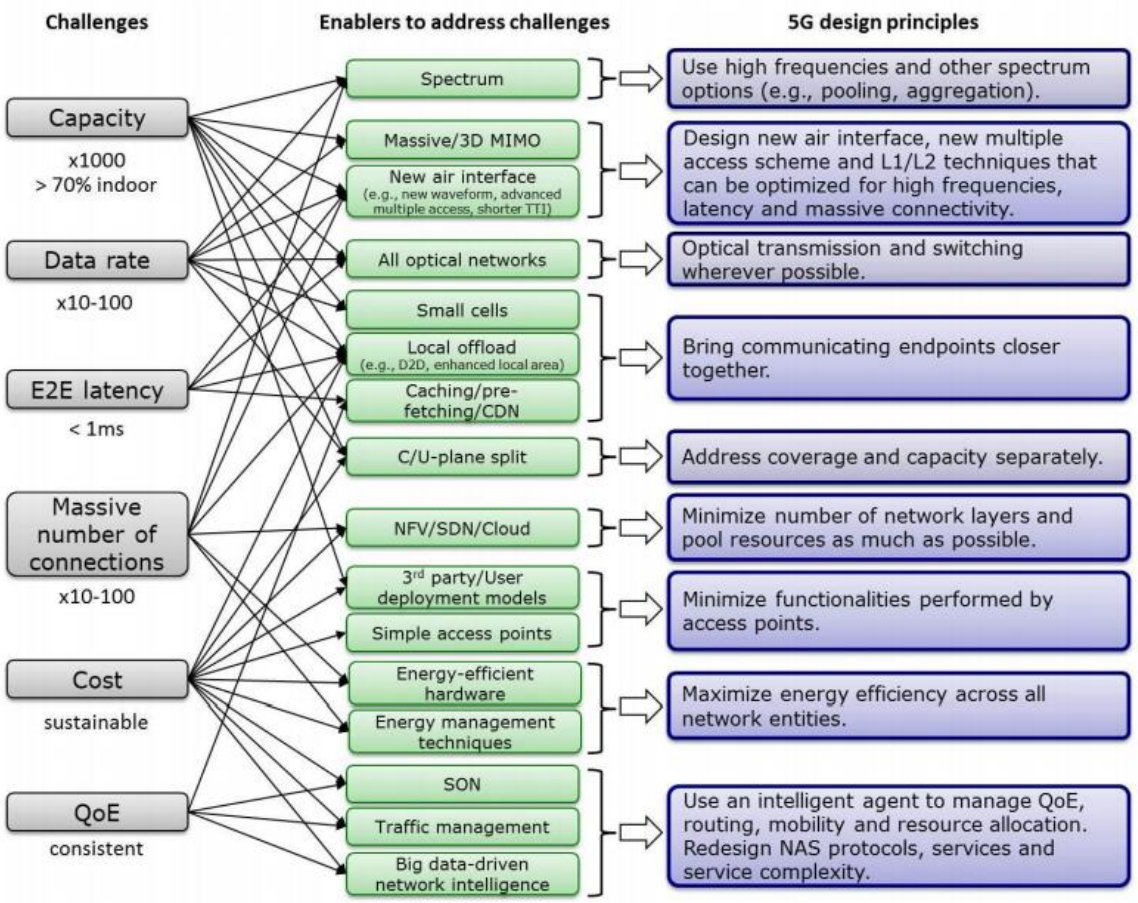

Figure 2 – 5G challenges, potential enablers and design principles

3 5G cellular network architecture

Before the demonstration 5G technology to end user it is necessary to modernize the existing basis. Current technologies like OFDMA will work at least for next 50 years, so there is no need to change wireless setup which had come about from 1G to 4G. In order to please user requirements, we could only complement existing fundamental network. This will provoke the package providers to drift for a 5G network as early as 4G is commercially set up [5]. We have to make drastic changes in the strategy of designing the 5G wireless cellular architecture, to meet the users demands and to overcome challenges that has been put forward in the 5G system. A general researchers' observation has shown that most of the wireless users stay inside for 80 % and outside 20 % of time [6]. In present wireless cellular architecture we have an outside base station in the middle of a cell, that allows a mobile user to communicate. While users inside, the signals from outside base station will have to travel through the walls, and this will result in high penetration loss, which correspondingly costs with reduced spectral efficiency, data rate and energy efficiency of wireless communications. To overcome this challenge there was proposed a new designing technique for scheming the 5G cellular architecture [5]. With this designing technique, the penetration loss through the walls of the building will be slightly reduced. This idea will be supported with the help of massive MIMO technology, in which geographically dispersed array of antenna's are deployed which have tens or hundreds of antenna units.

To build or construct a large massive MIMO network, firstly the outside base stations will be fitted with large antenna arrays and among them some are dispersed around the hexagonal cell and linked to the base station through optical fiber cables, aided with massive MIMO technologies. The mobile users present outside are usually fitted with a certain number of antenna units but with cooperation a large virtual antenna array can be constructed, which together with antenna arrays of base station form virtual massive MIMO links. Secondly, every building will be installed with large antenna arrays from outside, to communicate with outdoor base stations with the help of line of sight components. The wireless access points inside the building are connected with the large antenna arrays through cables for communicating with indoor users. This will significantly improves the energy efficiency, cell average throughput, data rate, and spectral efficiency of the cellular system but at the expense of increased infrastructure cost. With the introduction of such an architecture, the inside users will only have to connect or communicate with inside wireless access points while larger antenna arrays remained installed outside the buildings [5]. For indoor communication, certain technologies like Wi-Fi, Small cell, ultra wideband, millimeter wave communications, and visible light communications are useful for small range communications having large data rates [6]. But technologies like millimeter wave and visible light communication are utilizing higher frequencies which are not conventionally used for cellular communications. But it is not an efficient idea to use these high frequency waves for outside and long distance applications because these waves. Technical comparison between recent 802.11 standards. will not infiltrate from dense materials efficiently and can easily be dispersed by rain droplets, gases, and flora. Though, millimeter waves and visible light communications technologies can enhance the transmission data rate for indoor setups because they have come up with large bandwidth. Along with the introduction of new spectrum, which is not being conventionally used for wireless communication, there is one more method to solve the spectrum shortage problem by improving the spectrum utilization of current radio spectra through cognitive radio (CR) networks [6].

Since the 5G cellular architecture is heterogeneous, so it must include relays, macro-, micro- and small cells. A mobile small cell concept is an integral part of 5G wireless cellular network and partially comprises of mobile relay and small cell concepts [7]. It is being introduced to put up high mobility users, which are inside the automobiles and high speed trains. Mobile small cells are positioned inside the moving automobiles to communicate with the users inside the automobile, while the massive MIMO unit consisting of large antenna arrays is placed outside the automobile to communicate with the outside base station. According to user's opinion, a mobile small cell is realized as a regular base station and its allied users are all observed as a single unit to the base station which proves the above idea of splitting indoor and outdoor setups. Mobile small cell users [7] have

a high data rate for data rate services with considerably reduced signaling overhead, as shown in [5]. As the 5G wireless cellular network architecture consists of only two logical layers: a radio network and a network cloud. Different types of components performing different functions are constituting the radio network. The network function virtualization cloud consists of User and Control plane entities that perform higher layer functionalities related to the User and Control plane, respectively. Special network functionality as a service (XaaS) will provide service as per need, resource pooling is one of the examples. XaaS is the connection between a radio network and a network cloud [8].

The 5G cellular network architecture is explained in [5,8]. It has equal importance in terms of front end and backhaul network respectively. In this paper, a general 5G cellular network architecture has been proposed as shown in Fig. 3. It describes the interconnectivity among the different emerging technologies like Massive MIMO network, Cognitive Radio network, mobile and static small-cell networks. This proposed architecture also explains the role of network function virtualization cloud in the 5G cellular network architecture. The concept of Device-to-Device communication, small cell access points and Internet of things has also been incorporated in this proposed 5G cellular network architecture. In general, this proposed 5G cellular network architecture may provide a good platform for future 5G standardization network.

Figure 3 illustrates a 5G mobile network architecture that utilizes the enablers discussed previously [8]. The key elements in the architecture are summarized below.

- Two logical network layers, namely a radio network (RN) that provides only a minimum set of L1/L2 functionalities and a network cloud that provides all higher layer functionalities.
- Dynamic deployment and scaling of functions in the network cloud through SDN and NFV.
- Lean protocol stack achieved through elimination of redundant functionalities and integration of AS and NAS.
- Separate provisioning of coverage and capacity in the RN by use of C/U-plane split architecture and different frequency bands for coverage and capacity.
- Relaying and nesting (connecting devices with limited resources non-transparently to the network through one or more devices that have more resources) to support multiple devices, group mobility and nomadic hotspots.
- Connectionless and contention-based access with new waveforms for asynchronous access of massive number of MTC devices.
- Data-driven network intelligence to optimize network resource usage and planning.

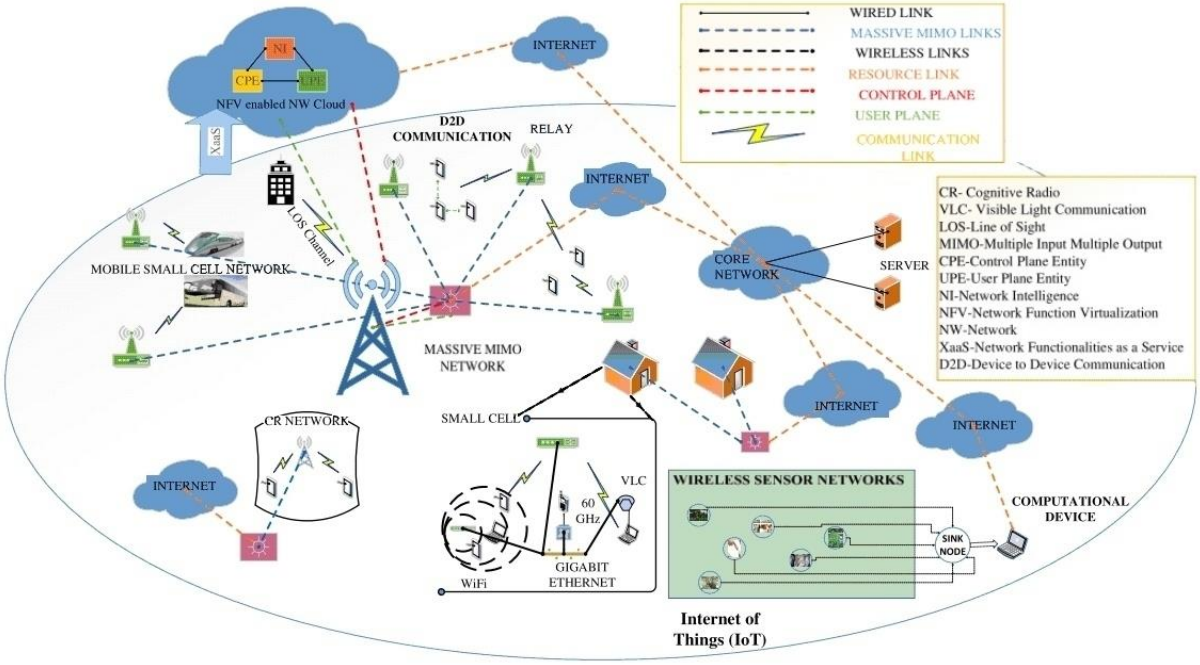

Figure 3 – A general 5G cellular network architecture

4 Conclusions

The modern world needs everything recently developed especially in terms of technologies also. First generation starts in the year of 1980s but now it seems to be older than a century because of its speed. From there onwards a new step or ladder is leaned as proportional to speed and year. In this paper, a detailed survey has been done on the generations history of cellular networks, network architecture and performance requirements for 5G wireless cellular communication systems that have been defined in terms of capacity, data rate, spectral efficiency, latency, energy efficiency, and quality of service. A 5G wireless has been explained in this paper with massive MIMO technology, network function virtualization cloud and device to device communication. This paper may be giving a good platform to motivate the researchers for better outcome of different types of problems in next generation networks.

References

[1] Baldemair R. Evolving wireless communications: Addressing the challenges and expectations of the future / Baldemair. // IEEE Veh. Technol. Mag. – №8. – pp. 24–30.
[2] Rappaport T. Wireless Communications: Principles and Practice (2nd Edition) / Theodore Rappaport. – NY: Prentice-Hall, 2002. – 736 p.
[3] Andrews J. Fundamentals of WiMAX / J. Andrews, A. Ghosh, R. Muhamed. – NY: Prentice-Hall, 2007. – 496 p.
[4] Goals of true broad band's wireless next wave (4G–5G) / K. Santhi, V. Srivastava, G. Senthil-Kumaran, A. Butare. // Proc. IEEE 58th Veh. Technol. Conf.. – 2003. – №4. – pp. 2317–2321.
[5] Cellular architecture and key technologies for 5G wireless communication networks / [C. Wang, F. Haider, G. Xiqi et. al.]. // IEEE Commun. Mag.. – 2014. – №52. – pp. 122–130.
[6] Gupta A. A Survey of 5G Network: Architecture and Emerging Technologies / A. Gupta, R. Jha. // IEEE Access. – 2015. – №3. – pp. 1206–1232.
[7] Spectral efficiency analysis of mobile Femtocell based cellular systems / [F. Haider, C. Wang, H. Haas et al.]. // Proc. IEEE ICCT. – 2011. – pp. 347–351.
[8] Design considerations for a 5G network architecture / [P. Agyapong, M. Iwamura, D. Staehle et al]. // IEEE Commun. Mag.. – 2014. – №552. – pp. 65–75.

Рецензент: Олександр Потій, д.т.н., проф., Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: potav@ua.fm

Надійшло: Вересень 2016.

Автори:
Олександр Замула, д.т.н., доцент, Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: zamylaaa@gmail.com
Владислав Морозов, аспірант, Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: morozov@boiko.com.ua

Мережева архітектура п'ятого покоління.

Анотація. Робота присвячена розгляду основних етапів в історії розвитку різних поколінь стільникового зв'язку та варіантів організації їх архітектури. Виконано короткий огляд основних особливостей функціонування і принципів організації мереж стільникового зв'язку різного покоління. Проведено аналіз можливостей та принципів побудови сучасних стільникових мереж п'ятого покоління. Окреслено перспективні напрями модернізації існуючих мереж стільникового зв'язку та визначено можливості нарощування їх потенційних можливостей.

Ключові слова: стільниковий зв'язок, 5G, MIMO, LTE, WiMAX.

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

Поступила: Сентябрь 2016.

Авторы:
Александр Замула, д.т.н., доцент, Харьковский национальный университет имени В. Н. Каразина, Харьков, Украина.

E-mail: zamylaaa@gmail.com

Владислав Морозов, аспирант, Харьковский национальный университет имени В. Н. Каразина, Харьков, Украина.
E-mail: morozov@boiko.com.ua

Сетевая архитектура пятого поколения.

Аннотация. Работа посвящена рассмотрению основных этапов в истории развития различных поколений сотовой связи и вариантов организации их архитектуры. Выполнен краткий обзор основных особенностей функционирования и принципов организации сетей сотовой связи различного поколения. Проведен анализ возможностей и принципов построения современных сотовых сетей пятого поколения. Обозначены перспективные направления модернизации существующих сетей сотовой связи и определены возможности наращивания их потенциальных возможностей.

Ключевые слова: сотовая связь, 5G, MIMO, LTE, WiMAX.

УДК 621.37:621.391

ИССЛЕДОВАНИЕ ГЕОМЕТРИИ РАЗМЕЩЕНИЯ ТОЧЕК ПСЕВДОСЛУЧАЙНЫХ КОДОВ В ЕВКЛИДОВОМ ПРОСТРАНСТВЕ

Тамила Лавровская

Харьковский национальный университет имени В.Н. Каразина, площадь Свободы, 4, г. Харьков, 61022, Украина
lavrovska92@gmail.com

Рецензент: Виктор Краснобаев, д.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, площадь Свободы, 4, г. Харьков, 61022, Украина.
krasnobaev@karazin.ua

Поступила в сентябре 2016

Аннотация. *Проведен анализ причин кризиса помехоустойчивого кодирования. Обоснована перспективность применения псевдослучайных кодов и разработана их математическая модель. Рассмотрены сравнительные вероятностные характеристики равномерных и нормальных случайных кодов. Проведена оценка свойств простейших равномерных псевдослучайных кодов, полученных методом линейной конгруэнтной генерации. Предложены рекомендации по выбору параметров линейных конгруэнтных генераторов кодовых символов.*

Ключевые слова: *кодирование, псевдослучайные коды, евклидово пространство кода, статистические модели процесса декодирования.*

1 Введение

В теории систем передачи информации известна историческая роль методологии, основанной на использовании случайно выбираемых кодов, в доказательстве фундаментальных теорем для зашумленных каналов [1,2]. Однако, доказательства на основе случайного выбора кода обычно называются неконструктивными, поскольку до сих пор ни одна попытка разработки конкретных кодов и методов их обработки не увенчалась успехом. Основная причина этого заключается в отсутствии вычислительно реализуемых методов построения псевдослучайных кодов, а также методов их декодирования.

В теории систем передачи информации известна историческая роль методологии, основанной на использовании случайно выбираемых кодов, в доказательстве фундаментальных теорем для зашумленных каналов [1,2]. Однако, доказательства на основе случайного выбора кода обычно называются неконструктивными, поскольку до сих пор ни одна попытка разработки конкретных кодов и методов их обработки не увенчалась успехом. Основная причина этого заключается в отсутствии вычислительно реализуемых методов построения псевдослучайных кодов, а также методов их декодирования.

Постановки проблем и постулирование важнейших положений теории информации дали толчок для поиска решения задач с использованием исключительно детерминированных (неслучайных) сигналов и алгебраических методов канального кодирования [3]. В этой области достигнуты серьезные результаты, имеющие важное теоретическое значение. Математический прогресс привел к кризису практики – объем фундаментальных исследований явно превышает требуемые прикладные потребности и является несопоставимым с недостаточным, на наш взгляд, приращением показателей удельной эффективности систем передачи информации (СПИ). Основной причиной этого является почти эквивалентный обмен приращения энергетической эффективности на проигрыш в частотной эффективности, характерный для систем с комбинаторным алгебраическим кодированием.

Перспективным направлением развития теории построения кодов следует считать исследование методов псевдослучайного кодирования (модуляции), которые приближают статистические характеристики канальных сигнально-кодовых конструкций к характеристикам реализаций шумовых последовательностей.

2 Анализ существующих результатов

Основным результатом, который дает объективные предпосылки для развития технологий случайного кодирования, является трактовка Шеннона физической сущности пропускной способности непрерывного канала *C* при ограничении средней мощности передатчика *P*. Процесс приближения к пропускной способности в этих условиях описывается следующим образом [1]. «… Пусть созданы $M=2^k$ выборок белого шума, каждая длительности *T*. Им приписываются двоичные числа от 0 до *(M-1)*. В передатчике последовательности сообщений разбиваются на группы по k двоичных знаков и для каждой группы в качестве сигнала передается соответствующая выборка шума. Приемнику эти *M* выборок известны, и принятый искаженный шумом сигнал сравнивается с каждой из них. Выборка, которая имеет наименьшее среднеквадратичное расстояние от принятого зашумленного сигнала, принимается за переданный сигнал, по которому восстанавливается соответствующее двоичное число. Этот прием эквивалентен выбору наиболее вероятного (апостериори) сигнала. Число используемых выборок шума *M* будет зависеть от допустимой частоты ошибок *p*, но для почти всех наборов выборок имеем

$$\lim_{\mathrm{p}\to 0}\lim_{\mathrm{T}\to\infty}\frac{\log \mathrm{M}(\mathrm{p},\mathrm{T})}{\mathrm{T}} = \mathrm{F}\log\frac{\mathrm{P}+\mathrm{N}}{\mathrm{N}}, \quad (1)$$

(где F – полоса частот канала, N – спектральная плотность мощности аддитивного шума). Таким образом, независимо от того, насколько малым выбрано p, можно, выбирая T достаточно большим, приблизиться сколь угодно близко к передаче $TF\log\frac{P+N}{N}$ двоичных единиц за время T…». Фактически, данное описание соответствует процессу декодирования случайно выбранного кода по правилу максимального правдоподобия [3], а пропускная способность – это предельно достижимая скорость передачи информации при помощи использования лучшего кода. Следовательно, лучшим является код, полученный как математическое ожидание по ансамблю случайно выбираемых кодов.

В работах [4] и [5] разработаны элементы теории, способной придать идеям случайного кодирования определенный конструктивизм за счет применения эвристических методов коррекции свойств кодовых книг случайных кодов. Однако, этого недостаточно для разработки робастных алгоритмов кодирования и, особенно, декодирования таких кодов. Поскольку вычислительно реализуемыми алгоритмами декодирования *(со сложностью не выше полиномиальной от длины блока)* могут быть только алгоритмы декодирования кодов, построенных с использованием детерминированных методов генерации кодовых слов, речь может идти исключительно о «псевдослучайном» кодировании. При определенных условиях такие коды могут приближаться по своим вероятностным характеристикам декодирования к случайным кодам, допуская при этом возможность разработки алгебраических алгоритмов декодирования.

Основными причинами, сдерживающими практическую реализацию псевдослучайных кодов (ПСК), являются: во-первых, отсутствие формализованного математического аппарата получения кодов с хорошими корректирующими свойствами, а, во-вторых, – отсутствие практических способов не переборного декодирования. В работе [6] обоснована перспективность простейшего алгебраического метода генерации равномерных кодов, основанного на методе линейной конгруэнтной генерации, однако не получены рекомендации по выбору параметров генераторов. Кроме того, рассмотренный в работе [6] метод декодирования на основе решения задачи целочисленного линейного программирования по методу отсекающих плоскостей Гомори, оказался нестойким к зацикливанию, что явилось причиной отсутствия возможности гарантированного получения решения. Указанные причины не позволяют применять метод для практически требуемых значений длин блоков кодовых слов.

Целью статьи является разработка математической модели случайных и псевдослучайных кодов для проведения анализа и обоснования требований к методу получения кодовых книг, а также к числовым параметрам линейной конгруэнтной генерации. А так же разработка статистических моделей для оценки вероятностных свойств случайных и псевдослучайных кодов.

3 Математическая модель и пространственная структура случайных кодов

Процедура получения кодовой книги произвольного случайного кода может быть представлена следующим образом. Пусть кодированию подлежит последовательность двоичных символов, разбитая на блоки длиной *k* бит. Каждому из блоков может быть сопоставлено целое число, обозначающее условный лексикографический номер комбинации двоичных символов. Таким образом, все возможные сообщения источника оказываются пронумерованными числами *i* из диапазона от 0 до $M=2^k$. Кодовая книга случайного кода *Kb* формируется, как набор векторов:

$$\mathrm{Kb}=\left\{\overrightarrow{\mathrm{kb_i}}\right\},\ \mathrm{i}\in\left[0,\left(\mathrm{M}-1\right)\right];$$
$$\overrightarrow{\mathrm{kb_i}}=\left\{\underbrace{\mathrm{x_0}^{\mathrm{i}},\mathrm{x_1}^{\mathrm{i}},\ldots,\mathrm{x_{n-1}}^{\mathrm{i}}}_{\mathrm{n}}\right\}, \tag{2}$$

где: – n – длина блока кода; – x_k^i, $\left\{i\in\left[0,\left(M-1\right)\right];k\in\left[0,\left(n-1\right)\right]\right\}$ – независимые, одинаково распределенные случайные величины с функцией плотности распределения вероятностей *f(x)* и нулевым средним $m_x=0$.

Обозначим $R=K\backslash n$ – скорость кода *(может быть как больше, так и меньше единицы)*. Дисперсия σ_x^2 распределения *f(x)* при кодировании информативных параметров сигналов в канале определяется выражением:

$$\sigma_{\mathrm{x}}{}^2=\alpha\cdot\mathrm{R}\cdot\mathrm{P}, \tag{3}$$

где: P – бюджет мощности, выделенный на передачу одного бита сообщения источника; α – коэффициент, зависящий от вида модуляции в канале.

Выбор распределения *f(x)* определяет тип укладки точек кодовых слов случайного кода в n - мерном евклидовом пространстве. Если функция *f(x)* непрерывна в некотором диапазоне *x*, то укладка объемная; если *f(x)* отлична от нуля только на некотором конечном множестве значений *x*, то укладка поверхностная. Поскольку поверхностное расположение точек в многомерном пространстве является частным (вырожденным) случаем объемной укладки, то для получения лучших характеристик кодовых книг следует использовать непрерывные функции распределения *f(x)*.

Ключевым вопросом построения случайного кода является выбор геометрии подпространства кода в n - мерном пространстве. Эта геометрия полностью определяется видом непрерывного распределения *f(x)*. Имеет смысл, без какого-либо снижения общности, рассмотреть всего лишь два варианта: нормальное *(гауссово)* и равномерное в заданном диапазоне распределения символов кодовых слов x_k^i.

Нормальный случайный код. Обозначим кодовую книгу (набор из *M* векторов) нормального кода, как $Kbn=\left\{\overrightarrow{kbn_i}\right\}$. Символы кодовых слов векторов $\overrightarrow{kbn_i}$ независимы и распределены по закону:

$$\mathrm{f_n}\left(\mathrm{x}\right)=\left(2\pi\sigma_{\mathrm{x}}{}^2\right)^{-\frac{1}{2}}\exp\left(\frac{\mathrm{x}^2}{2\sigma_{\mathrm{x}}{}^2}\right). \tag{4}$$

Поскольку при построении модели для статистических испытаний и использовании программных датчиков случайных чисел средняя по реализации ансамбля кодовых слов мощ-

ность (дисперсия) символов может оказаться отличной от требуемого значения, определяемого выражением (3), имеет смысл проведение нормировки кодовой книги:

$$\overline{\mathrm{Kbn}} = \mathrm{Kbn} \cdot \left\{ \frac{\alpha \mathrm{RP}}{\mathrm{M}} \sum_{\mathrm{m}=0}^{\mathrm{M}-1} \frac{\left| \overrightarrow{\mathrm{kbn}_{\mathrm{m}}} \right|^2}{\mathrm{n}} \right\}^{-\frac{1}{2}}. \tag{5}$$

Выполнение (5) гарантирует фиксированную среднюю мощность (3), приходящуюся на один символ каждого из M равновероятных кодовых слов нормального случайно выбранного кода. Использование гауссова распределения (4) при $\mathrm{n} \to \infty$ обеспечивает формирование кода объемно-сферической укладки: кодовые точки асимптотически располагаются внутри гиперсферы с центром в начале координат и радиусом $r = \sqrt{n\sigma_x^2}$.

На рис. 1 приведен вид сечения подпространства нормального случайного кода с кодовой книгой, определяемой (4), (5) произвольной плоскостью, проходящей через центр гиперсферы. При этом приняты значения

$$\mathrm{P} = \alpha = \mathrm{R} = 1, \mathrm{n} = 12. \tag{6}$$

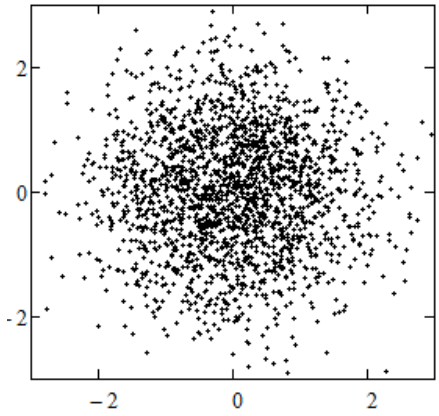

Рис. 1 – Плоскостное сечение подпространства нормального случайного кода

Ввиду особенностей геометрии подпространства кодовой книги нормальный случайный код можно называть *гиперсферическим кодом*.

Равномерный случайный код. Используем обозначение $Kbu = \left\{ \overrightarrow{kbu_i} \right\}$ для кодовой книги кода с равномерным распределением символов слов. Функция плотности распределения вероятностей символов кодовых слов имеет вид:

$$\mathrm{f_u}(\mathrm{x}) = \begin{cases} \dfrac{1}{2\sqrt{3\sigma_{\mathrm{x}}{}^2}}, & \text{при } |\mathrm{x}| \le \sqrt{3\sigma_{\mathrm{x}}{}^2}; \\ 0 \quad \text{в остальных случаях.} \end{cases} \tag{7}$$

Условие нормировки случайно выбранного кода:

$$\overline{\mathrm{Kbu}} = \mathrm{Kbu} \cdot \left\{ \frac{\alpha \mathrm{RP}}{\mathrm{M}} \sum_{\mathrm{m}=0}^{\mathrm{M}-1} \frac{\left| \overrightarrow{\mathrm{kbu}_{\mathrm{m}}} \right|^2}{\mathrm{n}} \right\}^{-\frac{1}{2}}. \tag{8}$$

Точки кодовых слов равномерного случайного кода располагаются внутри n -мерного гиперкуба с размером ребра, равным $r = 2\sqrt{3\sigma_x^2}$. Сечение подпространства кода произвольной

плоскостью, проходящей через пару координатных осей n мерного пространства при фиксированных условиях (6) показано на рис. 2.

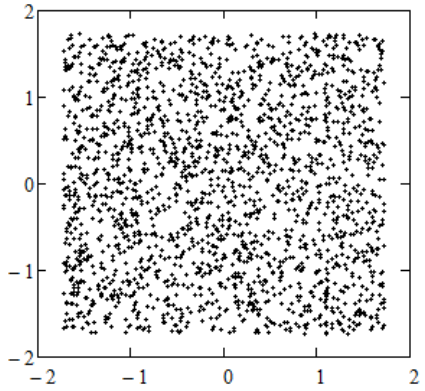

Рис. 2 – Плоскостное сечение подпространства равномерного случайного кода

Расположение точек кодовых слов равномерного случайного кода делает возможным применение для него названия *гиперкубический код*.

4 Статистическая модель для исследования вероятностных свойств случайных кодов

Объективной характеристикой помехоустойчивости случайных кодов является величина вероятности ошибки при декодировании, приведенная к блоку кода при заданном отношении сигнал/шум. Ввиду объективной невозможности аналитической оценки вероятностных характеристик случайно выбираемых кодов, единственным способом определения предпочтения между гиперсферическим и гиперкубическим кодами является их статистическое исследование. Структура статистической модели для исследования вероятностных свойств случайных кодов в гауссовом канале приведена на рис. 3.

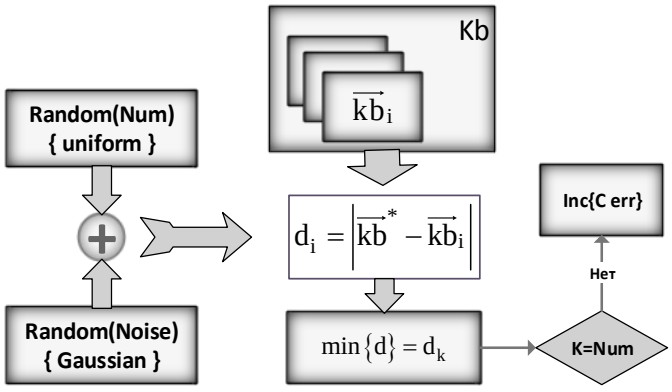

Рис. 3 – Структура одного цикла статистической модели

На каждом цикле испытаний модели производится равномерно случайный выбор номера *Num* одного из M кодовых слов $\overrightarrow{kbn_{Num}}$ или $\overrightarrow{kbu_{Num}}$, вектор которого складывается с вектором гауссовой помехи, $Random\{Noise\}$ обладающей мощностью, вычисляемой при заданном отношении сигнал/шум *h*. Затем, методом последовательного перебора вычисляются элементы массива взаимных расстояний d_i, $i \in [0,(M-1)]$ между искаженным кодовым словом и всеми словами кодовой книги. За истинный номер принимается номер кодового слова, ближайшего к анализируемому и соответствующего минимальному расстоянию d_k. В случае, если найденный номер ближайшего слова не совпадает с величиной *Num*, произво-

дится инкрементация счетчика ошибок *Cerr*. Реализуемый алгоритм соответствует декодированию по правилу максимального правдоподобия. Количество циклов испытаний подбирается, исходя из требуемой точности оценки и величины задаваемого отношения сигнал/шум. После проведения серии из K испытаний вероятность ошибки вычисляется отношением p = Cerr/K.

На рис. 4 представлены результаты статистического моделирования гиперсферического и гиперкубического кодов в равных энергетических условиях при трех различных отношениях сигнал/шум h=2,3,4. Вероятности декодирования с ошибкой p представлены, как функции длины блока случайных кодов *n* при фиксированной скорости кодирования R=1.

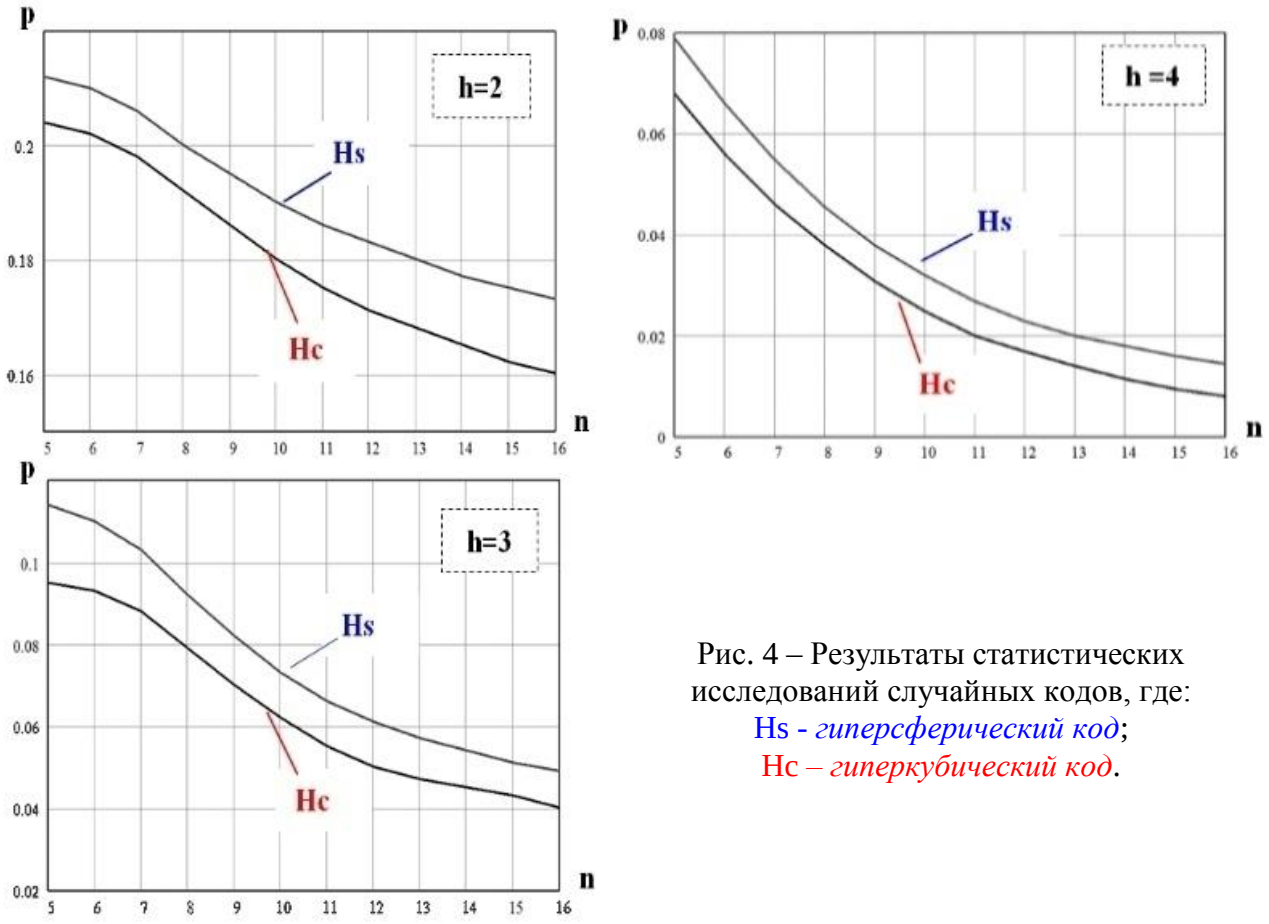

Рис. 4 – Результаты статистических исследований случайных кодов, где:
Hs - *гиперсферический код*;
Hc – *гиперкубический код*.

Анализ результатов статистических испытаний позволяет сделать заключение о несомненном преимуществе гиперкубических случайных кодов, получаемых при равномерном распределении символов кода в пределах заданного числового диапазона (7).

5 Математическая модель и пространственная структура псевдослучайных кодов линейной конгруэнтной генерации

Поскольку равномерное распределение символов обеспечивает лучшие характеристики случайных кодов, то для получения псевдослучайных кодовых книг целесообразно использовать детерминированные алгоритмы, обеспечивающие аппроксимацию (7), (8).

Наиболее простым и распространенным алгоритмом генерации равномерно распределенных псевдослучайных последовательностей (ПСП) является использование линейного конгруэнтного генератора (ЛКГ) [6]. При формировании канального кода получаемые числа, равномерно распределенные в заданном диапазоне, отождествляются с некоторыми значениями одного из информативных параметров сигнала (амплитудой, частотой или фазой). Под-

ходящими переносчиками для построения числовых кодов являются амплитудно-фазовые, частотные, амплитудно-частотные и времяимпульсные методы модуляции, допускающие многоуровневую шкалу градации одного или нескольких информативных параметров. Представление физической модели случайных кодов в канале не является предметом данной статьи, поэтому в дальнейшем рассматриваться не будет.

В соответствии со свойствами линейных конгруэнтных последовательностей [6] элементы векторов кодовых слов $\overrightarrow{kb_i} = \left\{ x_0^i, x_1^i, \cdots x_{n-1}^i \right\}$ имеют следующие значения:

• – $x_0^i = i \in \left[0 \cdots (M-1) \right]$, – число, определяющее порядковый номер i блока двоичных символов источника и являющееся порождающим числом ПСП;

• – $x_k^i = \mathrm{mod}\left[a x_{k-1}^i + b, m \right]$, k ∈ 1...n-1 (9)

числа ПСП, порождаемые x_0^i по рекуррентному алгоритму ЛКГ;

• – *a,b,m* – целые положительные константы, удовлетворяющие условиям: $m \geq M$, *b* и *m* - взаимно простые числа, величина *(a-1)* кратна любому простому числу, которое меньше *m* и является его делителем;

• – *(a-1)* кратно четырем, если *m* кратно четырем.

Очевидно, что при выполнении данных условий произвольное *k*-тое число *i*-того кодового вектора связано с порождающим числом ПСП x_0^i зависимостью:

$$\mathrm{x_k}^{\mathrm{i}} = \mathrm{mod}\left[\mathrm{a^k x_0}^{\mathrm{i}} + \frac{\mathrm{a^k} - 1}{\mathrm{a} - 1} \mathrm{b}, \mathrm{m} \right], \quad \mathrm{k} \in 1 \ldots \mathrm{n} - 1 \tag{10}$$

Таким образом, для получения любого кодового слова ПСК ЛКГ достаточно задание номера *i* и осуществления *(n-1)* рекуррентных вычислений по правилу (9) или (10). Это, в отличие от случайных кодов, избавляет от необходимости хранения в памяти передатчика и приемника полных кодовых книг. Каждая итерация (9), (10) содержит только одну нелинейную математическую операцию вычисления по модулю *m*. Это потенциально облегчает нахождение простого математического алгоритма не переборного декодирования, при этом процесс декодирования, по сути, может быть охарактеризован, как *факторизация* ПСП. Детерминированность алгоритма генерации псевдослучайных кодовых слов является причиной регулярной пространственной структуры кодовых книг ПСК ЛКГ. Это является естественным, поскольку получаемый код относится к классу линейных.

Для примера, на рис. 5 представлены сечения пространства ПСК ЛКГ девятью перпендикулярными плоскостями при *k=10, n=10, R=1, a=5, b=19, m=2^k*.

Геометрия кодовой книги ПСК ЛКГ демонстрирует неравномерность распределения взаимных расстояний кодовых точек в различных плоскостях. Несмотря на это корректно отнести ПСК ЛКГ к классу гиперкубических кодов. Для выравнивания энергетических условий с условиями, в которых рассматривались случайные коды Hs и Hc, после первичного формирования по правилам (9), (10), кодовая книга ПСК ЛКГ $KbL = \left\{ \overrightarrow{kbL} \right\}$, перед получением сечений, показанных на рис. 5, подвергнута центрированию и нормировке:

$$\overrightarrow{KbL} = \left(KbL - \frac{M-1}{2} \right) \left(\frac{M^2 - 1}{12} \right)^{-\frac{1}{2}}, \tag{11}$$

6 Статистическое исследование ПСК ЛКГ

Представляет интерес сравнение вероятностных свойств псевдослучайного кода ЛКГ с полученными ранее свойствами равномерно случайных гиперкубических кодов Hc. Для статистической оценки вероятности декодирования с ошибкой использовалось правило максимального правдоподобия и алгоритм, показанный на рис. 3.

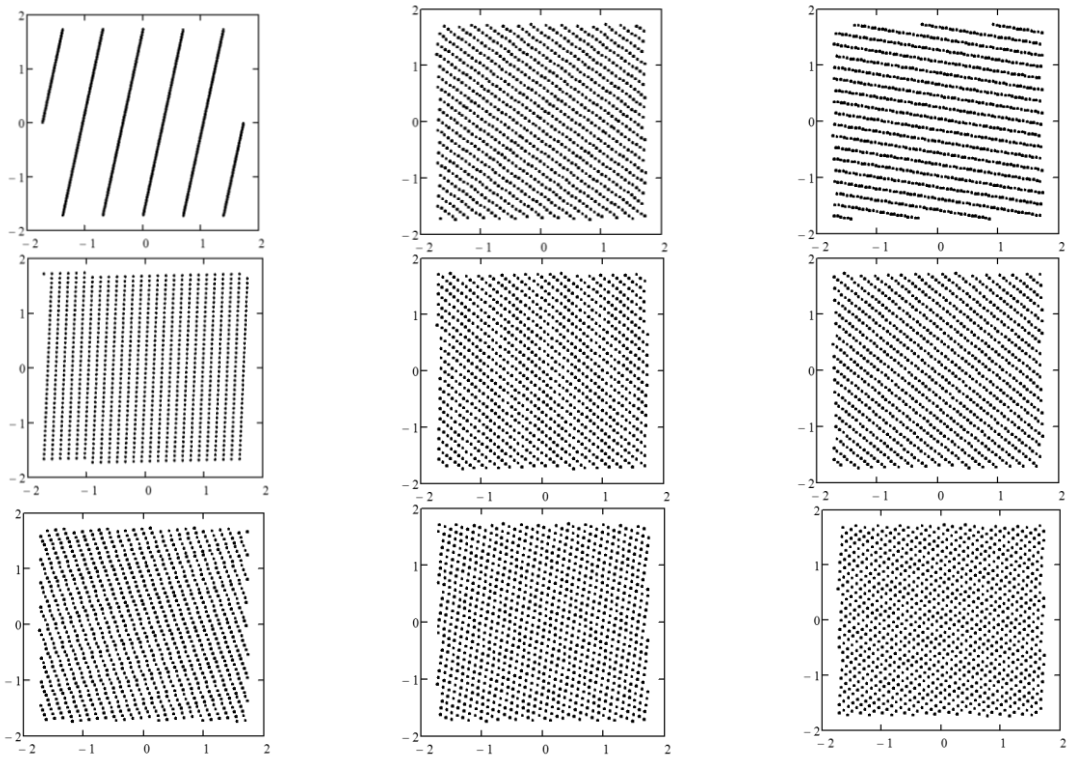

Рис. 5 – Сечения пространства ПСК линейной конгруэнтной генерации

Отсутствие свойства равномерно случайного распределения числовых символов кодовых слов ПСК ЛКГ, которое является следствием использования детерминированного способа генерации этих символов, проявляется в скачкообразном изменении остаточной вероятности декодирования с ошибкой p при изменении длины блока кода n. Результаты вычислительного эксперимента по исследованию вероятностных свойств ПСК ЛКГ для трех значений отношения сигнал/шум в гауссовом канале представлены на рис. 6.

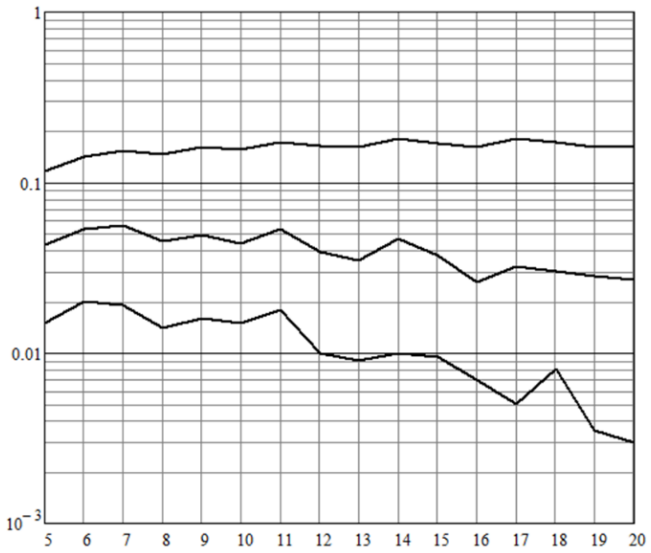

Рис. 6 – Результаты статистических исследований ПСК ЛКГ

Анализ полученных на рис. 6 зависимостей позволяет выявить несколько особенностей псевдослучайных кодов по сравнению со случайными кодами, характеристики которых показаны выше на рис. 4. Данные особенности можно описать следующим образом:

– функции p(n) не являются монотонными;

– при сохранении порядка величины p на уровне, соответствующем гиперкубическим случайным кодам Hc, наблюдается некоторое замедление снижения средней вероятности ошибки с ростом длины блока n. Это означает, что для достижения требуемой величины вероятности ошибки при заданном отношении сигнал/шум при использовании ПСК ЛКГ в условиях фиксированной скорости R необходимо использовать коды с большей длиной блока n, чем при использовании кодов Hc.

Кроме того, статистическое исследование ПСК ЛКГ позволило сформулировать два дополнительных требования к выбору параметров конгруэнтной генерации. Во-первых, наилучшее (в среднестатистическом смысле) значением аддитивной константы b рекуррентного алгоритма (9) является следующее правило:

$$b = 2^{n-1} \pm \beta, \qquad (12)$$

где $\beta=1,3,5\ldots$ – нечетное.

Во вторых, недопустимые значения мультипликативной константы a в условии (9) описываются выражением:

$$a = 2^{Q}+1, \quad \text{при } Q > 3. \qquad (13)$$

Полученные выражения (12) и (13) дополняют набор правил по выбору параметров стандартной конгруэнтной генерации в приложениях построения псевдослучайных кодов.

7 Выводы

Основным результатом данной работы является синтез универсальных математических моделей случайных кодов гиперсферической и гиперкубической укладки, а также модели псевдослучайного кода линейной конгруэнтной генерации.

Результаты статистического исследования полученных моделей позволили оценить вероятностные свойства кодов и сделать однозначное заключение о предпочтительности кодов гиперкубической укладки.

Использование детерминированного метода генерации кодовых слов ПСК на основе метода ЛКГ позволяет получить гиперкубические коды, практически совпадающие по своим свойствам со случайными кодами.

В ходе статистических исследований сформулированы дополнительные требования, касающиеся выбора параметров генерации ПСК с применением ЛКГ.

Ссылки

1. Shannon C.E. A Mathematical Theory of Communication / Shannon C. E. // Bell Syst. Tech. J., Julay-Oct. 1948. – Vol. 27. – P. 379 – 423, 623 – 656. (In English)
2. Shannon C.E. Communication in the presence of noise / Shannon C. E. // Proc. IRE.,Jan. 1949. – Vol. 37. – P. 10 – 21. (In English)
3. Hehmming R.V. Teoriya kodirovaniya i teoriya informacii: Per. s angl. – M.: Radio i svyaz', 1983. – 176 s. (In Russian)
4. Shulman N. Random Coding Techniques for Nonrandom Codes / Shulman N. // IEEE Trans. Inf. Theory, Sep. 1999. – Vol. 45, № 6. – P. 2101 – 2104. (In English)
5. Flejshman B.S. Konstruktivnye metody optimal'nogo kodirovaniya dlya kanalov s shumami. – M.: Izd. AN SSSR, 1963.– 224. (In Russian)
6. Rassomahin S.G. Linejnoe celochislennoe dekodirovanie psevdosluchajnyh kodov na osnove metoda otsechenij Gomori / Rassomahin S.G. // Sistemi obrobki informaciï. – 2011. – Vip. 5 (95). – S. 93 – 98. (In Russian)

Reviewer: Victor Krasnobayev, Doctor of Sciences (Engineering), Full Professor, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine. E-mail: krasnobayev@karazin.ua

Received: September 2016.

Authors:
Tamila Lavrovska, PhD student, V.N. Karazin Kharkiv National University, Kharkiv, Ukraine. E-mail: lavrovska92@gmail.com

Investigation of geometry of placement of points of pseudo-random codes in Euclidean space.

Abstract. Analysis of the reasons of crisis of error-correcting coding. Grounded prospects for application of pseudorandom codes and developed their mathematical model. Considered comparative probabilistic characteristics of equal-length and normal casual codes. The evaluation of the properties of the simplest equal-length pseudo-random codes, which were received by method of the linear congruent generation. Proposed of recommendations on the choice of parameters of linear congruent generators code symbols.

Keywords: coding, pseudo-random codes, Euclidean space code, a statistical model of the decoding process.

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

Надійшло: Вересень 2016.

Автори:
Таміла Лавровська, аспірантка, Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: lavrovska92@gmail.com

Дослідження геометрії розміщення точок псевдовипадкових кодів в евклідовому просторі.

Анотація. Проведено аналіз причин кризи завадостійкого кодування. Обгрунтовано перспективність використання завадостійких кодів і розроблена їх математична модель. Розглянуті порівняльні імовірнісні характеристики рівномірних і нормальних випадкових кодів. Проведена оцінка властивостей найпростіших рівномірних псевдовипадкових кодів, отриманих методом лінійної конгруентної генерації. Запропоновані рекомендації по вибору параметрів лінійних конгруентних генераторів кодових слів.

Ключові слова: кодування, псевдовипадкові коди, евклідів простір коду, статистичні моделі процесу декодування.

Vesa A. Niskanen
Ph.D., Adjunct Professor,
Department of Economics & Management, University of Helsinki,
P.O. Box 27 (Latokartanonkaari 9), 00014 Helsinki, Finland
E-mail: vesa.a.niskanen@helsinki.fi

Igor Romenskiy
Doktor für physikalische-mathematische Wissenschaften, GFaI Gesellschaft zur Förderung angewandter Informatik e.V.,
Volmerstraße 3, 12489 Berlin, Deutschland
E-mail: iromensky@mail.ru

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

Vadim Geurkov
Ph.D., Associate Professor,
Department of Electrical and Computer Engineering Ryerson University,
350 Victoria Street, Toronto, Ontario, M5B 2K3, Canada
E-mail: vgeurkov@ee.ryerson.ca

Fionn Murtagh
Ph.D., Professor,
Department of Computing and Mathematics, University of Derby,
Kedleston Road, Derby DE22 1GB, UK
Email: f.murtagh@derby.ac.uk
Department of Computing, Goldsmiths, University of London,
New Cross, London SE14 6NW, UK
E-mail: f.murtagh@gold.ac.uk

C. Pandu Rangan
Ph.D., FNAE, Senior Professor,
Department of Computer Science and Engineering,
Indian Institute of Technology,
Madras, Chennai - 600036, India
E-mail: prangan55@gmail.com

Håvard Raddum
Ph.D.,
Simula Research Laboratory, P.O. Box 134, 1325 Lysaker, Norway
E-mail: haavardr@simula.no

Oleksandr Kazymyrov
Ph.D.,
EVRY Norge AS,
Snarøyveien 30A, 1360 Fornebu, Norway
E-mail: oleksandr.kazymyrov@evry.com

Mikołaj Karpiński
Doctor of Sciences (Engineering), Full Professor,
University of Bielsko-Biala,
ul. Willowa 2, 43-309 Bielsko-Biala, Poland
E-mail: mkarpinski@ath.bielsko.pl

Веса А. Нисканен
доктор філософії, ад'юнкт професор,
департамент економіки та менеджменту, Університет Гельсінкі,
P.O. Бокс 27 (Латокартанонкаарі 9), 00014 Гельсінкі, Фінляндія
E-mail: vesa.a.niskanen@helsinki.fi

Ігор Роменський
доктор фізико-математичних наук,
GFaI - Спілка з просування прикладної інформатики,
Фольмерштрассе 3, 12489 Берлін, Німеччина
E-mail: iromensky@mail.ru

Олексій Стахов
доктор технічних наук, професор, академік Академії інженерних наук України,
Міжнародний Клуб Золотого Перетину,
6 МаккКрері Трейл, Болтон, Онтаріо, L7E 2C8, Канада
E-mail: goldenmuseum@rogers.com

Вадим Геурков
доктор філософії, доцент,
факультет електротехніки та обчислювальної техніки університету Раєрсон,
350 Вікторія-стріт, Торонто, Онтаріо, M5B 2K3, Канада
E-mail: vgeurkov@ee.ryerson.ca

Фінн Мерта
доктор філософії, професор,
факультет обчислювальної математики університету Дербі,
Кедлестон Роад, Дербі DE22 1GB, Великобританія
Email: f.murtagh@derby.ac.uk
факультет обчислень Голдсмітського коледжу Лондонського університету,
Нью-Крос, Лондон SE14 6NW, Великобританія
E-mail: f.murtagh@gold.ac.uk

С. Панду Ранган
доктор філософії, FNAE, старший викладач,
факультет комп'ютерних наук та інженерії Індійського технологічного інституту,
Мадрас, Ченнаї - 600036, Індія
E-mail: prangan55@gmail.com

Ховард Радум
доктор філософії,
науково-дослідна лабораторія Симула, P.O. Бокс 134, 1325, Лісакер, Норвегія
E-mail: haavardr@simula.no

Олександр Казіміров
доктор філософії,
EBPI Норге АС,
Снаройвиен 30A, 1360 Форнебу, Норвегія
E-mail: oleksandr.kazymyrov@evry.com

Микола Карпінський
доктор технічних наук, професор,
Університет Бельсько-Бяла,
вул. Віллова 2, 43-309 Бельсько-Бяла, Польща
E-mail: mkarpinski@ath.bielsko.pl

Volodymyr Khoma
Doctor of Sciences (Engineering), Full Professor,
Institute «Automatics and Informatics», The Opole University of Technology,
76 Prószkowska Street, 45-758 Opole, Poland
E-mail: xoma@wp.pl

Joanna Świątkowska
Ph.D., CYBERSEC Programme Director,
Senior Research Fellow of the Kosciuszko Institute,
Feldmana ul. 4/9-10, 31-130 Kraków,
Poland
E-mail: joanna.swiatkowska@ik.org.pl

Nick Bilogorskiy
Director of Security Research,
Cyphort, 5451 Great America Parkway, Suite 225,
Santa Clara, California 95054, USA
E-mail: nick@novaukraine.org

Richard Kemmerer
Ph.D., Professor,
Computer Science Department, University of California,
Santa Barbara, CA 93106, USA
E-mail: kemm@cs.ucsb.edu

Dimiter Velev
Ph.D., Professor,
Department of Information Technologies and Communications, Faculty of Applied Informatics and Statistics, University of National and World Economy,
„8-ми декември“ st., UNSS - Studentski grad, 1700
Sofia, Bulgaria
E-mail: dgvelev@unwe.bg

Robert Brumnik
Ph.D., Professor Assistant,
GEA College, Dunajska cesta 156, 1000 Ljubljana,
Slovenia
Metra Engineering Ltd, Špruha 19, 1236 Trzin, Slovenia
E-mail: robert.brumnik@metra.si

Stephan Dempe
Ph.D., Professor,
Department of Mathematics and Computer Science,
Technical University Bergakademie Freiberg, Germany
Akademischestrafte 6, D-09596, Freiberg,
Germany
E-mail: dempe@math.tu-freiberg.de

Ludmila Babenko
Doctor of Sciences (Engineering), Full Professor,
Institute of Computer Technologies and Information Safety of Southern Federal University
Chekhov str., 2, Taganrog, Rostov obl., Russia
E-mail: blk@tsure.ru

Valeriy Zadiraka
Doctor of Sciences (Physics and Mathematics),
Full Professor, Academician of the National Academy of Sciences of Ukraine, Glushkov Institute of Cybernetics (GIC) of National Academy of Sciences of Ukraine,
40 Glushkov av., Kyiv, 03187, Ukraine
E-mail: zvk140@ukr.net

Володимир Хома
доктор технічних наук, професор,
Інститут «Автоматика та інформатика», Технологічний університет Ополе,
вул, Пружовська 76, 45-758 Ополе, Польща
E-mail: xoma@wp.pl

Джоана Святковська
доктор філософії, директор програми CYBERSEC,
старший науковий співробітник Інституту Костюшки
вул. Фельдман 4 / 9-10, 31-130 Краків,
Польща
E-mail: joanna.swiatkowska@ik.org.pl

Нік Білогорський
директор з досліджень безпеки,
Цифорт, 5451 Гріт Америка Парквей, Люкс 225,
Санта-Клара, Каліфорнія 95054, США
E-mail: nick@novaukraine.org

Річард Кеммерер
доктор філософії, професор,
факультет інформатики, Каліфорнійський університет,
Санта-Барбарі, CA 93106, США
E-mail: kemm@cs.ucsb.edu

Дімітер Велев
доктор філософії, професор,
кафедра інформаційних технологій і комунікацій,
факультет прикладної інформатики та статистики,
Університет національної та світової економіки,
вул. "8-ми декември", UNSS - Студентські град, 1700
Софія, Болгарія
E-mail: dgvelev@unwe.bg

Роберт Брумнік
доктор філософії, доцент,
GEA коледж, Дунайська цеста 156, 1000 Любляна,
Словенія
Метра Інжиніринг ЛТД, Шпруха 19,1236 Тржин,
Словенія
E-mail: robert.brumnik@metra.si

Стефан Демп
доктор філософії, професор,
факультет математики та інформатики, технічний університет Фрайберзької Гірничої Академії,
Німеччина
Akademischestrafte 6, D -09596, Фрайберг, Німеччина
E-mail: dempe@math.tu-freiberg.de

Людмила Бабенко
доктор технічних наук, професор,
Інститут комп'ютерних технологій та інформаційної безпеки Південного федерального університету
вул. Чехова 2, Таганрог, Ростовська обл., Росія
E-mail: blk@tsure.ru

Валерій Задірака
доктор технічних наук, професор,
академік Національної академії наук України,
Інститут кібернетики імені В.М. Глушкова
Національної академії наук України,
проспект Академіка Глушкова, 40, Київ, 03187, Україна
E-mail: zvk140@ukr.net

Ludmila Kovalchuk
Doctor of Sciences (Engineering), Associate Professor,
Department of mathematical methods of information security Institute of Physics and Technology,
National Technical University of Ukraine
"Kyiv Polytechnic Institute"
37, Prospect Peremohy, 03056, Kyiv-56, Ukraine
E-mail: lusi.kovalchuk@gmail.com

Людмила Ковальчук
доктор технічних наук, доцент,
кафедра математичних методів захисту інформації фізико-технічного інституту
національного технічного університету України «КПІ»,
03056, Київ, пр. Перемоги, 37, НТУУ "КПІ"
E-mail: lusi.kovalchuk@gmail.com

Anton Alekseychuk
Doctor of Sciences (Engineering), Associate Professor,
Department of application of means of cryptographic and technical defense of information, Institute of Special Communication and Information Security,
National Technical University of Ukraine
"Kyiv Polytechnic Institute"
37, Prospect Peremohy, 03056, Kyiv-56, Ukraine
E-mail: alex-dtn@ukr.net

Антон Олексійчук
доктор технічних наук, доцент,
кафедра застосування засобів криптографічного та технічного захисту інформації Інституту спеціального зв'язку та захисту інформації національного технічного університету України «КПІ»,
03056, Київ, пр. Перемоги, 37, НТУУ "КПІ"
E-mail: alex-dtn@ukr.net

Volodymyr Maxymovych
Doctor of Sciences (Engineering), Full Professor,
Institute of Computer Technologies, Automation and Metrology (ICTA), Lviv Polytechnic National University,
12 Bandera st., Lviv, 79013, Ukraine
E-mail: vmax@polynet.lviv.ua

Володимир Максимович
доктор технічних наук, професор,
Інститут комп'ютерних технологій, автоматики та метрології Національного університету «Львівська політехніка»,
вул. Степана Бандери, 12, м. Львів, 79013, Україна
E-mail: vmax@polynet.lviv.ua

Oleksiy Borysenko
Doctor of Sciences (Engineering), Full Professor,
Sumy State University,
2, Rymskogo-Korsakova st., 40007 Sumy, Ukraine
E-mail: 5352008@ukr.net

Олексій Борисенко
доктор технічних наук, професор,
Сумський державний університет,
вул. Римського-Корсакова, 2, 40007 Суми, Україна
E-mail: 5352008@ukr.net

Anatoliy Biletsky
Doctor of Sciences (Engineering), Full Professor,
Institute of Air Navigation, National Aviation University,
Kosmonavta Komarova av. 1, Kyiv, 03058, Ukraine
E-mail: abelnau@ukr.net

Анатолій Білецький
доктор технічних наук, професор,
навчально-науковий інститут аеронавігації національного авіаційного університету,
пр. Космонавта Комарова 1, Київ, 03058, Україна
E-mail: abelnau@ukr.net

Sergii Kavun
Doctor of Sciences (Economics), Ph.D. (Engineering),
Full Professor, Department of Information Technologies,
Kharkiv Educational and Research Institute
of the University of Banking,
Peremogy av. 55, Kharkiv, 61174, Ukraine
E-mail: kavserg@gmail.com

Сергій Кавун
доктор економічних наук, кандидат технічних наук,
професор, кафедра інформаційних технологій,
Харківський навчально-науковий інститут
ДВНЗ "Університет банківської справи",
пр. Перемоги 55, м. Харків, 61174, Україна
E-mail: kavserg@gmail.com

Vyacheslav Kharchenko
Doctor of Sciences (Engineering), Full Professor,
Academician of the Academy of Applied Radioelectronics Sciences, N.Ye. Zhukovskiy National Aerospace University – Kharkiv Aviation Institute (KhAI),
17 Chkalov st., 61070, Kharkiv, Ukraine
E-mail: v_s_kharchenko@ukr.net

В'ячеслав Харченко
доктор технічних наук, професор,
академік Академії наук прикладної радіоелектроніки,
Національний аерокосмічний університет
ім. М. Є. Жуковського,
вул. Чкалова, 17, 61070, м. Харків, Україна
E-mail: v_s_kharchenko@ukr.net

Valentin Lazurik
Doctor of Sciences (Physics and Mathematics),
Full Professor, V. N. Karazin Kharkiv National University,
Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: vtlazurik@karazin.ua

Валентин Лазурик
доктор фізико-математичних наук, професор,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: vtlazurik@karazin.ua

Volodymyr Kuklin
Doctor of Sciences (Physics and Mathematics),
Full Professor, V. N. Karazin Kharkiv National University,
Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: kuklinvm1@gmail.com

Ivan Gorbenko
Doctor of Sciences (Engineering), Full Professor,
Academician of the Academy of Applied Radioelectronics Sciences, V. N. Karazin Kharkiv National University,
Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: gorbenkoi@iit.kharkov.ua

Victor Krasnobayev
Doctor of Sciences (Engineering), Full Professor,
Honourable Inventor of Ukraine,
Honourable Radio Specialist of the USSR,
V. N. Karazin Kharkiv National University,
Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: krasnobayev@karazin.ua

Irina Lisitska
Doctor of Sciences (Engineering), Full Professor,
Corresponding Member of the Academy of Applied Radioelectronics Sciences,
V. N. Karazin Kharkiv National University,
Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: lisitska@karazin.ua

Oleksandr Potii
Doctor of Sciences (Engineering), Full Professor,
Academician of the Academy of Applied Radioelectronics Sciences, V. N. Karazin Kharkiv National University,
Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: potav@ua.fm

Viktor Dolgov
Doctor of Sciences (Engineering), Full Professor,
Academician of the Academy of Applied Radioelectronics Sciences, V. N. Karazin Kharkiv National University,
Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: dolgovvi@mail.ru

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

Volodymyr Mashtalir
Doctor of Sciences (Engineering), Full Professor,
V. N. Karazin Kharkiv National University,
Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: mashtalir@kture.kharkov.ua

Grygoriy Zholtkevych
Doctor of Sciences (Engineering), Full Professor,
V. N. Karazin Kharkiv National University,
Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: g.zholtkevych@karazin.ua

Володимир Куклін
доктор фізико-математичних наук, професор,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: kuklinvm1@gmail.com

Іван Горбенко
доктор технічних наук, професор, академік Академії наук прикладної радіоелектроніки,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: gorbenkoi@iit.kharkov.ua

Віктор Краснобаєв
доктор технічних наук, професор, заслужений винахідник України, почесний радист СРСР,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: krasnobayev@karazin.ua

Ірина Лисицька
доктор технічних наук, професор,
член-кореспондент Академії наук прикладної радіоелектроніки, Харківський національний університет імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: lisitska@karazin.ua

Олександр Потій
доктор технічних наук, професор,
академік Академії наук прикладної радіоелектроніки,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: potav@ua.fm

Віктор Долгов
доктор технічних наук, професор,
академік Академії наук прикладної радіоелектроніки,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: dolgovvi@mail.ru

Роман Олійников
доктор технічних наук, професор,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: roliynykov@gmail.com

Володимир Машталір
доктор технічних наук, професор,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: mashtalir@kture.kharkov.ua

Григорій Жолткевич
доктор технічних наук, професор,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: g.zholtkevych@karazin.ua

Статті пройшли внутрішнє та зовнішнє рецензування.

Наукове видання

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА

Випуск 3(3) 2016

Міжнародний електронний науково-теоретичний журнал

Англійською, українською, російською мовами

Комп'ютерне верстання – Федоренко В.В.

61022, Харків, майдан Свободи, 6
Харківський національний університет імені В.Н. Каразіна

V. N. Karazin Kharkiv National University Publishing